UNIVERSITY OF RWANDA
AFRICAN CENTRE OF EXCELLENCE IN INTERNET OF THINGS (ACEIoT)
KIGALI-RWANDA

IMPROVED USABLE-SECURITY IN USER AUTHENTICATION OF THE INTERNET OF MEDICAL THINGS

PhD. THESIS

PRUDENCE MUNYARADZI MAVHEMWA

DOCTORAL DISSERTATION IN

INTERNET OF THINGS – EMBEDDED COMPUTING SYSTEMS

SEPTEMBER 2025

UNIVERSITY OF RWANDA

AFRICAN CENTRE OF EXCELLENCE IN INTERNET OF THINGS (ACEIoT)

IMPROVED USABLE-SECURITY IN USER AUTHENTICATION OF THE INTERNET OF MEDICAL THINGS

PhD. THESIS

PRUDENCE MUNYARADZI MAVHEMWA

(221018837)

DOCTORAL DISSERTATION IN

INTERNET OF THINGS – EMBEDDED COMPUTING SYSTEMS

Main Supervisor : Dr. Marco Zennaro, PhD

Co–Supervisors : Dr. Philibert Nsengiyumva, PhD

Dr. Frederic Nzanywayingoma, PhD

SEPTEMBER 2025

Declaration

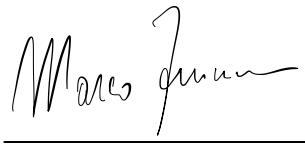
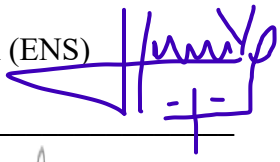
I hereby declare that the dissertation entitled " *Improved Usable-Security In User Authentication Of The Internet Of Medical Things"* to be submitted for the Degree of Doctor of Philosophy is my original work and the dissertation has not formed the basis for the award of any degree, diploma, associateship or fellowship of similar other titles. It has not been submitted to any other University or Institution for the award of any degree or diploma.

Prudence Munyaradzi Mavhemwa

Signature……

Date: **5th September 2025**

Prudence M. Mavhemwa, a PhD student of UR-ACEIoT registration ID **221018837**, successfully defended the PhD thesis/dissertation entitled "**Improved Usable-Security In User Authentication Of The Internet Of Medical Things**", which he prepared after fulfilling the requirements specified in the associated legislation, before the thesis examination members whose signatures are below.

Thesis Supervisor:	**Dr. Marco Zennaro** ICTP	
Co-Supervisor:	**Dr. Philibert Nsengiyumva** University of Rwanda	
Resident Co-Supervisor:	**Dr. Frederic Nzanywayingoma** University of Rwanda	
Viva Voce Members:	**Prof. Wali U. Garba (Chair)** University of Rwanda	
	Prof. Abdi T. Abdalla University of Dar es Salaam	
	Prof. Vincent Hayarimana Burundi Higher Institute of Education (ENS)	
	Dr. Mwitende Gervais Rwanda Polytechnic	
Date of Defense:	**03/09/2025**	

Dedication

To Marilyn, Kayleen & Adelene

You deserve special recognition, my daughters, for you are my inspiration and joy. You are my source of strength, and you make me a better person. Your energy, desires, joy, love and exceptional performance at school are a constant reminder that I must set a standard for you, a standard that you will surpass. I hope you also find as much inspiration as I find in you, and you shall dominate.
Colossians 3:23 "Whatever you do, work at it with all your heart, as working for the Lord, not for human masters."

Acknowledgements

First and foremost, I want to express my sincere gratitude to God, the Almighty, for taking me this far. Without His grace, I would not have made it this far, and I say Ebenezer. By His grace, I gained the courage and strength to do my research in pursuit of academic excellence.

I would also like to thank my supervisor, Dr. Marco Zennaro, and co-supervisors, Dr. Philibert Nsengiyumva, Frederic Nzanywayingoma, Prof. Herman Myburgh, and Dr. Allan de Freitas, for their continuous guidance and support, as well as for providing me with the opportunity to work under their supervision. My heartfelt gratitude goes out to Dr. Marco Zennaro for his professional and technical support during this journey. His unwavering support and motivation gave me the fortitude I needed to finish my studies. I would also be remiss if I did not separately express my gratitude to Dr. Allan de Freitas for his technical guidance; he helped mould and encourage me to be where I am today.

I would like to thank Mr. Leo Hassan Ali for his dedication, patience, and technical assistance during my research. Prototype development and evaluation would not have been feasible without your technical assistance, and I am eternally thankful. Words cannot explain how grateful I am to my colleagues, Barbara K Asingwire, Eric Nizeyimana, and Fidele Maniraguha. You became a family that fostered a positive learning environment. Your encouragement helped me stay strong and hopeful during this journey. I will always be grateful to you.

My heartfelt appreciation and thoughts also go to my siblings Kudzai, Namatai, and Kumbirai, as well as my late sister Gamuchirai. Gamuchirai, I know you would be proud of me today because you were so supportive of me during my studies; continue to rest in peace. Thank you for believing in me and being there for me, for enduring the loneliness when I was away. You covered for me, and your prayers were extremely helpful; I will be eternally thankful.

Most significantly, I want to thank my beloved wife, Laika, and our gorgeous daughters, Marilyn Tawananyasha, Kayleen Makanaka, and Adelene Munenyasha. Your encouragement, support, and patience sustained me throughout this journey. You carried the burden with me. My daughters, you missed major events throughout your lives because of my absence, but you believed in me and prayed for me. My wife, you put up with my late nights with you despite my limited time at home. I thank God for all of you, and may He generously reward you.

This PhD journey would not have been possible without PASET-RSIF's generous funding, which provided me with the opportunity to pursue this journey. Their scholarship allowed me to attend the prestigious University of Rwanda, and I am forever grateful. I would also like to thank the director of ACEIoT, Prof. Damien Hanyurwimfura. You are God sent, and may God generously bless you. I would like to express my heartfelt gratitude to Dr. Omar Gatera, the head of postgraduate studies, and the entire Centre team. Continue to provide unconditional support, encouragement, and advice, and God will bless you abundantly. My gratitude also extends to Prof Manatsa, Prof Nyambo, and former colleagues at Bindura University of Science Education. You nurtured and encouraged me, and I am always grateful and beholden to you.

Prudence M. Mavhemwa
Kigali – Rwanda
September 2025

Abstract

The ever-increasing global disease burden, exacerbated by pandemics like COVID-19 and other global scourges, underscores the critical need for robust healthcare solutions that complement often overburdened medical staff. The Internet of Medical Things (IoMT) offers a transformative possibility, especially for regions such as Sub-Saharan Africa (SSA), where conventional healthcare models are predominant, yet they encounter significant challenges.

However, the successful adoption of IoMT is hampered by prevalent cybersecurity threats, mostly stemming from the increased online activity of untrained users and the inherent security and usability deficiencies of current authentication systems. This thesis contributes to addressing these critical gaps by developing and evaluating a novel Machine Learning (ML) based adaptive user authentication framework aimed at improving secure and seamless access to medical IoT resources. The framework employs an edge-centric methodology, fusing the Naive Bayes classifier with the CoFRA model to dynamically evaluate the authenticity and associated risk of a login attempt.

This risk assessment is based on a comprehensive set of inputs, including biometric wearable sensor data, non-biometric smartphone sensor data, and predefined user contextual information. Through a User-Centred Design (UCD) methodology, an Android application was developed and tested with a PineTime smartwatch connected via Bluetooth Low Energy, demonstrating the practical application of the model.

Our results show that users consistently prefer basic physiological biometrics for authentication, regardless of their age, experience, or level of ICT proficiency. Simulation was conducted and comparative analyses across various ML algorithms, including Naive Bayes variations, Decision Trees, SVM, XGB, and Random Forests, demonstrated superior performance with weighted datasets, highlighting the importance of data characteristics and splitting methodologies. Other classifiers performed exceptionally well in multi-classification circumstances, whereas Naive Bayes demonstrated optimum performance for up to three authentication classes. Despite noted shortcomings, including class imbalance and a 19% false rejection rate, post-deployment evaluations verified good accuracy (100% and 98.6% in useful security metrics) and great user acceptability of the application.

Ultimately, this research provides a user-centric and context-aware authentication solution that adapts to individuals' personal profiles such as age, risk scores, and health conditions, enabling secure access while striking a balance between security rigor and usability.

By enhancing technology adherence and fostering confidence in digital health solutions, this adaptive authentication model significantly contributes to improving patient care, easing caregiver burdens, and advancing the attainment of Sustainable Development Goal (SDG) 3: Ensure healthy lives and promote well-being for all at all ages.

Future work will explore explainable AI and advanced risk assessments to further refine the framework's capabilities.

Preface

This thesis summarises the work I conducted on improving usable security in user authentication of the Internet of Medical Things. The work was carried out at the African Centre of Excellence in Internet of Things, College of Science and Technology, University of Rwanda. The thesis consists of five sections (introduction, literature, methodology, overall conclusion and future works) with the methodology including three research parts, which are the following:

Part I

User-Centred design of a Machine Learning-based adaptive user authentication framework for Internet of Medical Things (IoMT).

Part II

Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication.

Part III

A. An Android-Based Internet Of Medical Things Adaptive User Authentication And Authorisation Model For The Elderly.
B. Naïve Bayes Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users.

Publications

Part I is published as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma, "User-Centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones." Lecture Notes in Networks and Systems book series (LNNS, volume 724), Pages 783-799. Published July 2023. URL: https://link.springer.com/chapter/10.1007/978-3-031-35314-7_65

Part II is published as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma, "Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication." Journal of Physics Communications, Volume 8, Issue 10, 2024, Page 105005, Publisher: IOP Publishing, doi =0.1088/2399-6528/ad8a16, URL = https://dx.doi.org/10.1088/2399-6528/ad8a16

Part III-A is published as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma, "An Android-Based Internet Of Medical Things Adaptive User Authentication And Authorisation Model For The Elderly," J.Cybersecur. Priv. 2024, 4, 993–1017. https://doi.org/10.3390/jcp4040046.

Part III-B is based on the following article:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma," Naïve Bayes Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users." Submitted for publication (accepted).Publisher: IET Communications, **Print ISSN:** 1751-8628,**Online ISSN:** 1751-8636,**Article ID:** CMU270082

Acronyms

ACEIoT	African Centre of Excellence in Internet of Things
ADABoost	Adaptive Boosting
AI	Artificial Intelligence
AUC	Area Under the ROC Curve
BLE	Low-energy Bluetooth
BVP	Blood Volume Pulse
CA	Continuous Authentication
CAGR	Compound Annual Growth Rate
CASA	Context-Aware Scalable Authentication
CoFRA	Context-driven modelling Framework
CYOA	Choose Your Own Authenticator
DAC	Discretionary Access Control
DH	Digital Health
DID	Decentralised Identities (DIDs)
DT	Decision Trees
DTLS	Datagram Transport Layer Security
ECG	Electrocardiography
EER	Equal Error Rate
FAR	False Acceptance Rate
FNR	False Negative Rate
FPR	False Positive Rate
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HFACS	Human Factors Analysis and Classification System
HIPAA	Health Insurance Portability and Accountability Act
HRV	Heart Rate Variability
IDC	International Data Cooperation

IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MAC	Mandatory Access Control
MAPE-K$_{HMT}$	Monitor Analyse Plan Execute – Knowledge with Human Machine Teaming
MDGs	Millennium Development Goals
MENA	Middle East and North Africa
MFA	Multi-Factor Authentication
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NB	Naïve Bayes
NPV	Negative Predictive Value
OTP	One-Time Password
PIN	Personal Identification Number
PPG	Photoplethysmography
PPV	Positive Predictive Value
RBA	Risk-Based Authentication
RBAC	Role-Based Access Control
RMSSD	Root Mean Square of Successive Differences
RSIF-PASET	Regional Scholarship and Innovation Fund – Partnership for Applied Skills in Science, Engineering and Technology
SDGs	Sustainable Development Goals
SDNN	Standard Deviation of Normal RR (NN) Intervals
SSA	Sub-Saharan Africa
SVM	Support Vector Machine
TAM	Technology Acceptance Model
TLS	Transport Layer Security
UCD	User Centred Design
VCs	Verifiable Credentials

Wi-Fi	Wireless Fidelity
XGB	eXtreme Gradient Boosting

Contents

Contents

Prudence M. Mavhemwa

This page has been intentionally left blank

1 Introduction

1.0 Motivation

At some point during a person's sickness, constant dependence on the caregiver can become frustrating, as the patient may feel helpless. However, because everyone is susceptible to illness and caregivers have other obligations in their personal lives, they cannot always be there to keep an eye on the patient [1]. In 2015, nations adopted seventeen Sustainable Development Goals (SDGs) as a successor to Millennium Development Goals (MDGs), aiming at ending extreme poverty, hunger, health, gender equality, clean water, sanitation, energy, economic growth, industry, innovation, infrastructure, reduced inequality, sustainable cities, climate action, marine conservation, peace, justice, and international cooperation [2]. SDGs are an expansion of the MDGs and are nationally owned and cater for all countries, whether rich, middle, or poor, unlike the latter, which targeted developing countries only [2]. These SDGs are universal and applicable to all countries, as they try to capture the most contemporary development issues and are based on the principles of equity, where everyone has to have access to human rights, among other basic amenities [3]. The third goal is to "Ensure healthy lives and promote well-being for all at all ages", WHO [2] and the inclusion of health in the SDGs underscores the importance of addressing health for a nation's socioeconomic growth and prosperity [3]. The Internet of Things (IoT) has become a game-changer in healthcare, with over 70% of US healthcare providers already utilising the IoT in their healthcare systems [4]. Sub-Saharan Africa (SSA) can benefit from these technological advancements to improve the health of its citizens. IoT in the healthcare industry, termed the Internet of Medical Things (IoMT), enables the integration of smart health systems like hospital management, health, and e-health [5].

While some African nations, such as Mauritius, South Africa, Seychelles, Rwanda, and Kenya, have prioritised IoT in health [6] most SSA nations continue to use the conventional hospital-centric model, in which patients frequently visit medical facilities to manage their diseases. This model, centred on disease and physicians, is reactive and fails to actively engage patients in the medical process [4][5]. Also, the quality and scale of medical services usually do not meet the needs of patients [7][8]. Alongside traditional challenges, COVID-19 has significantly impacted

healthcare institutions [9], encouraging people to reduce visits to health centres and instead adopt technology-based solutions to minimise disease spread [10]. IoT has revolutionised the healthcare industry in several ways [3][11][12] which include illness control, cost reduction, autonomous and remote caregiving, diagnostics, newly available patient data, and combating infectious diseases [5][13][14]. The global adoption of IoT in healthcare is increasing. Figure 1 shows the projected growth of IoT in health worldwide.

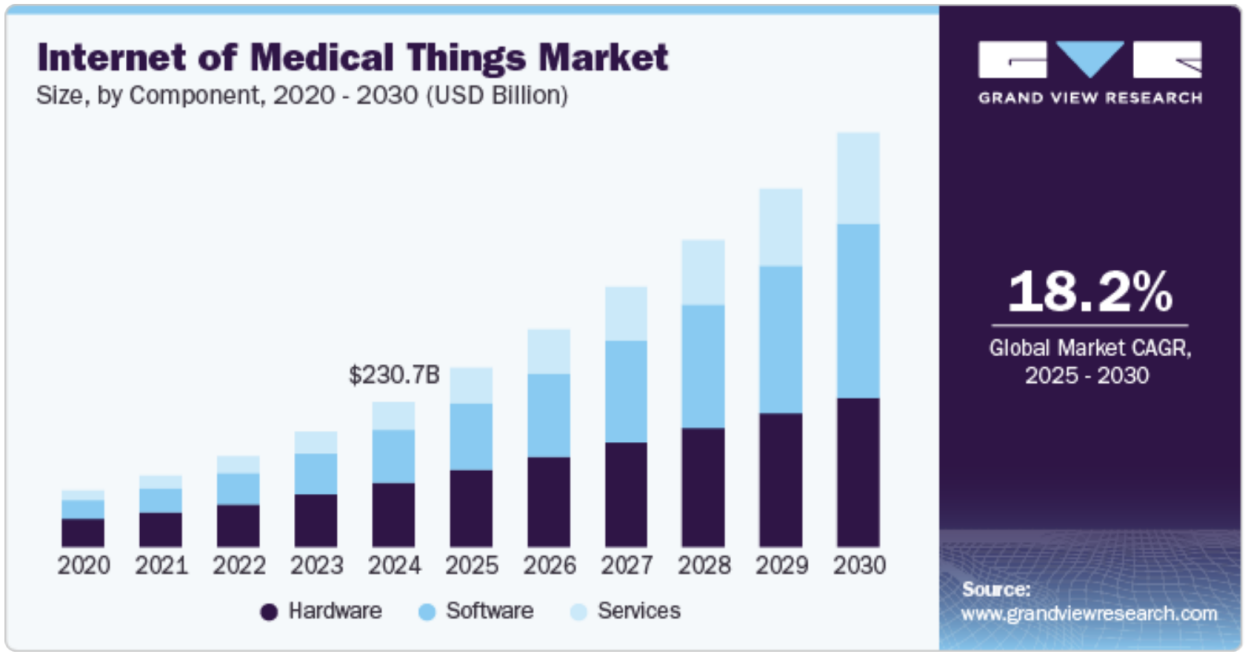


Figure 1: IoMT growth. Adapted from [15]

The global IoMT market was valued at $USD 230.69 billion in 2024 and is expected to increase at a CAGR of 18.2% from 2025 to 2030. The IoMT market is expanding rapidly due to increased demand for remote patient monitoring, wearable technology acceptance, telehealth integration, big data, and improved device accuracy and connectivity [15]. The inpatient monitoring segment is expected to register the fastest CAGR from 2025 to 2030. In 2024, the U.S. in North America dominated the use of IoMT.

Still, SSA has limited activities [6][16][17] although the region holds significant potential for growth due to its highest global growth rate in mobile subscriptions [18][19] and various healthcare applications [17-21]. IoT is the future of the internet and an integrated part of the modern person‘s daily life [22-24], with the IoMT market expected to grow every year. Figure 2 shows some of the areas in healthcare where IoT can be applied.

Figure 2: Medical and healthcare industry in the context of functions, operations, and applications where IoT can be applied. Adapted with permission from [20]

1.0.1 IoT Adoption

The adoption of IoT in SSA, despite its potential, is slow, as evidenced by the few countries already utilising it despite its immense potential to transform the healthcare system [21][22]. Several problems that need to be identified and corrected are slowing down its adoption. IoT devices are increasing every day [23] extending to SSA, which is a mere consumer. Security issues that have not been fully addressed globally are exacerbated in SSA because of its unique challenges. Africans often overestimate their technological knowledge and readiness, leading to increased vulnerability to cybersecurity threats [24]. The unique challenges of SSA necessitate a comprehensive understanding of its sociotechnical issues for the development of tailored solutions [25]. Current IoT initiatives primarily target developed countries Nigussie *et al.* [17] with no clear vision as to what IoT providers can do to ease challenges in regions such as SSA [25] . This calls for security measures like authorisation, privacy, message integrity, content integrity, data security, and authentication.

1.0.2 Security and privacy concerns in healthcare

IoT-enabled healthcare poses security and privacy risks Kuaban *et al.* [26], particularly to humans, due to the potential harm that autonomous devices can cause when improperly configured. Figure 3 shows the top ten vulnerabilities of IoT according to Coll [27].

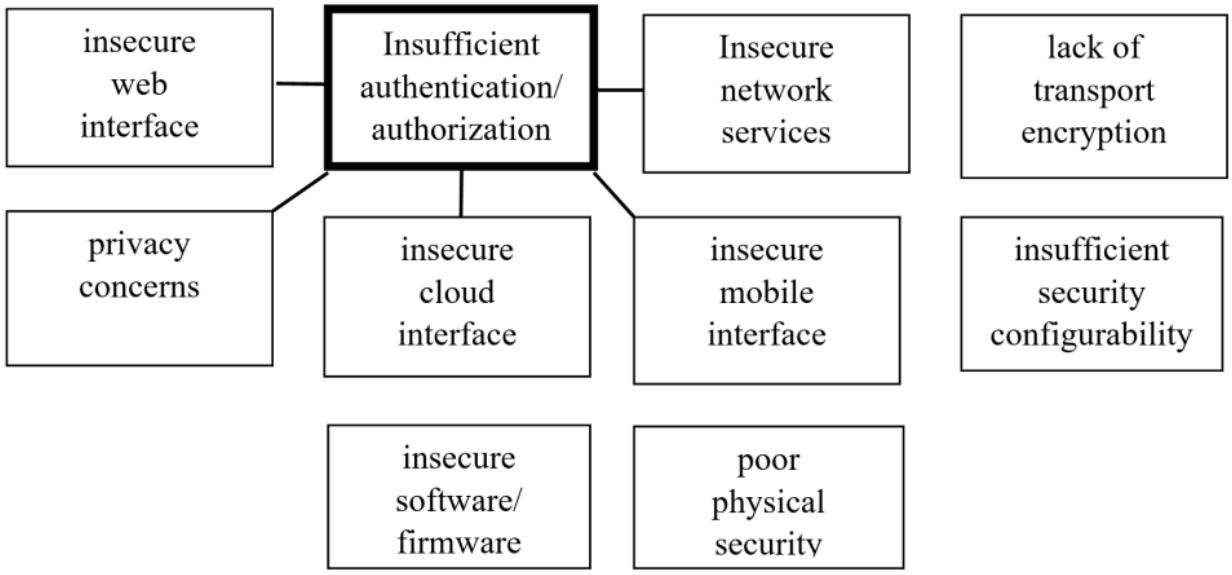


Figure 3 : Top Ten IoT vulnerabilities adapted from www.owasp.org by [27]

There are several security issues related to the use of IoT [28] and IoT requires security, which includes authentication, authorisation, privacy, message integrity, content integrity, and data security [5]. The healthcare industry, which also benefits from IoT, is not exempt from the security and privacy issues [29][27][30]. However, the risk is much greater to humans because these devices act autonomously and can cause harm when improperly configured. They often lack the necessary security [31] which makes them vulnerable to attacks and potential network downfall if compromised Acar *et al.* [30] and cyberattacks exploit flaws in IoMT devices to gain unauthorised access to vital medical data, a prevalent issue in the Middle East and North Africa (MENA) [32]. Medical devices that utilise wireless technologies like Wi-Fi, mobile cellular, or Bluetooth are susceptible to attacks such as interception, disruption, falsification, hijacking, or denial of service [33]. IoMT environments require unique security controls compared to general IoT devices due to their vastly different threat landscape and malicious motives [30].

Current IoMT user authentication techniques face several challenges, demanding a delicate balance between security and usability [34][35]. Challenges include the resource constraints of IoMT devices [36] , diversity and heterogeneity of devices and protocols [37], vulnerability to

traditional attacks [42-45], lack of regular updates and patching [38], a distributed and remote nature [39], data sensitivity [40][41] and insider threats. Security is the primary objective of standard user authentication, with usability being treated as a secondary factor.

Most current authentication methods require user selection and instructions, necessitating an immediate need for appropriate security measures in IoT architectures [42] due to flaws in common authentication mechanisms.

1.1 Research Objectives

The main objective of this study is to design, implement, and evaluate an adaptive IoMT user authentication framework that adapts to contextual changes and user profiles for their authentication in a developing world setup, particularly in Sub-Saharan Africa (SSA). In particular, the following objectives have been achieved.

- Proposing a smartphone-based adaptive user authentication solution that uses machine learning to adapt to user profiles and make authorisation decisions on the IoMT device's end users.
- Develop a hybrid algorithm that incorporates feature and contextual weights in the Naive Bayes algorithm to cater for the conditional independence bias in login risk calculation.
- To evaluate the proposed smartphone-based adaptive user authentication framework that uses a hybrid algorithm for conformity to usability and security.

1.2 Research Questions

To contribute to improving usable security in user authentication in IoMT, we proposed to answer the following questions.

1. What user authentication technique can be implemented on IoMT devices that adapt to user profiles for the benefit of legitimate users?
2. What types of authentication methods balance usability and security, holding the potential to successfully balance the consequences of falsely allowing and denying access?
3. Does adaptive authentication of IoMT improve usable security in healthcare delivery?

This research focuses on the usability of user authentication techniques in IoMT devices, ensuring that patients and health workers can fully utilise the benefits of IoMT. These devices are often closed and not standardised or openly developed [43] and Dutta [44] suggests that users are the weakest link in security setups, who may fail to follow the rigour of security, and that usability is seen as a trade-off rather than a security-enhancing component in the cybersecurity industry. The authors further assert that a system's usability is only achieved when the user can use the mechanisms correctly and with minimal errors. This is because if a system is secure from a technical point of view, it is the end user who operates it and determines its usability, and e-health is human-centric, requiring it to meet human needs [30].

Therefore, more work needs to be done, and a monitoring solution is essential to protect the end-users [26][43][45]. This brings about the need for a thorough understanding of the users' sociotechnical issues for the development of more customised solutions [25][46]. Therefore, a study is needed to ensure the usability and security of user authentication, the first line of defence, to create user-centric IoT devices.

This research seeks to contribute to the academic body of knowledge on usable security by proposing an authentication solution that considers user profiles in determining the authentication mechanism to assign to them. Research on IoT user authentication worldwide has been extensive, but little has been done on its appropriateness for specific users, particularly the unique SSA user. The high number of untrained users [47], who perceive themselves as informed and prepared to use technology create a highly attractive environment for cybercriminals [48]. There are other issues, like high digital illiteracy [19][23], gender divide [1][49], perceived technological complexity and support [50], language [44], policy and regulation [6][51], cost of technology [19][52], as well as security and privacy [43][51] that are unique to Africa. The significant disparity between theoretical security and actual security in practice is often due to the poor usability of security solutions [26]. On the social side, diseases and other public health problems impose a heavy burden on SSA communities, and efforts are being made to use technology to ease the problems [26]. As a result, the usability of authentication is crucial for the IoMT's successful adoption in SSA's digital health, requiring local context, African needs, and decision-makers' endorsement to address individual barriers.

The issues discussed led to the development and evaluation of an adaptive user authentication model, specifically aimed at enhancing seamless authentication in developing

nations. This model considers the user's age, risk score, medical conditions, and available authenticators. The goal is to ensure secure access to medical IoT resources for all ages and medical conditions, thereby promoting technology adherence and achieving SDG 3.

This thesis has three main parts. In the first part, we designed a Machine Learning based adaptive user authentication framework that adapts to user profiles and context during login to determine the likelihood of the attempt being illegitimate before assigning appropriate authentication mechanisms. The proposed edge-centric framework fuses the Naive Bayes classifier and CoFRA model to determine the risk associated with a login attempt based on biometric wearable sensor data, non-biometric smartphone sensor data, and some predefined data. User backgrounds and preferences were solicited, and results showed that users, despite their ICTSkills, ages, jobs, and years of experience, prefer to use simple physiological biometrics for authentication. An Android App was then developed using the User-Centred Design and installed on a smartphone, which communicated with a PineTime smartwatch using Bluetooth. Sensor data was used as input in calculating the risk associated with an access request to decide whether to authenticate, step up authentication, or block a request using rule and role-based access control techniques while also non-intrusively monitoring health. Once implemented, the framework is expected to improve user experience in authentication, promoting the use of IoT in healthcare.

In the second part, we leveraged the Naive Bayes theorem for user authentication endeavours to assess the risk associated with login attempts. The Naive Bayes Machine Learning algorithm, along with its variations such as Gaussian, Categorical, and Bernoulli, was applied on both weighted and unweighted datasets to ascertain risk levels and categorise them into six classes. A majority of solutions categorise users into three classes, whereas adaptive authentication scenarios necessitate classification beyond this threshold. Additionally, the classification task was executed using alternative algorithms. The outcomes of cross-validation and comparative analyses revealed that the performance was commendable for up to three classes, after which a decrease was observed in certain Naive Bayes and SVM classifiers. Among the Naïve Bayes family, the BernoulliNB algorithm exhibited superior performance but was surpassed by Decision Trees, SVM, XGB, and Random Forests. Notably, the weighted dataset consistently outperformed the unweighted counterpart, with the allocation of weights significantly influencing algorithmic efficacy. The 80:20 split strategy yielded the most favourable outcomes in contrast to the 70:30

and 60:40 splits, albeit no significant variances were detected during cross-validation. Non-Naïve Bayes algorithms demonstrated superior performance compared to Naïve Bayes algorithms. For Naïve Bayes, optimal performance is achieved with three classes, highlighting its utility in conditional risk calculation, while non-Naïve Bayes multiclassification algorithms are more suitable for classification tasks due to the problem's inherent compatibility with conditional probabilities. In conclusion, it is imperative to acknowledge that the characteristics of the data, the use of weights, and the data splitting methodology significantly influence the accuracy of machine learning algorithms in multi-class user classification.

In the third section, we developed a Naive Bayes-based adaptive user authentication app that calculates the risk associated with a login attempt on an Android device for elderly users, using their health conditions, risk score, and available authenticators. This authentication technique, guided by the MAPE-K_{HMT} framework, makes use of embedded smartphone sensors. Knowledge-based and physiological biometrics were employed in the research, which constitutes static authentication. Results indicate 100% and 98.6% accuracy in usable security metrics, while cross-validation and normalisation results also support the accuracy, efficiency, effectiveness, and usability of our model, with room for scaling it up without computational costs and generalising it beyond SSA. The post-deployment evaluation also confirms that users found the app usable and secure. A few areas need further refinement to improve the accuracy, usability, security, and acceptance, but the model shows potential to improve users' compliance with IoMT security, thereby promoting the attainment of SDG3.

We also performed an evaluation on young users using continuous authentication. This research focuses on enhancing the security and usability of IoMT for young users through a robust, adaptive, continuous authentication model using physiological biometrics on Android devices and heart rate data from smartwatches. By integrating user behaviour, environmental context, and health conditions, the model dynamically determines risk, trust, and authorisation decisions. Machine learning techniques analyse data related to devices, networks, locations, and user habits while considering demographics like age and medical conditions to assign suitable authenticators. The model balances accuracy and usability, favouring correct positive predictions, but faces limitations such as class imbalance, feature selection, and overfitting, with a false rejection rate (FRR) of 19%. Behavioural biometrics, personalised authentication, and continuous authentication

enhance security and accessibility. However, moderate sensitivity affects its ability to capture all positive cases. Age-group analysis reveals varying engagement with technology, emphasising tailored authentication flows. This research demonstrates the potential of risk-based adaptive authentication to deliver secure, user-friendly solutions in complex healthcare environments.

The rest of this introduction is organised as follows. Section 2 provides the literature review for the study, while the methodology is presented in section 3, with an overall conclusion in section 4 and recommendations and future works discussed in section 5.

This page has been intentionally left blank

2 Literature Review

2.0 Introduction

This section provides an overview of the IoT and its uses. It then focuses on IoT in healthcare, paying special emphasis to user authentication. The study focuses on the usability of user authentication systems to achieve a balance between usability and security.

2.1 An Overview of IoT

IETF [53] and ITU-T [54] define IoT as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information communication technologies (ICT)”. It depicts a network of real-world objects, or "things," that are equipped with sensors, software, and other technologies to gather and share data with other systems and devices online [55]. In essence, it involves bringing everyday objects online so they may interact and communicate in ways that were previously unthinkable.

IoT has grown at an exponential rate. In just a few years, the number of connected devices has increased from billions to tens of billions, driven by developments in wireless communication, low-power sensors, and cloud computing [56]. The global IoMT market was valued at $USD 230.69 billion in 2024 and is expected to increase at a CAGR of 18.2% from 2025 to 2030 [15]. This rapid expansion continues as technology becomes more affordable and its applications become increasingly diverse, impacting everything from smart homes and wearable technology to industrial automation and smart cities. IoT is the future of the internet and an integrated part of the modern person‘s daily life [57][58]. Figure 4 shows the projected growth of IoT with the major market players and the market trends.

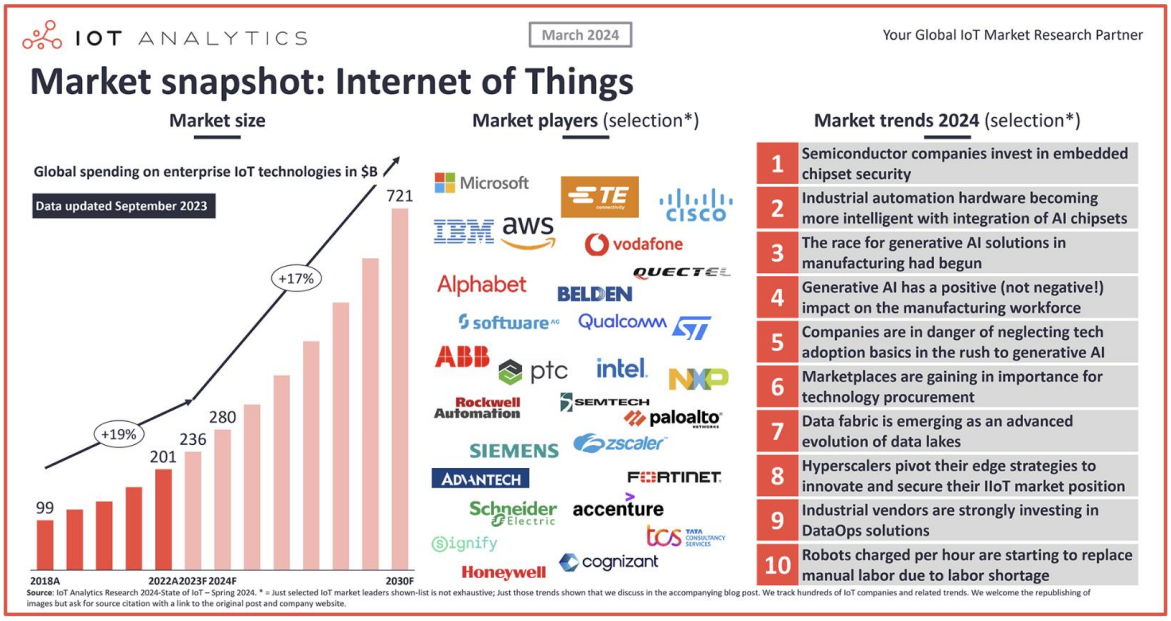


Figure 4: Projected growth of IoT. Source [56]

2.1.1 Attributes of IoT

The capabilities and impact of IoT are defined by several essential features:

1. Connectivity: This is the essential feature that allows "things" to connect to other devices and the internet. Numerous protocols, including cellular networks, Bluetooth, Wi-Fi, and others, can be used to provide this connectivity [58][59]. Remote control and smooth data exchange are made possible by it.

2. Sensing: Sensors on IoT devices can detect and measure changes in their surroundings. These sensors transform physical phenomena into digital signals by collecting a variety of data signals, such as temperature, humidity, motion, light, and pressure [60][61].

3. Intelligence: A certain degree of intelligence is frequently present in IoT devices, allowing them to interpret data locally or on the cloud and make decisions using machine learning algorithms or predefined rules. Autonomous operation and automation are made possible by this.

4. Data Collection and Analysis: A core aspect of IoT is the ability to collect immense amounts of data from connected devices. This data is then transmitted to the cloud or local servers for processing, analysis, and extraction of valuable insights.

5. Dynamic and Self-Adapting: IoT devices can frequently dynamically adjust to changing user demands or environmental conditions. They may optimise their performance by learning from data, updating software, and reconfiguring themselves [62][63].

6. Interoperability: Devices made by various manufacturers and utilising various communication protocols ought to be able to interact and cooperate without any problems in an IoT ecosystem. Interoperability makes it possible for various devices to communicate and work together efficiently [64][65].

7. Unique Identity: In order to be recognised and addressed within the network, every IoT device usually has a unique identification (such as a MAC address or IP address). This is essential for management and communication.

8. Scalability: Because IoT systems are scalable, they can support a large number of devices and manage growing data volumes without experiencing performance issues. For IoT implementations to expand and spread, this is essential.

9. Security: Security is a crucial feature as IoT devices gather and send sensitive data. To safeguard devices and data from online dangers, measures like access control, authentication, and encryption are crucial.

10. Autonomous Operation: Numerous IoT devices are made to function autonomously, carrying out operations and reaching conclusions without constant human intervention. Efficiency and convenience are improved by this automation.

Together, these qualities allow the IoT to bridge the gap between the digital and physical worlds, opening up a plethora of applications and revolutionising a number of facets of our lives and businesses.

2.1.2 IoT Architecture

The structured framework known as the IoT architecture makes it easier for different parts of the IoT ecosystem to integrate and interact. It has several layers, each of which performs specific tasks that improve system performance and user experience. The main layers and their functions are described below.

Perception Layer: This basic layer includes sensors and actuators that gather environmental data. It is essential for the initial data collection procedure [66].

Network Layer: Responsible for data transmission, it ensures seamless communication between devices, the cloud, or other systems employing various protocols to effectively manage data flow [66][67].

Middleware Layer: Also called the Data processing layer, it processes the data collected, providing essential services such as data storage, integration, and management. It ensures interoperability among diverse devices [67].

Application Layer: The topmost layer delivers specific applications and services to end-users, tailored to various industries such as healthcare, smart cities, and more [66]. Having understood the general IoT layers, we will now look at the IoT security architecture. Figure 5 illustrates the IoT architecture.

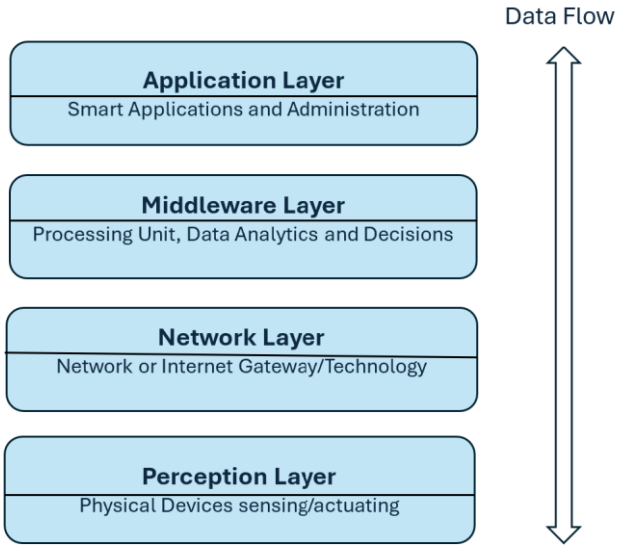


Figure 5 : IoT Architecture

2.1.3 IoT Security Architecture

IoT is rapidly increasing, connecting a wide range of devices, and generating massive volumes of data. However, this interconnectedness creates significant security challenges and designing a strong security architecture is critical for protecting IoT systems from a variety of attacks. This section looks at the IoT security architecture, including major principles, difficulties, and possible solutions.

The IoT security architecture is a multidimensional framework for safeguarding devices, networks, and cloud environments from various cyber threats. This design focuses on a holistic strategy that incorporates security measures at different levels, ensuring strong protection against developing vulnerabilities. The key components of this architecture are the Multi-Layer Security Framework,

Adaptive Architecture and Integration of Advanced Technologies. The adaptive architecture (AA) consists of the Holistic Security Measures [68] and the Continuous Risk Assessment [69] while the Integration of Advanced Technologies encompasses Machine Learning and Blockchain [70] and Operational Supervision [71]. We will describe the Multi-Layer Security Framework, whose layers are described below.

- *Perception Layer Security:* Focuses on safeguarding IoT devices via authentication, access control, and secure firmware updates [71].
- *Network Layer Security:* Uses secure communication technologies such as TLS and DTLS to safeguard data in transit [69].
- *Processing Layer Security:* Uses real-time monitoring and anomaly detection to identify and mitigate risks [70].
- *Application Security:* Ensures that applications communicating with IoT devices are secure and conform to standards [71].

All these frameworks try to capture security measures at various levels, including devices, networks, data, users, and the cloud. While the proposed frameworks provide a strong foundation for IoT security, issues remain in standardisation and interoperability, resource constraints, scalability, and the rapid evolution of threats, necessitating continual adaptation and innovation in security policies.

2.2 Applications of IoT

IoT has rapidly progressed from a theoretical concept to a transformative technology with a wide range of practical applications. It connects physical devices to the internet, allowing data to be collected, exchanged, and analysed, promoting innovation and efficiency across industries. IoT is revolutionising several industries by allowing for seamless connectivity and data exchange between devices. We will now delve into some of the most important applications of IoT, emphasising its impact on numerous businesses and facets of daily life.

Smart Homes: IoT allows for the automation and control of household appliances, lights, and security systems, increasing convenience, comfort, and energy efficiency. For example, smart thermostats may automatically alter temperatures based on occupancy and weather conditions, and smart lighting systems can be controlled remotely [72].

Healthcare: IoT is transforming healthcare through remote patient monitoring, wearable devices, and smart sensors. These technologies provide continuous health monitoring, personalised therapy, and improved disease management. Wearable sensors can monitor vital signs, sleep patterns, and detect irregularities, allowing for timely interventions [73].

Smart Cities: In smart cities IoT is critical to their development because it enables effective management of resources, infrastructure, and public services. Applications include intelligent traffic management, trash management, and environmental monitoring. Smart streetlights, for example, may alter their brightness depending on traffic and pedestrian activities, lowering energy use [74].

Industrial IoT (IIoT): In the industrial sector, IoT is used to improve efficiency, productivity, and safety through machine monitoring, predictive maintenance, and automation. Sensors deployed in factories can track equipment performance, detect potential failures, and optimise production processes [75].

Agriculture: Precision farming, which uses sensors, drones, and data analytics to optimise crop management, is revolutionising agriculture thanks to IoT. IoT devices monitor soil conditions, weather patterns, and crop health, allowing farmers to make informed decisions about irrigation, fertilisation, and insect management [76].

Transportation: IoT enhances transportation systems through connected vehicles, smart traffic management, and supply chain optimisation. Connected vehicles can connect with one another and with infrastructure, thereby enhancing traffic flow and safety. IoT sensors may also track the location and condition of items in transit, which improve supply chain visibility [77][78].

These applications are graphically depicted in Figure 6.

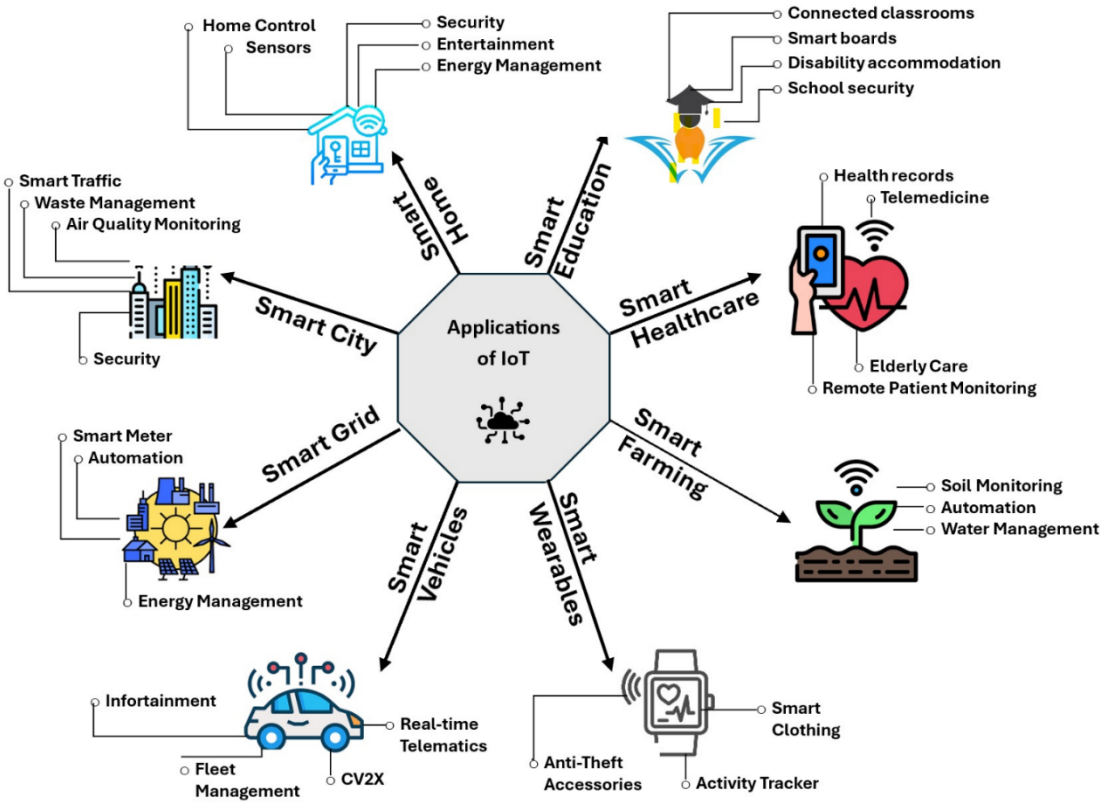


Figure 6 : Applications of IoT. Modified from [74]

2.2.1 IoT in health

IoT is revolutionising healthcare through remote patient monitoring, wearable devices, and smart sensors. These technologies provide continuous health monitoring, personalised therapy and improved disease management. Wearable sensors can monitor vital signs and detect anomalies, allowing for early interventions [73]. IoT devices and applications are transforming healthcare by improving patient care, increasing efficiency, and reducing costs. Some of the key applications in healthcare include:

Remote Patient Monitoring: IoT devices make it possible for patients to continuously monitor their health and vital signs from the comfort of their own homes, which minimises the need for hospital visits and allows for timely interventions [85-87].

Wearable Devices: Wearable sensors, such as smartwatches and fitness trackers, collect health data, including heart rate, activity levels, and sleep patterns. This data can be used to provide personalised health insights and support preventive care [79][80].

Chronic Disease Management: Diabetes, asthma, and heart disease are among the chronic ailments that IoT can assist in managing. Smart glucose monitors and insulin pens, for instance, can assist patients in better managing their diabetes [80][81].

Smart Hospitals: IoT is used in hospitals to improve operations, such as asset tracking, patient flow management, and medication management. This can lead to increased efficiency and improved patient safety [79][81].

Thus, the benefits of IoT in healthcare can be summed up as follows: enhanced patient monitoring through continuous monitoring, personalised care, and timely interventions, which improves patient outcomes; increased efficiency through automated tasks, reducing manual errors, and streamlining processes; improved provider efficiency; decreased costs through fewer emergency room visits and hospitalisations, which lowers healthcare costs; and finally, improved accessibility to healthcare for patients in underserved or remote areas.

2.2.2 The need for IoT in Health

IoMT is a system of hardware and software that aids in treating and preventing illnesses both within and outside of traditional patient care settings [82]. Its adoption is now seen as one of the most attractive areas of application for IoTs [83]. IoMT expansion in SSA is driven by factors like the aged population [84] which is 3.06 % of SSA's population [85], chronic diseases that are killing 15 million people per year in low to middle-income countries [86], healthcare specialists' shortages [87], rising medical care costs [10], and COVID-19 [88]. Experts predict that most of the billions of linked objects will be medical devices that include personal exercise equipment, mobile medical workstations, pacemakers, infusion pumps, and in-home monitoring [89]. Despite the small number of IoMT-using nations in SSA, Rwanda is utilising IoT to improve healthcare services, such as ZipLine-drone-assisted blood transport, Jembi-Rwanda Health Information Exchange (RHIE), human-sized robots for vital sign checks and compliance reinforcement, Babyl Rwanda-medical consultations for anyone with a mobile device, IntraHealth International-a decentralised health care system, and TeleMedicine-a medical student-run hospital in Rwanda [10][90]. These initiatives aim to improve patient care, reduce costs, and enhance patient experience. Therefore, IoT can be used to complement medical staff in preventing and managing diseases.

But using IoT in healthcare also has drawbacks, which can be summed up as follows: interoperability issues, where a lack of standardisation can make it difficult to integrate data from various IoT devices and systems [91]; device reliability, where the accuracy and dependability of IoT devices can vary, which may affect the quality of healthcare decisions [92] and implementation costs. Putting IoT ideas into practice in the healthcare industry can be costly and necessitate large expenditures in technology and infrastructure [93].

2.2.3 Need for Security in IoT Healthcare Applications

The collection and transmission of sensitive patient data raises concerns about security breaches when it comes to the use of electronic devices. Therefore, the security of IoT devices and the data they produce is crucial. Security breaches may result in serious repercussions [79][80][81][94], such as:

Compromised Patient Data: Unauthorised access to patient data can lead to privacy violations, identity theft, and discrimination.

Device Tampering: Malicious people can tamper with medical devices, leading to incorrect readings, misdiagnosis, or even harm to patients.

Disrupted Healthcare Services: Cyberattacks on healthcare systems can disrupt critical services, such as medication delivery and patient monitoring, thereby endangering lives.

Legal and Regulatory Implications: Healthcare organisations must comply with strict regulations, such as HIPAA, which mandate the protection of patient data.

IoMT has transformed healthcare by connecting medical devices and systems, allowing for remote patient monitoring, personalised therapy, and effective healthcare management. However, this interconnection creates substantial security risks, compelling the use of strong authentication procedures. Authentication in IoMT is used to validate the identification of devices, users, and systems, ensuring that only authorised personnel have access to sensitive medical data and vital resources.

Several studies have focused on the unique issues of IoMT authentication, but IoMT devices are frequently resource-constrained, with limited computing power, memory, and energy, rendering typical authentication methods ineffective [95]. Furthermore, the diverse nature of IoMT devices and the variety of communication protocols create a difficult security environment [96]. To solve these issues, researchers investigated a variety of authentication systems. A survey conducted by

Alsaeed and Nadeem [97] classified IoMT authentication solutions based on various factors, including architecture (centralised vs. distributed), authentication level (device, user, network), and scheme type (basic, key-based, certificate-based, cryptography-based). The study found a tendency towards distributed architectures, as well as an increase in the adoption of hybrid cryptographic approaches to improve security and performance. Another study by Aslam *et al.*[98] emphasised the significance of authentication in safeguarding patient information and preventing unauthorised access to IoMT resources. It addressed the issues of implementing strict authentication algorithms in IoMT, such as resource limitations, different platforms and protocols, and the distributed nature of IoMT systems.

To solve IoMT devices' resource limitations, researchers devised lightweight authentication mechanisms. These protocols seek to reduce computing overhead and communication costs while ensuring a high level of security. For example, some research has looked into the usage of elliptic curve cryptography (ECC) and physically unclonable functions (PUFs) for lightweight authentication in IoMT [99]. The necessity for safe and efficient authentication in IoMT is well understood. As the IoMT evolves, continuing research is required to build strong authentication techniques capable of protecting sensitive medical data while ensuring the security and reliability of IoMT systems.

Therefore, while IoT offers significant potential to improve healthcare, it also introduces substantial security risks. Robust security measures are therefore essential to protect patient data, ensure device reliability, and maintain the integrity of healthcare systems.

2.4 Usability of Security Solutions: User Authentication

Security solutions, particularly those that need user authentication, are frequently viewed as impeding usability. Strong authentication systems, while necessary for securing sensitive data, can result in complex and time-consuming procedures, causing user irritation and lower productivity, with users circumventing security protocols or abandoning services altogether [100]. This section examines the challenges and considerations surrounding the usability of user authentication methods. Furnell and Clarke [101] conduct an investigation on the inherent tradeoff between usability and security in authentication methods. The authors discuss how the requirement for strong security measures frequently conflicts with users' needs for convenience and efficiency.

They emphasise the significance of striking a balance between these two competing variables to achieve both effective security and user satisfaction.

Yan *et-al.* [102] investigate the usability of various user authentication methods for mobile phones. The study examines the advantages and disadvantages of standard password-based authentication, as well as alternative approaches, including biometric authentication and graphical passwords. The findings demonstrate how different authentication techniques affect user experience, task completion time, and error rates.

Das *et-al.* [103] investigate the low acceptance rate of multi-factor authentication (MFA) among users, despite its potential to improve security against cyber threats, notably in the workplace. The study looks into users' mental models, risk perceptions, and difficulties with MFA use, and finds that while professionals recognise its benefits, non-experts frequently regard it as unnecessary work. The findings underscore the importance of increased risk communication from service providers in raising user awareness and knowledge of MFA.

Wahid [104] investigates the factors influencing smartphone owners' acceptance of biometric authentication methods by developing a new model based on the Technology Acceptance Model (TAM). They discover that the perceived usefulness of a biometric authentication method on smartphones outweighs its perceived ease of use, implying that the user's belief in the intrinsic value of biometric authentication methods in the form of perceived security outweighs both the internal user motivation of perceived enjoyment and the external user motivation of social influence in terms of acceptance of biometric authentication methods.

Zimmermann *et-al.* [105] conducted an in-depth analysis of user perceptions of the password, fingerprint, and a smartphone-based scheme in an online study, and revealed how perceptions of usability, security, privacy, trust, effort, and qualitative features of the schemes are related to user preferences.

Pilson [106] focuses on a typology of authentication systems based on security and cognitive complexity, emphasising the importance of striking a balance between security and user needs. The authors argue that when creating authentication systems, it is important to include the human factor.

Oluwafemi and Feng [107] study the balance between security and usability in authentication techniques, emphasising the significance of letting users select their preferred authentication method. The study discovers that, while users appreciate security, they frequently choose one-

factor authentication due to its simplicity, indicating a complex link between user preferences and security perception.

Gupta *et-al.* [108] emphasise the importance of usability in authentication procedures, implying that user acceptability is impacted by how well these systems correspond to users' knowledge. The authors propose building accessible authentication methods that improve security while considering user perceptions, which is critical for effective deployment and user satisfaction in smartphone security measures.

Therefore, the usability of user authentication methods is a critical factor in the widespread adoption and effectiveness of security solutions. Researchers continue to explore new approaches and technologies that can enhance both security and usability, aiming to create authentication systems that are both robust and user-friendly.

2.5 IoMT User Authentication

In the IoMT, user authentication is the process of validating the identity of individuals (e.g., patients, healthcare providers) who utilise IoMT systems or data [5]. This is an important security feature that protects sensitive medical information and ensures that only authorised individuals can access and manage patient data and medical devices. Reasons for user authentication include :

- **Data Confidentiality**: IoMT systems handle extremely sensitive patient data, such as medical history, treatment plans, and real-time health information. User authentication guarantees that only authorised individuals have access to this data, hence ensuring patient privacy[109][110].
- **Data Integrity:** Authentication helps to protect the integrity of medical data by guaranteeing that only authorised users can edit or update it. This avoids unauthorised changes, which could lead to a misdiagnosis or inappropriate treatment [111].
- **System Security:** User authentication is critical for safeguarding IoMT systems against unauthorised access, which could result in disruptions in healthcare services, device tampering, or denial-of-service assaults [109][112].
- **Regulatory Compliance:** Healthcare organisations must follow standards such as HIPAA, which require tight access controls and authentication mechanisms to secure patient data [110][112].

However, user authentication has several challenges associated with its implementation [120-122]. Some of the challenges include:

- **Diverse User Requirements:** IoMT systems involve a diverse set of users with various access requirements and technical skills, including doctors, nurses, patients, and carers. Creating a one-size-fits-all authentication system is therefore difficult.
- **Usability:** To ensure that healthcare workflows are not disrupted, authentication techniques should be simple and efficient. Complex or time-consuming authentication procedures might cause user frustration and noncompliance [5][44][113].
- **Device Limitations:** Some IoMT devices, such as wearable sensors, may have limited processing power and input capabilities, making it challenging to implement complex authentication schemes [95][124-126].
- **Security Vulnerabilities:** IoMT systems are exposed to a vast array of security risks, including phishing attempts, password theft, and insider threats. Authentication measures must be strong enough to withstand such attacks [43][114][115].

To improve security in healthcare systems, the authors of [116] suggested a safe Lightweight Authentication Scheme (LAS) for IoMT-based healthcare systems. The suggested approach outperformed prior lightweight schemes and permitted peer-to-peer communication without central intervention during the authentication and communication stages, but it did require device registration and central authority permission. But only the scheme's technical aspects were assessed.

In order to enhance security and user experience during the COVID-19 pandemic, a graphical password-based user authentication mechanism for the IoMT was proposed in [117]. Using the Post-Study System Usability Questionnaire (PSSUQ) instrument, the suggested scheme, which was implemented via an Android application, was evaluated for system, information, and interface quality, showing promise for improving user authentication experiences in the healthcare industry.

The hash function and XOR operation were utilised for operating in low-spec healthcare IoT sensors, similarly by Kim *et al.* [118] who presented an enhanced lightweight user authentication strategy for the IoMT. Although the suggested plan did not include smartphone sensors, it performed better and was more secure than existing protocols.

Farhan *et al.* [119] suggested using decentralised identities (DIDs) and verifiable credentials (VCs) in conjunction with an OAuth-based authorisation framework to safeguard the confidentiality of patient data on IoT devices. The suggested framework simplified the administration of access control by highlighting improved privacy and security via a smart pill dispenser. However, the effort mostly concentrated on the model's technical aspects rather than its user aspects. In order to improve security, scalability, and efficacy in patient care, a study by Bali and Yenkikar [120] proposed a multi-factor authentication method for IoT-based Wireless Medical Sensor Networks. Smartphones were not included in the proposed system, despite the fact that they offered improved functioning and defence against frequent attacks.

The use of Artificial Intelligence (AI) to enhance the authentication of IoMT users through the design of a framework using bioelectrical signals for authentication and AI with contextual data was proposed in [121]. The framework enhanced security in healthcare, maintained user trust and data integrity, balanced usability and security, and was adaptable to various devices. Their work, however, was restricted only to bioelectrical signals.

In Kumar *et al.* [122], a biometric-based authentication system was suggested for hospital settings where patients engaged with smart environments without the use of specific devices. Although the effort focused on general security and did not specifically address the needs of all age groups of users, particularly the elderly, the method was able to withstand several well-known attacks, demonstrating the importance of biometric keys for identification and authentication.

In Sharma and Singh [123], a novel, robust, and low-complexity remote user authentication system for IoT-enabled healthcare applications was introduced. The scheme's security and suitability for use in actual healthcare applications were established through thorough verification.

In contrast, a taxonomy of threats and an investigation of authentication methods for IoT-enabled healthcare systems at various network levels were carried out in [124]. The work focused on user and device verification. Bayesian probability in Context-Aware Scalable Authentication (CASA) was developed by Hayashi *et al.* [125] for adaptive authentication. It selected active authentication techniques based on location contexts and passive variables, and it locked the screen using a password and PIN. The model served as the basis for contemporary adaptive authentication, even though it reduced usability.

Choose Your Own Authenticator (CYOA), which was proposed by Forget *et al.* [126], gives users the option to select their authentication system according to their preferences, skills, and usage environment. However, it limits flexibility and introduces delays, particularly for older users.

In Wójtowicz and Chmielewski [127], a smartphone adaptation was developed that modified lock functionality between fingerprint, facial scan, and vocal sound recognition based on usability; however, because of its emphasis on usability, security was disregarded.

Previous researchers have explored various authentication methods for IoMT users, including:

- **Password-based authentication:** Traditional techniques rely on usernames and passwords, but they are vulnerable to phishing and brute force attacks.
- **Multi-factor authentication (MFA):** Combines several authentication elements, such as passwords, smart cards, and biometrics, to boost security [128][129].
- **Biometric authentication:** Uses unique biological traits, such as fingerprints, facial recognition, or iris scans, to verify user identity [117][128][130][131].
- **Role-based access control (RBAC):** Restricts system access based on the user's role within the healthcare organisation [98].

2.5.1 Challenges with Current IoMT User Authentication Techniques

Current IoMT user authentication techniques face several challenges, requiring a gentle balance between security and usability. These challenges include:

1. **Resource Constraints of IoMT Devices:** Several IoMT devices, including implantable and wearable sensors, are low-power devices with constrained memory, computing capability, and battery life. Therefore, implementing multi-factor authentication (MFA) systems and complex cryptographic algorithms that require a lot of processing power and storage are difficult [36].
2. **Vulnerability to Traditional Attacks:** Since security was not a top priority while designing many IoMT devices, they are vulnerable to frequent cyberattacks, such as:
    - **Weak Authentication Methods:** Using default credentials or passwords that are simple to guess [132].

- **Offline Password Guessing:** Without setting off alerts, attackers can attempt to guess passwords offline and steal device data.
- **Man-in-the-Middle (MITM) Attacks:** Communication between users and devices being intercepted [133].
- **Impersonation Attacks:** Malicious actors may attempt to imitate trustworthy users or gadgets [134].
- **Replay Attacks:** Sending valid data transmissions again to obtain unauthorised access [135].

3. **Diversity and Heterogeneity of Devices and Protocols:** With a wide range of devices from several manufacturers utilising different platforms, operating systems, and communication protocols, the IoMT ecosystem is quite diversified. Creating a rigorous and globally compatible authentication system in this diverse setting is a challenge [37].
4. **Lack of regular updates and patches:** Some medical equipment has long operational lifespans that frequently extend beyond the operating system's support lifecycle, resulting in out-of-date software with known vulnerabilities that are difficult to fix [38].
5. **Insider Threats:** Malicious insider acts or configuration errors inside the healthcare organisation might also result in unauthorised access.
6. **Data Sensitivity:** Sensitive patient health information (PHI) is handled by IoMT devices. Data breaches, privacy violations, and even direct patient injury (such as an insulin pump that has been compromised and is giving out the wrong dosages) can result from any compromise of authentication [40][41].
7. **Distributed and Remote Nature:** IoMT systems often operate in distributed and remote environments, making it more difficult to physically secure devices and monitor access [39].

2.5.2 The Need for a Balance Between Usability and Security

It is crucial to have strong security in IoMT without compromising usability. Overly complicated authentication processes can impede timely patient care, resulting in mistakes, delays, and frustration for medical staff or patients.

Usability can be measured in terms of the following:

- **Efficiency:** Particularly during emergencies, healthcare personnel require easy and quick access to patient data and device controls. Important medical interventions may be hampered by laborious authentication procedures [136].
- **Simplicity:** A diverse range of people, some of whom might not be tech-savvy, frequently utilise IoMT devices. Methods of authentication ought to be simple and intuitive.
- **Accessibility:** Users with disabilities or those operating in demanding situations should not encounter obstacles as a result of authentication.

At the same time, the following considerations are necessary for security.

- **Data Confidentiality and Integrity:** Patient data must be protected from unauthorised access, alteration, or destruction.
- **Device and Data Integrity and Availability:** For patient safety, it is essential to make sure that devices operate as intended and are immune to denial-of-service attacks and hijacking [137].
- **Regulatory Compliance:** Strict adherence to healthcare laws such as GDPR and HIPAA necessitates strong authentication and other security measures [138].

To strike a balance between usability and security, an ideal authentication scheme should :

- **Employ Multi-Factor Authentication (MFA):** Security is greatly increased by combining at least two distinct authentication mechanisms (such as knowledge-based and biometric) [139].
- **Utilise Biometric Authentication:** For devices with limited resources, fingerprint, facial recognition, or even electrocardiogram (ECG) biometrics can provide a robust, yet reasonably easy, authentication technique that lessens the need for conventional passwords.
- **Implement Lightweight Cryptography:** For devices with limited processing power, lightweight cryptographic methods can provide a balance between security strength and computational overhead [140].
- **Enforce Strong Password Policies (where applicable):** Remove the default login information and require the usage of strong, one-of-a-kind passwords.
- **Leverage Centralised Identity and Access Management (IAM):** Security may be improved and administration made easier with a single system for controlling user identities and access rights throughout the IoMT ecosystem [141].

- **Adopt Zero Trust Principles:** Even inside the network perimeter, assume that no user or device is intrinsically dependable. It is crucial to continuously verify access and identification.
- **Regular Security Audits and Vulnerability Assessments:** It is essential to proactively identify and fix security flaws.
- **Embrace Context-Aware Authentication:** Depending on the role of the user, the location, the time of day, and the sensitivity of the data being accessed, authentication can be dynamically changed. For instance, a doctor writing a prescription might need more rigorous authentication than a nurse accessing a patient's vital signs.

The characteristics of medical devices and the sensitive nature of healthcare data make securing IoMT user authentication a challenge. To guarantee patient safety and efficient healthcare delivery, it is crucial to provide cutting-edge authentication solutions that are robust enough to resist complex cyberattacks while being user-friendly and effective for the intended users [97]. A potentially feasible solution that can be both usable and secure is adaptive authentication.

2.6 Adaptive User Authentication

Adaptive user authentication (AUA) is a potential solution for improving security and usability in IoMT systems. Adaptive security is a self-monitoring security method that prevents network attacks by altering its behaviour and controlling the conditions under observation [142] reducing the monotonous selection of the same authentication factors and identifying risks more effectively than the one-size-fits-all approach [143]. Adaptive user authentication techniques that can be implemented in the IoMT environment include:

- **Behavioural Biometrics:** AUA can integrate behavioural biometrics, such as typing patterns, mouse movements, and gait analysis, to continually monitor user behaviour and detect anomalies that could indicate a security breach [144][145] .
- **Context-Aware Authentication:** AUA can leverage contextual information, such as the user's location, time of access, and device type, to assess the risk level. For example, accessing sensitive data from an unusual location or device may trigger stronger authentication measures.
- **Risk-Based Authentication:** AUA can provide a risk score to each access attempt based on a variety of criteria, including the sensitivity of the data being accessed and the user's

previous behaviour. High-risk access attempts may necessitate additional authentication measures [146].

- **Continuous Authentication:** AUA can continuously verify the user's identity throughout the session, rather than just at the initial login. This can help detect compromised accounts or insider threats [155-157].
- **Machine Learning:** Machine learning algorithms can be used to analyse user behaviour patterns and identify deviations that may indicate malicious activity [121].

While user authentication is crucial, it is also important to strike a balance between security and usability. Overly complex authentication systems may impede healthcare personnel's ability to access critical data quickly, thus jeopardising patient care. Adaptive user authentication allows IoMT systems to provide a more secure and user-friendly experience, protecting sensitive medical data while minimising disturbance to healthcare procedures. In conclusion, there is no universally applicable solution for IoMT security, and thus, the various authentication mechanisms can be used in conjunction to improve security at the elderly users' convenience [147].

This page has been intentionally left blank

3 Methodology

3.0 Introduction

This research proposes a machine learning-based adaptive user authentication framework that adapts to user profiles and context during login, determining illegitimacy likelihood before assigning appropriate authentication mechanisms. A mixed approach was employed, which made use of both qualitative and quantitative data. Each part of this research study constitutes objectives and contributes to the achievement of the research objectives.

Part 1 of the study proposes the architectural design of a Machine Learning-based adaptive user authentication framework for the IoMT. The proposed edge-centric framework fuses the Naive Bayes classifier and CoFRA model to determine the risk associated with a login attempt based on biometric wearable sensor data, non-biometric smartphone sensor data, and some predefined data. User backgrounds and preferences were solicited, and results showed that users, regardless of their ICT skills, ages, jobs, and years of experience, prefer to use simple physiological biometrics for authentication. An Android App was then developed using the User-Centred Design and installed on a smartphone, which communicated with a PineTime smartwatch using Bluetooth low-energy (BLE). Sensor data was used as input in calculating the risk associated with an access request to decide whether to authenticate, step up authentication, or block a request using rule and role-based access control techniques while also non-intrusively monitoring health. Analysis shows that the framework is expected to improve user experience in authentication, promoting the use of IoT in healthcare.

In Part II, we leveraged the Naive Bayes theorem for user authentication endeavours to assess the risk associated with login attempts. The Naive Bayes Machine Learning algorithm, along with its variations such as Gaussian, Categorical, and Bernoulli, was applied on both weighted and unweighted datasets to ascertain risk levels and categorise them into six classes. A majority of solutions categorise users into three classes, whereas adaptive authentication scenarios necessitate classification beyond this threshold. Additionally, the classification task was executed using alternative algorithms. The outcomes of cross-validation and comparative analyses revealed that the performance was commendable for up to three classes, after which a decrease was observed in certain Naive Bayes and SVM classifiers. Among the Naïve Bayes family, the BernoulliNB algorithm exhibited superior performance but was surpassed by Decision Trees, SVM, XGB, and

Random Forests. Notably, the weighted dataset consistently outperformed the unweighted counterpart, with the allocation of weights significantly influencing algorithmic efficacy. The 80:20 split strategy yielded the most favourable outcomes in contrast to the 70:30 and 60:40 splits, albeit no significant variances were detected during cross-validation. Non-Naïve Bayes algorithms demonstrated superior performance compared to Naïve Bayes algorithms. For Naïve Bayes, optimal performance is achieved with three classes, highlighting its utility in conditional risk calculation, while non-Naïve Bayes multiclassification algorithms are more suitable for classification tasks due to the problem's inherent compatibility with conditional probabilities. In conclusion, it is imperative to acknowledge that the characteristics of the data, the use of weights, and the data splitting methodology significantly influence the accuracy of machine learning algorithms in multi-class user classification.

In Part III-A, we developed a Naive Bayes-based adaptive user authentication app that calculates the risk associated with a login attempt on an Android device for elderly users, using their health conditions, risk score, and available authenticators. This authentication technique, guided by the MAPE-K_{HMT} framework, makes use of embedded smartphone sensors. Knowledge-based and physiological biometrics were employed in the research, which constitutes static authentication. Results indicate 100% and 98.6% accuracy in usable security metrics, while cross-validation and normalisation results also support the accuracy, efficiency, effectiveness, and usability of our model, with room for scaling it up without computational costs and generalising it beyond SSA. The post-deployment evaluation also confirms that users found the app usable and secure. A few areas need further refinement to improve the accuracy, usability, security, and acceptance, but the model shows potential to improve users' compliance with IoMT security, thereby promoting the attainment of SDG3.

In Part III-B, we performed an evaluation on young users using continuous authentication to protect users and devices against attacks that occur after initial login. This research focuses on enhancing the security and usability of IoMT for young users through a robust, adaptive, continuous authentication model using physiological biometrics on Android devices and heart rate data from smartwatches. By integrating user behaviour, environmental context, and health conditions, the model dynamically determines risk, trust, and authorisation decisions. Machine learning techniques analyse data related to devices, networks, locations, and user habits while considering demographics like age and medical conditions to assign suitable authenticators.

The model balances accuracy and usability, favouring correct positive predictions, but faces limitations such as class imbalance, feature selection, and overfitting, with a false rejection rate (FRR) of 19%. Behavioural biometrics, personalised authentication, and continuous authentication enhance security and accessibility. However, moderate sensitivity affects its ability to capture all positive cases. Age-group analysis reveals varying engagement with technology, emphasising tailored authentication flows. This research demonstrates the potential of risk-based adaptive authentication to deliver secure, user-friendly solutions in complex healthcare environments.

3.1 Objectives and Research Strategy

Various strategies were employed to fulfil each research objective and are summarised in Table 1.

Table 1: Research Strategies

S/No.	Research Objective	Research Method used	How the Research Method was used
1	Proposing a smartphone-based adaptive user authentication solution that uses machine learning to adapt to user profiles and make authorisation decisions on IoMT devices' end users.	Designed an adaptive user authentication model for IoMT users using the User-Centred Design Approach	Used modelling tools to design and simulate an adaptive user authentication model guided by user requirements. This was presented in the paper: User-centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones.
2	Develop a hybrid algorithm that incorporates feature and contextual weights in the Naïve Bayes algorithm to cater for the conditional	Designed and deployed a Naïve Bayes-based adaptive user authentication prototype for	Deployed an Android-based adaptive user authentication prototype for patients and medical staff, which performed static and dynamic authentication. This was presented in the papers:

	independence bias in login risk calculation.	patients and medical staff.	1) User-centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones. 2) Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication.
3	To evaluate the proposed smartphone-based adaptive user authentication framework that uses a hybrid algorithm for conformity to usability and security.	Evaluated the prototype from a user and security perspective.	Used post-deployment evaluation to evaluate the prototype with users for conformity to usability and security during user authentication. This was presented in the paper: 1) An Android-Based Internet of Medical Things Adaptive User Authentication and Authorisation Model For The Elderly. 2) Naive Bayes-Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users.

3.2 Conceptual Model

The conceptual model used in this research is the SHELL model, modified by Hawkins [148] in 1975, from SHEL developed by Edwards in 1972. It is an acronym for Software, Hardware, Environment, Liveware (Self), with additional Liveware (Others). It explains the relationship between human factors and aviation system resources and environment, focusing on security issues related to these components [149]. It was chosen in this research because it systematically addresses the human, technological, and environmental factors that influence authentication usability and security. It is user-centric, context-aware, and offers a security-usability balance and

therefore, can be used in any security research that involves the user and the environment. Figure 7 shows the interacting components of the model.

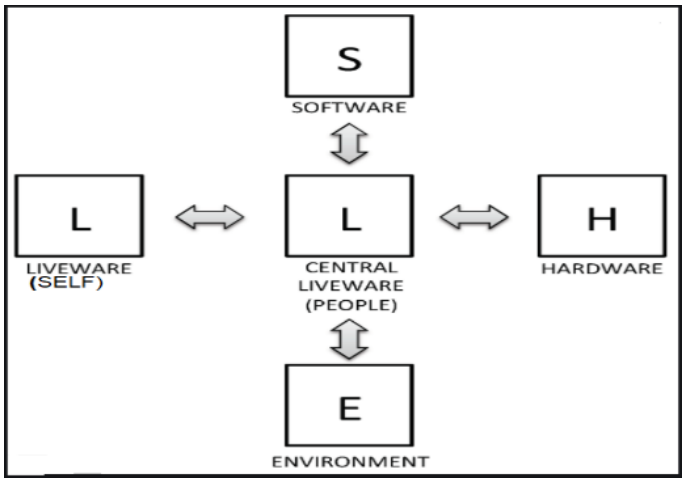


Figure 7 : SHELL Model. Adapted from Hawkins[148]

The model in relation to the thesis is explained as below:

- **Software:** The thesis revolves around software. It consists of the rule and role-based access control methods, the hybrid algorithm, the risk calculation model, and the adaptive user authentication app based on Naïve Bayes. Human contact with this software is explicitly addressed by the user-centred design (UCD) methodology.
- **Hardware:** These are the physical devices used. The hardware used is the Android smartphone and the PineTime smartwatch, which communicate via Bluetooth Low Energy (BLE).
- **Environment:** This is the context in which the system operates. This includes the unique environment of developing world healthcare, the challenges of resource-constrained IoMT devices, and the need for solutions that function outside of a controlled laboratory environment.
- **Liveware (L-L):** This is the most crucial link, which represents the human user. The research is fundamentally about the elderly and young users, their ICT skills, health conditions, and their preferences for simple physiological biometrics. The entire framework is designed to adapt to these individual user profiles and improve their experience.

3.2.1 Usability Models

Human Factors Analysis and Classification System (HFACS) Model

The HFACS model provides a framework for understanding and classifying human errors. It was developed by Shappel and Wiegmann [150] was built from the Swiss Cheese Model and guided the usability component of this research. It identifies active and latent factors in incidents and asserts that unfortunate security incidents occur when both active and latent failures coincide [151]. This thesis, by focusing on improving usable security, tries to decrease human mistakes that could lead to security breaches.

- **Unsafe Acts:** Unsafe acts, such as an unauthorised user attempting to log in, are immediately addressed by the adaptive authentication framework. In order to avert a possible security crisis, the system is designed to dynamically assess the probability of such an attempt and either authenticate, step up authentication, or block the request.
- **Preconditions for Unsafe Acts:** The study specifically points out issues like the inability to strike a balance between security and usability that function as prerequisites for risky behaviour. The thesis seeks to eliminate this requirement by creating a system that is both secure and usable. The adaptable framework is also made to take into account the different ICT proficiency levels of users, particularly the elderly.
- **Supervision:** The proposed framework offers a technology solution that lessens the need for constant human supervision for user authentication.
- **Organisational Influences:** By recognising the security and privacy concerns in the healthcare sector, the barriers to home-based patient management in developing countries, and the necessity of moving away from a security-only focus and towards a balance with usability, the thesis tackles the larger organisational environment. An organisational shift that encourages improved security procedures and user compliance is the proposed solution.

The model, together with the Social Shaping of Technology (SST) [152] and the Social Construction of Technology (SCOT) model [153] will explain the Liveware component of the SHELL model. These examine user-centred design and preferences, context-specific design for developing world settings, meeting a societal need—the achievement of SDG 3—and customised prototypes for diverse users.

3.3 Overview of Publications

Part I: User-centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones.

This part first reviews existing IoMT user authentication techniques, analysing challenges concerning the African users' contexts and then goes on to design a Machine Learning based adaptive user authentication framework that adapts to user profiles and context during login to determine the likelihood of the attempt being illegitimate before assigning appropriate authentication mechanisms. The proposed edge-centric framework fuses the Naive Bayes classifier and CoFRA model to determine the risk associated with a login attempt based on biometric wearable sensor data, non-biometric smartphone sensor data, and some predefined data. User backgrounds and preferences are solicited and incorporated into the design. Results show that users, despite their ICT Skills, ages, jobs, and years of experience, prefer to use simple physiological biometrics for authentication. The proposed architecture is then implemented in an Android App that is developed following the User-Centred Design and installed on a smartphone, which communicates with a PineTime smartwatch. Sensor data is used as input in calculating the risk associated with an access request to decide whether to authenticate, step up authentication, or block a request using rule and role-based access control techniques while also non-intrusively monitoring health. The app is tested in a laboratory environment, and results show potential of the framework is expected to improve user experience in authentication, promoting the use of IoT in healthcare.

- The study developed an Android Application that uses the Naïve Bayes Conditional Probability Theorem to calculate the risk associated with a login attempt to decide how to authenticate a user based on the risk score.
- The App is designed to communicate with a PineTime smartwatch via Bluetooth Low Energy (BLE).
- The app is tested in the lab environment with total login time compared to the generally accepted, and user preferences are solicited using questionnaires.

Part II: Weighted Naïve Bayes multi-user classification for adaptive authentication.

Following the design of an adaptive user authentication framework for use in smartphones and wearables, this section presents a multiclass classification algorithm that classifies users into six distinct risk classes. We note that machine learning classification algorithms have been extensively utilised in addressing user authentication challenges. Nonetheless, a majority of solutions

categorise users into three classes, with the most popular being binary, where a user is either classified as legitimate or not. The rationale behind this limitation has not been comprehensively examined, and through this research, we seek to find out why a few risk classes are used. If we are to authenticate a user more amiably, we need not bundle users as legitimate or not but rather spread the users on a scale between zero and one, such that the authentication difficulty will be based on the actual risk associated with a user. The study, therefore, leveraged the Naive Bayes theorem for user authentication endeavors to assess the risk associated with login attempts. We plan to develop a hybrid algorithm that incorporates feature and contextual weights in the Naive Bayes algorithm to cater for the conditional independence bias in login risk calculation. For multiclass classification, the Naive Bayes Machine Learning algorithm, along with its variations such as Gaussian, Categorical, and Bernoulli, is applied on both weighted and unweighted datasets to ascertain risk levels and categorise them into six classes. Additionally, the classification model is tested using alternative algorithms.

The main contributions and results are summarised as below:

- We developed our own risk calculation model based on the Naïve Bayes theorem.
- We assigned weights to our contextual factors that we used as variables in the risk calculation formula.
- The risk is calculated from deviations of contextual factors from the known that occur at login time.
- The outcomes of cross-validation and comparative analyses reveal that the performance is commendable for up to three classes, after which a decrease is observed in certain Naive Bayes and SVM classifiers.
- Among the Naïve Bayes family, the BernoulliNB algorithm exhibits superior performance but is surpassed by Decision Trees, SVM, XGB, and Random Forests.

- The weighted dataset consistently outperforms the unweighted counterpart, with the allocation of weights significantly influencing algorithmic efficacy.
- The 80:20 split strategy yields the most favorable outcomes in contrast to the 70:30 and 60:40 splits, albeit no significant variances are detected during cross-validation.
- Non-Naïve Bayes algorithms demonstrate superior performance compared to Naïve Bayes algorithms.
- For Naïve Bayes, optimal performance is achieved with three classes, highlighting its utility in conditional risk calculation, while non-Naïve Bayes multiclassification algorithms are more suitable for classification tasks due to the problem's inherent compatibility with conditional probabilities.

Part III – A: An Android-Based Internet Of Medical Things Adaptive User Authentication And Authorisation Model For The Elderly.

This section demonstrates how our risk-based adaptive user authentication model is implemented in a smartphone and tests its adherence to usable security using senior citizens. Research states that globally, 77% of the elderly aged 65 and above suffer from multiple chronic ailments, but several barriers within the healthcare system in the developing world hinder the adoption of home-based patient management, hence the need for the IoMT, whose application raises security concerns, particularly in authentication. Several authentication techniques have been proposed; however, they lack a balance of security and usability.

The main contributions and results are summarised below:

- We propose a Naive Bayes-based adaptive user authentication app that calculates the risk associated with a login attempt on an Android device for elderly users, using their health conditions, risk score, and available authenticators.
- This authentication technique, guided by the MAPE-K_{HMT} framework, makes use of embedded smartphone sensors.
- The model makes use of knowledge-based and biometric authenticators, which constitute static authentication.
- Results indicate a 100% and 98.6% accuracy in usable security metrics, while cross-validation and normalisation results also support the accuracy, efficiency, effectiveness,

- and usability of our model, with room for scaling it up without computational costs and generalising it beyond SSA.
- The post-deployment evaluation also confirms that users found the app usable and secure.
- A few areas need further refinement to improve accuracy, usability, security, and acceptance.
- The model shows potential to improve users' compliance with IoMT security, thereby promoting the attainment of SDG3.

Part III – B: Based on the article: Naïve Bayes Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users.

This section also presents the implementation of an adaptive authentication prototype for young IoMT users. The increasing use of the IoMT in healthcare highlights privacy and security concerns surrounding sensitive health data. Some attacks occur after initial login, implying the need for security beyond initial login. This brings about the need for authentication that can run continuously in the background based on several parameters.

The main contributions and results are summarised below:

- This work focuses on enhancing the security and usability of IoMT for young users through a robust, adaptive, continuous authentication model.
- The model uses knowledge-based and physiological biometrics for initial static authentication of Android devices and then heart rate data from smartwatches for behavioural authentication.
- By integrating user behaviour, environmental context, and health conditions, the model dynamically determines risk, trust, and authorisation decisions.
- Machine learning techniques analyse data related to devices, networks, locations, and user habits while considering demographics like age and medical conditions to assign suitable authenticators.
- The model balances accuracy and usability, favouring correct positive predictions, but faces limitations such as class imbalance, feature selection, and overfitting, with a false rejection rate (FRR) of 19%.

- Behavioural biometrics, personalised authentication, and continuous authentication enhance security and accessibility; however, moderate sensitivity affects their ability to capture all positive cases.
- Age-group analysis reveals varying engagement with technology, emphasising tailored authentication flows.

This page has been intentionally left blank

Part I

PART I

User-Centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones

Part I is published as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma. User-Centered Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones. Lecture Notes in Networks and Systems book series (LNNS, volume 724) Pages 783-799. Published July 2023.URL: https://link.springer.com/chapter/10.1007/978-3-031-35314-7_65

User-Centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, and Frederic Nzanywayingoma

Abstract

As the world grapples with an increase in diseases, including COVID-19, the Internet of Medical Things emerges as a complementary technology to the healthcare staff, which is constantly overburdened. Untrained users increased online presence exposes them to cyberattack threats. Authentication is the first line of defence for protecting medical data, but existing solutions do not consider the user's context and capabilities, making them unusable for some groups of users who eventually shun them. This paper proposes a Machine Learning based adaptive user authentication framework that adapts to user profiles and context during login to determine the likelihood of the attempt being illegitimate before assigning appropriate authentication mechanisms. The proposed edge-centric framework fuses the Naive Bayes classifier and CoFRA model to determine the risk associated with a login attempt based on biometric wearable sensor data, non-biometric smartphone sensor data, and some predefined data. User backgrounds and preferences were solicited, and results showed that users, despite their ICT skills, ages, jobs, and years of experience, prefer to use simple physiological biometrics for authentication. An Android App was then developed using the User-Centred design and installed on a smartphone, which communicated with a PineTime smartwatch. Sensor data was used as input in calculating the risk associated with an access request to decide whether to authenticate, step up authentication, or block a request using rule and role-based access control techniques while also non-intrusively monitoring health. Once implemented, the framework is expected to improve user experience in authentication promoting the use of IoT in healthcare.

1.0 Introduction

Constant reliance on the caregiver can become frustrating at some point during a person's illness, but terminal illnesses necessitate constant medical care and monitoring. At the same time, caregivers cannot be present all of the time to monitor patients, imposing the need for self-help [1]. IoT is being used in pervasive healthcare to complement healthcare workers and caregivers worldwide, with International Data Corporation (IDC) estimating that more than 70% of healthcare providers in the United States are already using it [154]. IoT plays a significant role in combating infectious diseases and transforming the entire healthcare sector [14], with benefits and applications detailed in Hintze *et al.* [12]. The aged population, prevalence of chronic diseases, shortage of healthcare specialists, rising medical care costs, and the COVID-19 pandemic, among other factors, have contributed to the expansion of the IoMT as a pervasive healthcare enabler. However, its introduction comes with several challenges compounded by the fact that the same security used to protect general IoT devices cannot secure IoMT environments because the threat landscape and malicious motives in them differ greatly [128]. Various security mechanisms have been proposed to prevent attacks on IoTs, with authentication and authorisation being the primary security concerns [155]. However, the commonly used authentication mechanisms are frequently rigid and do not consider user profiles, making them difficult to use. It is therefore critical to make it difficult for a suspicious user while making it simple for a trusted user. Usability is frequently treated as an afterthought, resulting in security solutions that are not adopted by end users, hence the need for a proper study into the balance of usability versus security on user authentication [156]. Also, a user is the weakest link who may fail to follow the rigour of security mechanisms, and as observed by Steger [157], internal misconduct accounts for a greater proportion of incidents in healthcare, making it the only industry where insiders inflict more cyber-harm.

By proposing a smartphone-based authentication solution that adapts to user profiles and context when determining which authentication mechanism to assign to them in an IoT environment, this research seeks to contribute to usable security and complement previous proposals. A plethora of research on IoT user authentication has been conducted in various parts of the world, but little has been done in relation to what may be appropriate for a specific group of users who are generally treated the same when they are different [158]. This paper will also describe a case study that will help shape the design of an adaptive authentication prototype.

1.1 Related Work

As mentioned earlier, research is ongoing, but when it comes to adaptive authentication, the research output is not practical enough to benefit end users. We will now look at adaptive authentication work that has been carried out by other researchers, and our analysis is not limited to the medical environment. Forget *et al.* [126] proposed a choose your own authentication architecture (CYOA) in which users select a scheme from available alternatives based on their preferences, abilities, and usage context. The approach, however, is not dynamic, thereby introducing some delay. In Wojtowicz [127], a scheme for adjusting a smartphone's lock between voice recognition, face scan, and fingerprint, based on which will be currently usable, was proposed. The work focused solely on usability, leaving out security and context. Hintze *et al.* [159] used location-based risk assessment in conjunction with multi-modal biometrics to adjust the level of authentication required to the situational risk of unauthorised access. However, relying solely on GSM cell IDs and Wi-Fi access point MAC addresses may be difficult if third-party information is withheld. The researchers Kumar *et al.* in [122] assumed that the best authentication method for wearables and nearables is the owner's biometric information. However, not all biometrics may apply to all users as user context affects usability, with, for example, a user with body tremors may find it difficult to use fingerprint, the same with a person in a noisy environment who may be unable to use voice. In a resource-constrained environment, Gebrie *et al.* [160] proposed a method for continuously monitoring and analysing user and device activities and selecting authentication or reauthentication based on the risk involved using the Naive Bayes Machine Learning algorithm. This kind of authentication minimises attacks that occur after login but may not work well for inactive users. Misbahuddin and Bhindumadhava [161] created a risk engine that examines a user's previous login records and generates a pattern using Machine Learning to calculate the user's risk level. This approach relied heavily on previous logins and only used recall mechanisms, which hampered usability for some elderly users and dementia patients. Vhaduri and Poellabauer [162] described an implicit wearable device user authentication mechanism that used a combination of three types of biometrics: behavioural (step counts), physiological (heart rate), and hybrid (calorie burn and metabolic equivalent of task). The work was not adaptive, and the experiment only used an expensive iPhone and a Fitbit. He *et al.* [163] conducted a home IoT authentication usability study and discovered that smartphones are the most

used devices to access IoT devices in the home and can closely meet user expectations. The findings concur with those of Forget *et al.*[126] and Batool *et al.* [164] who evaluated smartphone sensors and concluded that sensors embedded in smartphones and wearables enable the collection of a user's specific dataset at very low financial and computational cost. It is, however, worth noting that most previous studies were carried out in a controlled laboratory setting. They have not examined:

- investigating suspicious activity in the user authentication profile.
- feature selection that allows for precise and effective modelling of user behaviour.
- the ability of authentication systems to adapt to changes in user behaviour.

1.2 Contribution

In this paper, we attempt to address the above shortcomings through presenting an adaptive IoMT user authentication framework for determining authentication based on context, user profiles and available authenticators, among other factors described in Section 2. This framework combines edge computing, machine learning, role-based access control, and rule-based access control guided by the CoFRA [165] modelling framework. We intend to develop, as part of the proposed framework,

i) a contextual model that identifies a user using smartphone and wearable sensors and their pre-defined characteristics,

ii) a Naive Bayes classifier that uses the contextual model and fuzzy logic to calculate the risk associated with a user's login attempt based on his/her role, and

iii) rule-based access control to assign appropriate authenticators to a user based on their context risk score, usability, and availability of authenticators. We intend to use a smartphone that most users already own, as well as a low-cost PineTime smartwatch.

2.0 Requirements for Adaptive Authentication

Most existing user authentication mechanisms are rigid and do not consider the user's capabilities, highlighting the need to classify users and tailor authentication to their needs, particularly in healthcare. Multi-factor authentication (MFA), which was once considered entirely secure in organisations with a relatively small number of users, became ineffective in instances where the

risk is relatively high [166]. This necessitated the use of adaptive authentication, the requirements for which are outlined below.

Usability. This is defined in Gordieiev *et al.* [167], if a user correctly employs a technology, he or she will not pose a security risk. User interfaces must be usable and correspond to the user's mental model of security mechanisms, and even if a system is technically secure, it is the end user who operates it and determines its usability [168].

Security. Security is also defined in Gordieiev *et al.* [167], and because the same security controls used to protect general IoT devices cannot secure IoMT environments, a lightweight security solution must be implemented. With an unprecedented increase in online activities, there is a significant increase in security breaches within healthcare [169].

Cost. One of the barriers to full adoption of IoMT in Sub-Saharan Africa (SSA) is cost [170]. To ensure a cost-effective solution, we intend to use the sensors of an Android smartphone and a smartwatch for context establishment and authentication.

Portability. A PineTime smartwatch will be used to supplement smartphone sensors, which will use a Low Energy Bluetooth module for offloading to the smartphone. It is small enough and compatible with most Android smartphones.

Low Energy Consumption. The proposed scheme's devices will run on rechargeable batteries. The smartphone will function in its normal way, and the smartwatch will be charged via USB. To save energy, wearable sensors should operate in duty cycle mode.

Low Latency. The edge-centric architecture is an appealing alternative to other models, such as the cloud-centric approach, because the collected data is first preprocessed and analysed on the edge, allowing for time-sensitive authentication decisions to be made within the local network, reducing time consumed and congestion between the gateway and the cloud [171].

Deployability. Deployability plays a significant role in strengthening the security of IoMT. Some authentication mechanisms may offer significant protection but may not be deployable in some situations. For instance, compatibility of a mechanism with a device, in our case, on smartphones electrocardiograms may offer unique features, but cannot be deployed on smartphones that already have some built-in sensors.

3.0 Research Methodology

The User Centered Design (UCD) in Santana-Mancilla *et al.* [158] methodology was used in this study, which is an iterative process with four stages described below.

3.1 User Centred Design

3.1.1 Specifying Usage Context

Adaptive authentication is required for all age groups, including the elderly, who may be digitally illiterate [172] and may have underlying medical conditions that will likely influence the choice of authenticators to be used.

3.1.2 Specify Requirements

Questionnaires were distributed to patients and medical staff to gather information about their backgrounds, skills, and needs for inclusion in the prototype design.

3.1.3 Producing Design Solutions

The proposed adaptive authentication scheme is classified as one of the four IoT layers.

Perception Layer. This layer includes biometric and non-biometric sensors that are located on the owner's wearable and smartphone.

Network Layer. This layer is made up of edge and fog layers. The edge layer is made up of a network of sensors found in wearables and smartphones. In this case, the smartphone, which serves both senses and processes, serves as a gateway to process data before sending it to the cloud. Low-energy Bluetooth will ensure communication between the smartwatch and the smartphone.

Cloud Layer. This layer performs analytics and additional processing to assist in decision-making when necessary. Google Cloud Services are used to store and extract geolocations and maps.

Application Layer. This layer is critical for users who require a pleasant user experience. Users will be authenticated using an app installed on their smartphone. Android Studio and Java will be used to create the app with XAMP 3.2.4 backend.

The proposed adaptive authentication model is based on a modified version of the Monitor Adapt Plan Execute – Knowledge with Human Machine Teaming (MAPE-K $_{HMT}$) framework, modified from [173]. Figure 1 depicts the detailed framework and its relationship to the IoMT architecture.

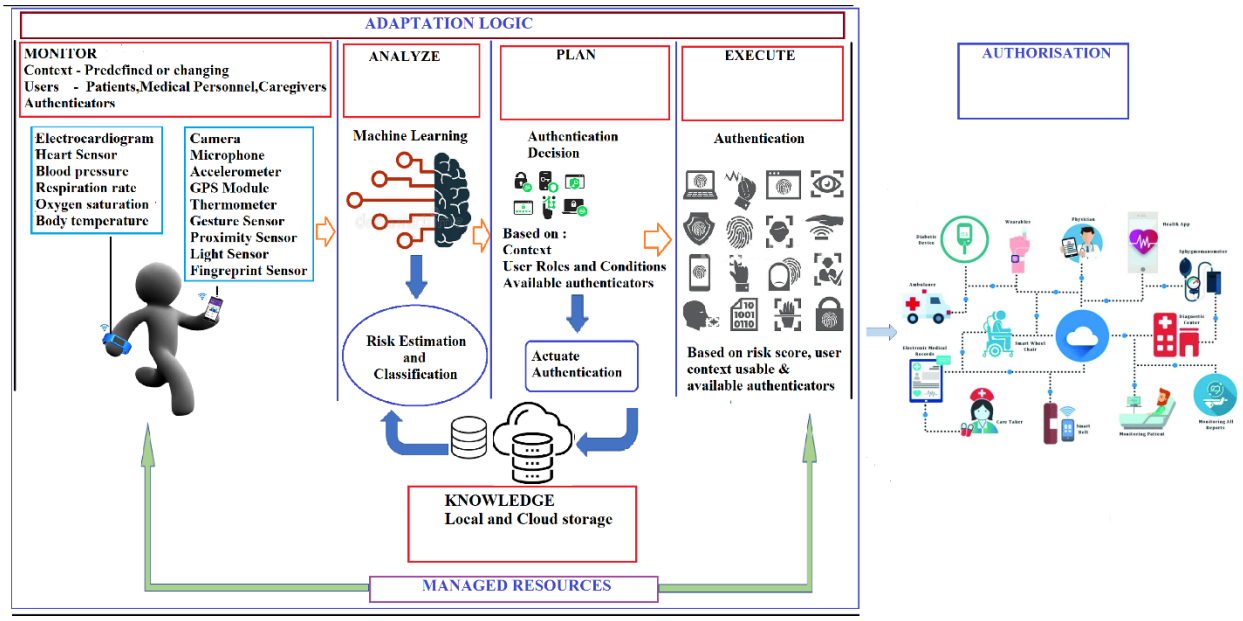


Figure 1: Proposed framework using the MAPE-K$_{HMT}$ model

The framework was broken down to gain a better understanding of the interacting entities from the beginning to the end. It was also during this phase that several risk calculating frameworks were evaluated before settling for fusing the Naïve Bayes and the CoFRA model. Figure 2 shows the simplified graphical context model of the framework.

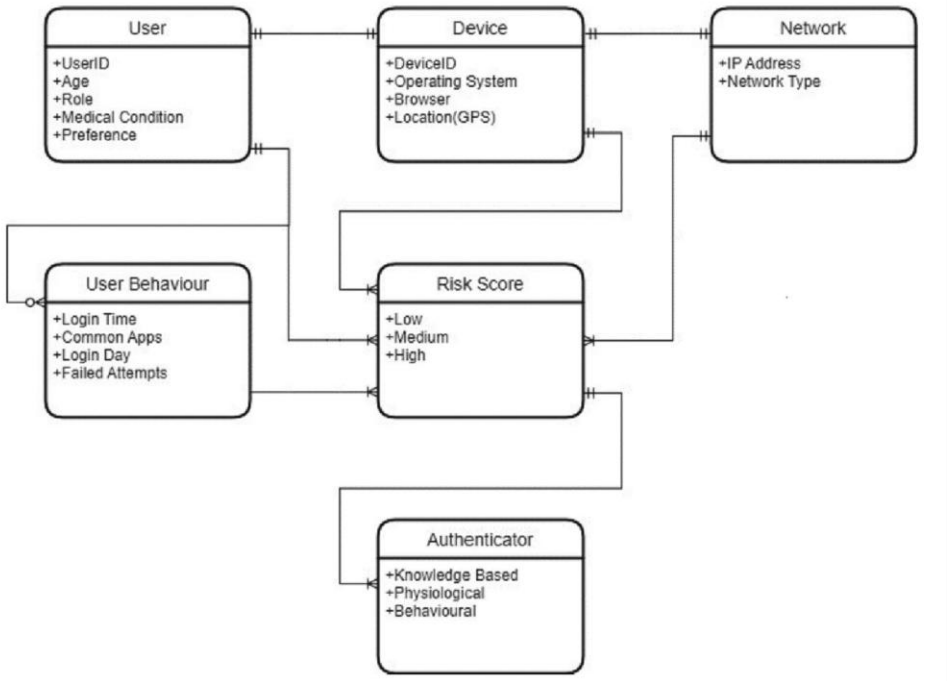


Figure 2: Context Model showing relationships between entities on proposed system

Figure 3 depicts the detailed implementation schema in which the smartwatch will communicate with the smartphone and medical devices.

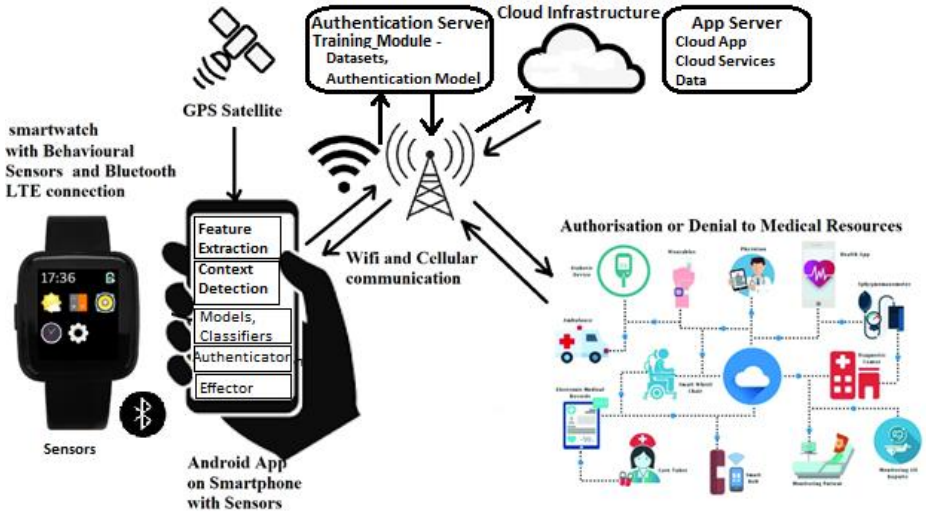


Figure 3: Proposed Detailed Implementation Architecture

Because of the sensors shown in Figure 4, the smartphone and smartwatch were chosen for user authentication.

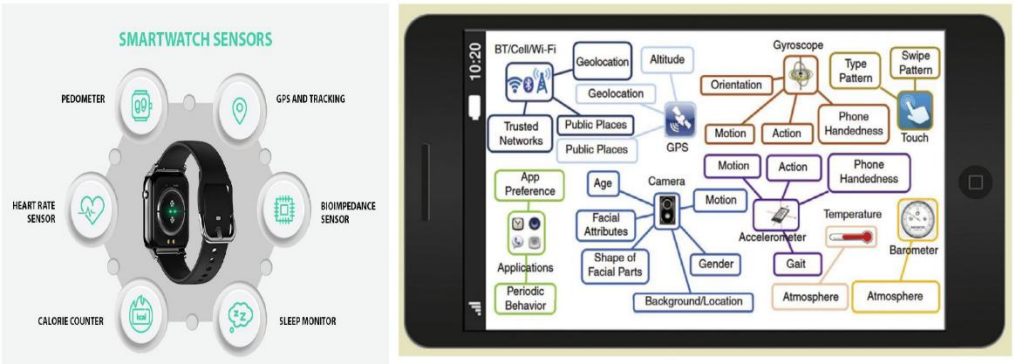


Figure 4. Candidate sensors for authentication (Source [174][175])

The smartphone facilitates communication between IoMT device ensuring protocol compatibility and interoperability.

Working Mechanism of Adaptive Authentication.

During user authentication, an assessment of context (both fixed and variable factors) is performed to estimate the risk of the request, resulting in risk calculation for user classification. The proposed algorithm consists of the following:

Input

C – Contextual factors $\{c_1, c_2, c_3 \ldots c_n\}$ describing a user

A – Available and usable authenticators for a user profile

Output

Adaptive authentication that adaptively selects an optimal set of available authenticators based on intersection of calculated risk score *(RS)* and user profile *(UP)* expressed as $(AA) \rightarrow (RS) \cap (UP)$.

The following steps follow the MAPE-K_{HMT} adaptive framework.

Monitor

This stage is primarily concerned with gathering data from the self-adaptive system and its environment via hardware sensors and software. The following steps are followed in the proposed scheme.

a) *Define the access control subsystem* $s_i \in S$;
b) *Prepare set C of the possible*
   i. contextual factors that describe a subject
   $\forall s_i \in S$: $C = \{c_1, c_2, \ldots c_n\}$,

   ii. usable authenticators available
   $A \in A'$ *(all authenticators)*
c) *Train a mathematical model for decision-making, factoring in context, user, available authenticators, and risk score.*
   $P \rightarrow <C, U, A, RS>$ *where P is the user profile.*
d) *Create a set of user profiles as a knowledge base for the next authentication attempts.*

Mathematical Model Training

We will train a Naive Bayes Classifier, a statistical model for decision-making that assesses the risk of a user's authentication attempt. The training procedure learns what is considered a "normal" or "legitimate" access attempt and what indicates a possible risk based on the user's past data.

Creating a personalised probabilistic model for every user is the main goal of the training procedure. Because it is an adaptive model, it keeps learning from fresh attempts at authentication. Previous authentication attempts that have been classified as successful or unsuccessful make up the training data.

Given a set of observed features, the model is trained to determine the posterior probability that an authentication attempt falls into a specific class (such as "legitimate" or "fraudulent"). The basic formula is a variant of the Bayes' Theorem:

$$P(Class|Features) \propto P(Class) \times \prod_{i=1}^{n} P(Feature_i|Class)$$

Where

- **Context (C)**: The contextual factors (C) like IPAddress, Network_Type, and GPS_Coordinates are treated as the input features (X) of the model. The model learns the probability of these factors appearing in a legitimate login attempt for a specific user. For example, the model learns that a user typically logs in from a specific IP address range or certain GPS_Coordinates. Any deviation from these learned probabilities will increase the calculated risk score.
- **User (U) and User Profile (P)**: The model is customised for every user; it is not generic. The knowledge base is the user profile (P), which houses all of the learned probabilities and historical data for that particular person. The model compares the current features to the baseline set in that user's profile whenever a new login attempt takes place.
- **Available Authenticators (A)**: The available authenticators are also taken into account by the model. For example, having a "usable" authenticator (such as a biometric scan) lowers the risk score because it greatly raises the likelihood of a valid attempt if it is successful. A crucial element in the training and decision-making process is the usability of these authenticators (for example, as established by age and health status from the first algorithm).
- **Risk Score (RS):** The trained model's output is the risk score. This score is calculated by summing all the weighted conditional probabilities in the model's decision-making process. The system is more likely to believe that the attempt is fake if the risk score is higher. Whether this computed risk score exceeds a predetermined threshold determines whether access is ultimately granted or denied.

3.3.2 Initial user and device registration

The user *(U)* must first register on the app installed on their smartphone (SP), which serves as both a Gateway *(GW)* and an Authenticating Device *(AD).* The following steps are taken during the user registration phase:

1. *U chooses PIN, Password, Pattern, answer to secret question, Inputs his/her fingerprint (FP) and any other authentication factor available on AD and Wearable (WB) for storage.*
2. *U's predefined conditions i.e., Age, Role, Disability, Access-Time(T), Role (patient, nurse, doctor) are defined and captured.*

3. *U's known location(L) from Google Maps, the device fingerprint (DFP) is captured, and mapping occurs U→SP, U→L, U→T.*
4. *Mappings are saved in the local server which is the SP memory.*

If a wearable (WB) is used, the user is mapped to it *U →WB.*

5. *Wearable (WB) is mapped to the smartphone (SP) WB→SP.*
   SP on receiving the registration request from WB, does the following:
   Checks U →WB, if they are not related, the registration is terminated,
   otherwise. The next stage is followed.
6. *Relationships are saved in SP memory.*

Adapt

Based on the monitored and expected state, environment, and any other related constraints, this phase determines whether adaptation is required.

Login Stage

Following successful registration, an authorised user *(U)* can gain access to the desired medical IoT via the adaptive authentication phase. To start the authentication process, *(U)* must open the app on their smartphone *(SP).* The opening will trigger communication between SP, WB, and other related services. The following steps are followed during the user authentication process.

1. *First, User U uses the smartphone to open the application.*
2. *The application checks the pre-conditions associated with the user which are:*
   (U→SP) AND (U→WB) AND (U→L) AND (U→T)

Risk Calculation

3. *Naïve Bayes classifier is then invoked to calculate the risk and classify user based on the degree of match of predefined conditions and contextual factors. The fuzzy score is between 0 and 1.*

   The calculation is as shown in equation (1) below.

$$P(y|x_1, \dots \dots \dots x_n) = \frac{P(x_1|y)P(x_2|y)\dots P(x_n|y)P(Y)}{P(x_1)P(x_2)\dots\dots P(x_n)} \quad (1)$$

Where x_1 represents the contextual factors and y represents the risk probability.

4. *The Fuzzy Score is mapped to predefined classes. Scores are shown in Table 1.*

Table 2:Proposed Risk Score classes

Normal	**Low**	**Medium**	**High**
0 - 0.19	0.2 – 0.39	0.4 – 0.79	0.8 – 0.89

Plan

Rule-based authentication is planned, considering the user context, capabilities stored in the database, and available authenticators. The planned self-adaptation includes choosing appropriate authenticators or even denying access, guided by the CoFRA [165][19] framework shown in Figure 2.

Execute

This is the stage at which the previously generated plan is carried out, in this case, authentication using the appropriate, usable, or available authenticator and denial if the attempt is deemed fraudulent as defined in [165].

5. Rule-Based Authentication
   Initialise Count to 0 {Number of authentication attempts}

While Count<=3
If U class is Normal, use normal single authenticator provided the user can use it.
Elseif (Low)
Use Authenticator A provided the user can use it.
Elseif (Medium)
Use Authenticator A AND Authenticator B provided the user can use it.
Elseif (High)
Use Authenticator A AND Authenticator B AND Authenticator C
Else
Re-authenticate.
Count ++
Do Terminate Authentication, Block User, Report

Authorisation

If the user meets all the security requirements, authorisation occurs and access to a variety of medical resources required based on his or her role is granted.

Knowledge Base

The Knowledge base stores user and runtime models, as well as contextual models.

Human Machine Teaming

Human Machine Teaming refers to the interaction of the devices with the user.

4.0 Case Study: Adaptive User Authentication

Smartphones, smartwatches, and fitness apps are major data collectors. Figure 5 to 7 depicts IoT adaptive authentication user characteristics for our case study. As shown in Figure 3, an Android mobile app was created to enable communication between a user's User-Centred Design of Machine Learning smartphone and a PineTime smartwatch. The user can be a patient, or a member of the medical staff and the patient may be in a hospital or at home. We expect our case study to help us refine our adaptive authentication framework for improved usability and security as adaptive security. A total of eighty-five (85) patients and twenty-four (24) health workers from the SSA context, specifically from Rwanda and Zimbabwe completed the pre-deployment questionnaires whose results are presented below.

5.0 Results and Discussion

Questionnaires gathered data that informed the design of the prototype. Furthermore, the findings were compared to previous findings and were incorporated into the Android app that was created. When compared to patients, there was an equal distribution of males and females among medical staff. Women are 26% less likely than men to use mobile internet services in low and middle-income countries [176], indicating that the gender divide has an impact on IoT adoption. This may be true for patients, but not for medical staff, who may be forced to use technology at work. Figure 5a) shows the analysis of patients' age groups, and 5b) medical staff.

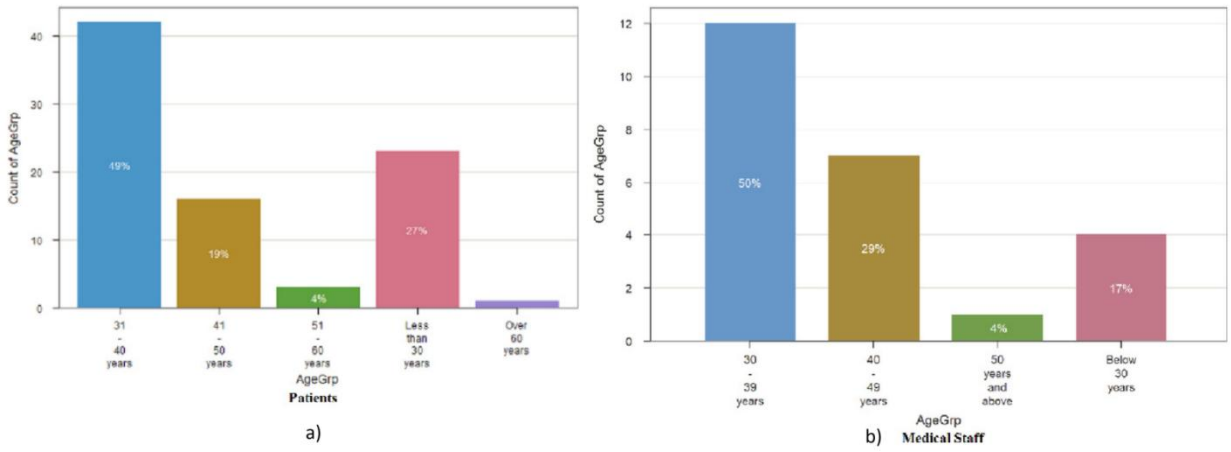


Figure 5: Analysis of responses by age group

The 30–39 age group dominated the sample, with a smaller proportion representing the older population. This may influence the study's outcome.

Medical Conditions: Medical conditions can affect an authentication candidate's cognitive, physical, and visual abilities. Only three of the elderly patients admitted to having some medical conditions in the survey. The low response rate is due in part to the small number of elderly patients among the respondents.

A question was asked to see if respondents understood the significance of protecting their medical data. Figure 6a) depicts the responses of patients, while Figure 6b) shows responses of medical personnel.

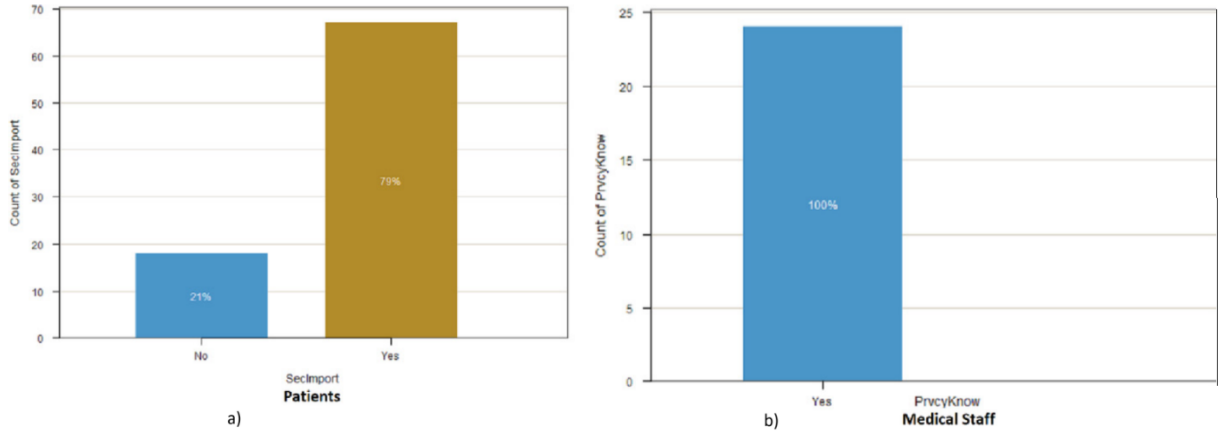


Figure 6: Analysis of knowledge of the importance of security

In terms of patient respondents, 34% of the female population and 14% of the male population were unaware of the importance of medical data security. 66% of the female population and 86% of the male population were aware of the importance of medical data security. Although there are differences in the reasons for protecting medical data, all members of the Medical Staff agreed on the importance of securing medical data.

An analysis of preferred smartphone authentication by job title and gender was performed. As previously stated, gender influences the ease of use of technology. Figure 7 shows an analysis of preferred authentication on medical devices by gender where Figure 7a) shows patients while Figure 7b) shows medical personnel.

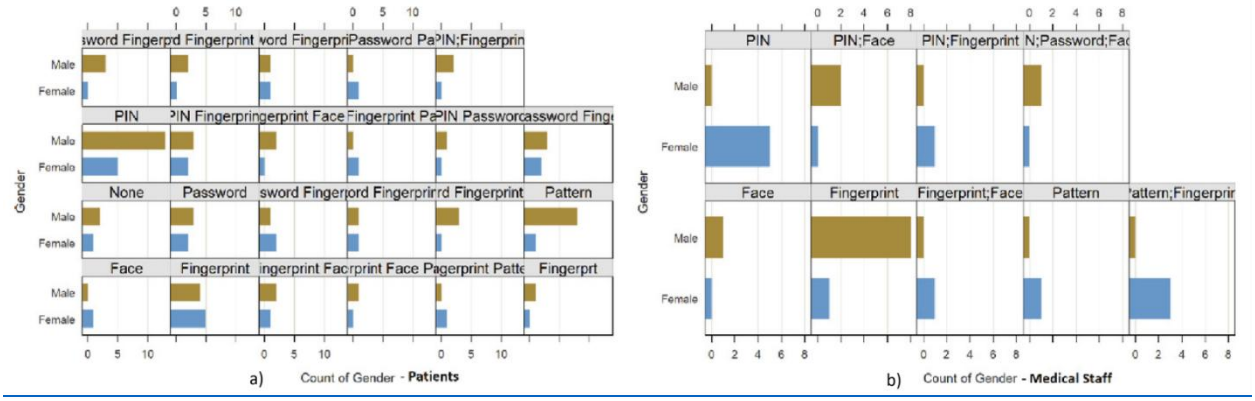
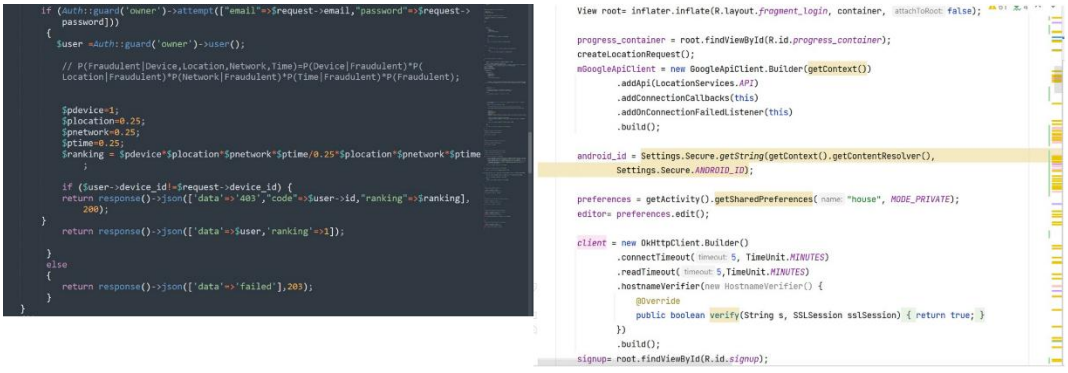
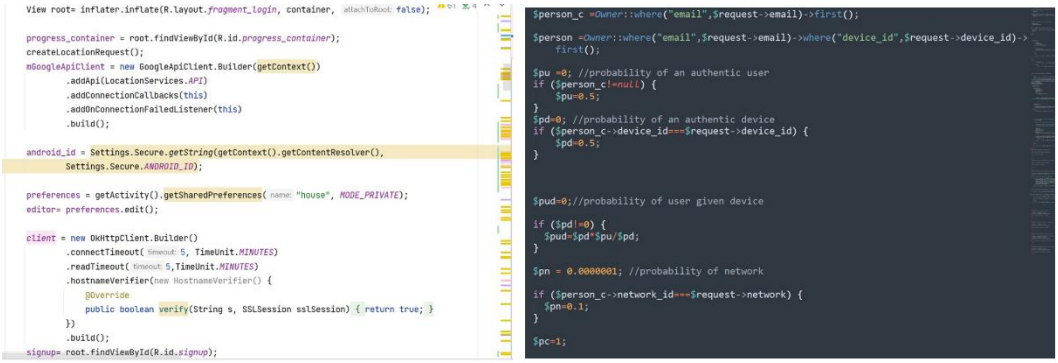


Figure 7: Analysis of preferred medical device authentication by gender

There was no statistically significant difference between smartphone and medical device authentication among respondents. An analysis of preferred authenticators by age group was made. PIN and fingerprint authentication were the most popular single-factor authentication methods among both patients and medical staff, followed by password and none. Even when medical staff were analysed by job, PIN and Fingerprint dominated, followed by face and multi-factor combinations. Although it has technical disadvantages, PIN is preferred because it provides quick authentication [177]. According to Grindrod *et al.* [178], Fingerprint recognition, despite being popular and widely used, has a low success rate. Although the elderly population was small, the results confirmed Ehatisham-ul-Haq *et al*. [177] and AMROUN *et al*.[179] who identified reasons for the password's unpopularity among elderly users. The combination of PIN and fingerprint also dominated two-factor authentication. On multi-factor authentication, the combination of PIN, Fingerprint, and Password were dominant. This shows that despite the maturity of authentication, users still prefer the basic authentications. All the collected data was analysed and used to create an Android prototype, which is depicted in Figure 8 where Figure 8a) shows context weights assignment and initial risk calculation, while Figure 8b) shows second stage of risk calculation.



a) Weight assignment and initial risk calculation



```
View root= inflater.inflate(R.layout.fragment_login, container, attachToRoot: false);

progress_container = root.findViewById(R.id.progress_container);
createLocationRequest();
mGoogleApiClient = new GoogleApiClient.Builder(getContext())
        .addApi(LocationServices.API)
        .addConnectionCallbacks(this)
        .addOnConnectionFailedListener(this)
        .build();

android_id = Settings.Secure.getString(getContext().getContentResolver(),
        Settings.Secure.ANDROID_ID);

preferences = getActivity().getSharedPreferences( name: "house", MODE_PRIVATE);
editor= preferences.edit();

client = new OkHttpClient.Builder()
        .connectTimeout( timeout: 5, TimeUnit.MINUTES)
        .readTimeout( timeout: 5,TimeUnit.MINUTES)
        .hostnameVerifier(new HostnameVerifier() {
            @Override
            public boolean verify(String s, SSLSession sslSession) { return true; }
        })
        .build();
signup= root.findViewById(R.id.signup);
```

```
$person_c =Owner::where("email",$request->email)->first();

$person =Owner::where("email",$request->email)->where("device_id",$request->device_id)->
    first();

$pu =0; //probability of an authentic user
if ($person_c!=null) {
    $pu=0.5;
}
$pd=0; //probability of an authentic device
if ($person_c->device_id===$request->device_id) {
    $pd=0.5;
}



$pud=0;//probability of user given device

if ($pd!=0) {
   $pud=$pd*$pu/$pd;
}

$pn = 0.0000001; //probability of network

if ($person_c->network_id===$request->network) {
   $pn=0.1;
}

$pc=1;
```

b) Second stage of risk calculation

Figure 8:Code snippet of proposed prototype

Figure 9 depicts the prototype interface together with the smartwatch that was used.

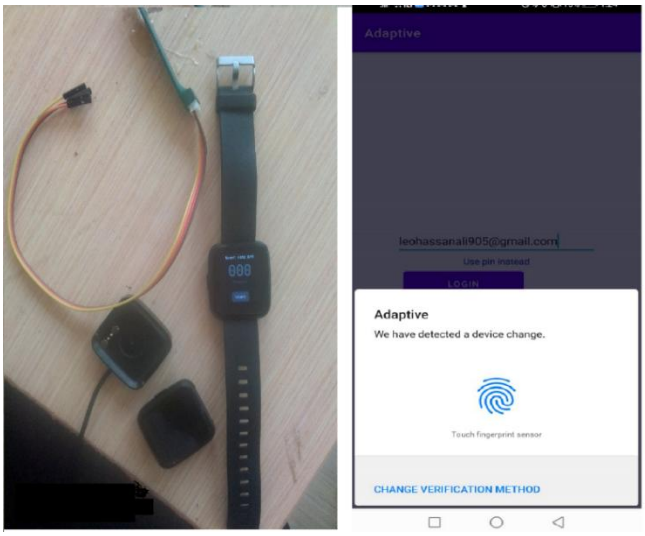


Figure 9: Screenshots of smartwatch and mobile app

Sample data collected in the laboratory environment when the prototype was tested produced promising results. Verification time was done by comparing with the formula in Helkana and Snekkenes [180] and results were in a reasonable range. Upon implementation, we intend to do an extensive evaluation of the prototype and use the usable security metrics to test its conformity to the acceptable units defined in [181]. Machine Learning Metrics will also be used for evaluation which include False Positive, False Negative, True Positive and True Negative. Energy consumption, time and space complexity will also be compared with other existing solutions. A sample of test results is as shown in Figure 10.

ID	DevicePIN	Latitude	Longitude	Network Type	NetworkID	Age	HasMental	HasVisual	HasPhysical	TimeTaken
1	$2y$10$h73YUkIlhFogem	-17.2898	31.3474	wifi	"Software Hub"	26	1	0	1	24.7
2	$2y$10$PRIIGmI8goABWI	-17.2898	31.3474	wifi	"Software Hub"	42	0	1	0	35.8
3	$2y$10$ZXFPynpwzvnBXS	-17.2898	31.3474	wifi	"Software Hub"	22	0	0	0	25.7
4	$2y$10$tO53xeRnYo/P3S	-17.2898	31.3476	wifi	"Software Hub"	28	0	1	0	35.8
5	$2y$10$P6kqPnsq6MHm	-17.2901	31.3479	wifi	"Software Hub"	22	0	1	0	22.5
6	$2y$10$2myqMJx4ypdvF	-17.2898	31.3476	wifi	"Software Hub"	26	0	1	0	24.8
7	$2y$10$zXy6hf.FcjjR323Z/	-17.2898	31.3475	wifi	"Software Hub"	26	0	0	0	17.2
8	$2y$10$pVDDOIrBfWfjhY	-17.2898	31.3477	wifi	"Software Hub"	27	0	1	0	23

Figure 10 : Sample data of proposed prototype collected from a laboratory test

6.0 Conclusion and Future Work

In this paper we presented an adaptive risk based IoMT user authentication framework that uses edge computing to collect user context information and biomedical data from a wearable and a smartphone to determine the risk associated with a user's login attempt and accord the appropriate authenticators based on the user's role, services required and context. The combined use of edge computing, machine learning, role and rule-based access control is expected to create a robust adaptive user authentication system for IoMT at a low cost. The authentication scheme offers several advantages, including improved security, usability, leveraging biomedical signals from wearables for health monitoring and security, high accuracy, the ability to integrate with other smart applications, and lower costs. The aim of this work is to contribute to improving security to patients and medical staff when they access various medical resources using bio data which will also monitor their health. It is expected that the ease of use will contribute to increased adherence thereby contributing to the health and well-being as enshrined in SDG number three.

Part II

PART II

Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication

Part II is published as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma. Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication. Journal of Physics Communications, Volume 8, Issue 10, 2024, Page 105005, Publisher: IOP Publishing, doi =0.1088/2399-6528/ad8a16,URL = https://dx.doi.org/10.1088/2399-6528/ad8a16

Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, and Frederic Nzanywayingoma

Abstract

Machine learning classification algorithms have been extensively utilized in addressing user authentication challenges. Nonetheless, a majority of solutions categorize users into three classes, whereas adaptive authentication scenarios necessitate classification beyond this threshold. The rationale behind this limitation has not been thoroughly explored. The current study leveraged the Naive Bayes theorem for user authentication endeavors to assess the risk associated with login attempts. The Naive Bayes Machine Learning algorithm, along with its variations such as Gaussian, Categorical, and Bernoulli, was applied on both weighted and unweighted datasets to ascertain risk levels and categorize them into six classes. Additionally, the classification task was executed using alternative algorithms. The outcomes of cross-validation and comparative analyses revealed that the performance was commendable for up to three classes, after which a decrease was observed in certain Naive Bayes and SVM classifiers. Among the Naïve Bayes family, the BernoulliNB algorithm exhibited superior performance but was surpassed by Decision Trees, SVM, XGB, and Random Forests. Notably, the weighted dataset consistently outperformed the unweighted counterpart, with the allocation of weights significantly influencing algorithmic efficacy. The 80:20 split strategy yielded the most favourable outcomes in contrast to the 70:30 and 60:40 splits, albeit no significant variances were detected during cross-validation. Non-Naïve Bayes algorithms demonstrated superior performance compared to Naïve Bayes algorithms. For Naïve Bayes, optimal performance is achieved with three classes, highlighting its utility in conditional risk calculation, while non-Naïve Bayes multiclassification algorithms are more suitable for classification tasks due to the problem's inherent compatibility with conditional probabilities. In conclusion, it is imperative to acknowledge that the characteristics of the data, the use of weights, and the data splitting methodology significantly influence the accuracy of machine learning algorithms in multi-class user classification.

1.0 Introduction

IoMT has profoundly reshaped the medical sector by facilitating remote resource access and enabling seamless online interaction between healthcare providers and patients. The global health crisis caused by the COVID-19 pandemic has expedited the implementation of intelligent health technologies such as cloud computing, big data, and machine learning [97]. IoT plays a pivotal role in revolutionising healthcare by offering various advantages [12][182]. These emerging computational frameworks are intricately woven into all aspects of human existence, underscoring the critical need for robust security measures [183]. Ensuring security is paramount in mitigating unauthorised access and the potential misuse of sensitive data exchanged between patients and healthcare professionals. Thorough research focusing on the usability and security of user authentication, it is imperative to ensure that IoT devices are designed with user-centric principles. The examination ought to pinpoint prevalent vulnerabilities in IoT systems, as detailed in the work by [184]. Most IoT devices encounter numerous security challenges [24][185] and many IoMT devices lack the required security [185][186]. However, developing secure authentication protocols is challenging owing to device limitations that limit their ability to perform complex computations, diverse IoMT devices made using different platforms and protocols, and their decentralised nature, which makes them vulnerable to exploitation [97] and the distinct threat landscape and malicious intentions prevalent in IoMT environments, compared to traditional IoT devices [183][187][188][189][190]. Authentication methods differ across devices, often utilising a uniform approach, notwithstanding the more effective strategy of tailoring treatment to individual users based on their level of risk. The integration of riskscore could improve the user experience during authentication by imposing greater challenges on suspicious users while easing the process for less suspicious ones. This, in turn, supports compliance with the IoMT, enhancing overall health and well-being, and contributing to the achievement of Goal 3 outlined in the Sustainable Development Goals (SDG3) aimed at ensuring universal access to healthcare [191]. Various techniques have been amalgamated with machine learning for authentication purposes which leverage techniques such as multi-factor authentication, implicit authentication, and behavioral biometrics, to enhance security and usability in shared environments. However, challenges remain in balancing security with user experience, particularly in dynamic environments where future research may focus on refining these models to enhance adaptability and robustness against emerging threats. According to [192][193][194], there are several limitations in problem classification, primarily due to issues like imbalanced data, computational

constraints, and inadequate training data, where addressing these challenges is crucial for enhancing the effectiveness of ML applications. On the other hand, although these constraints provide difficulties, they also provide room for creativity in machine learning techniques, promoting the investigation of hybrid strategies and cutting-edge algorithms to improve classification precision. Therefore, it is recommended to conduct controlled experiments to determine the most suitable algorithm. Furthermore, the assessment of classification and predictive modelling algorithms predominantly hinges on their outcomes and typically falls into either binary or multi-class categories.

1.1 Main contributions

Previous studies used binary classifiers to categorise users as valid or illegitimate using standard NB, ensuring individuals face the same level of verification difficulty. Our proposed method is part of ongoing work that aims to authenticate users based on their actual risk scores by decoupling user classification. Considering the aforementioned, we plan to develop a hybrid algorithm that incorporates feature and contextual weights in the Naive Bayes algorithm to cater for the conditional independence bias in login risk calculation. The novelty of our work is in incorporating the weighted features in the risk probability calculation, where the deviation from the known context will increase the risk score. We plan to go beyond binary classification as a way of ensuring authentication based on risk score for improved usability of the authentication process. A number of industry frameworks and standards have adopted a more sophisticated, risk-based approach to authentication, moving beyond straightforward binary authentication. The foundation and rationale for your suggested multi-class risk classification are provided by these criteria.

These include the NIST Special Publication 800-63 (Digital Identity Guidelines), FIDO Alliance Standards (FIDO2, WebAuthn), and the OpenID Connect (OIDC). Risk scores will be categorised into several classes. We will compare our weighted scheme with other classification models, observing model behaviours as more classes are added. The summary of previous work and our proposed work is shown in Table 1.

Table 3: Our proposed work against previous work

Item	Previous work	Our proposed work
Usable-Security	The cybersecurity industry regards usability as a trade-off on security rather	We propose to use the Risk score to enhance the usability of the

	than as a security-enhancing component [195][196][197]. Works by Nocera *et al*. [195] acknowledge that bridging the usability/security gap has not been satisfactory and offer a theoretical and practical perspective that they assume will hold in the cybersecurity domain	authentication process by increasing the burden on more suspicious users and decreasing it on less suspicious ones. Our work is part of ongoing authentication research that seeks to address some of the issues identified in Alsaeed *et al.* [97] which include adjustability, re-authentication and user-friendly authentication.
Adaptive authentication	Current authentication techniques impose what users must use [198].	We aim to enable adaptive user authentication by assigning suitable authenticators based on the Risk score and the user profile.
Applying Machine learning to classification problems	There are several limitations in ML classification problems where addressing these challenges is crucial for enhancing the effectiveness of ML Applications [192][193][194][195].	We carry out controlled tests to find the optimal algorithm.
Naïve Bayes accuracy	The general Naïve Bayes approach has been found to perform poorly and is less accurate when attribute independence is violated [199][200][201][202]	We introduce attribute and context weighting, where we assign weights to predictors in risk score calculation for authentication.
Weighted Naïve Bayes accuracy	Research shows that the feature weighting approach outperforms standard NB in many of the examined datasets [203][204].	We propose to show how w_i affects the final risk score, testing different weights.
Multi-class classification	Previous studies used binary classifiers to categorise users as valid or illegitimate, ensuring individuals face the same level of verification difficulty [205][206][207].	The proposed method aims to decouple user classification, extending up to six classes.

2.0 Related Work

2.1 Naïve Bayes algorithm

The Naive Bayes (NB) conditional probability theory has been extensively utilised in the realm of classification tasks, yet its assumption of conditional independence hinders its competitiveness in comparison to alternative algorithms. This theory, as delineated in [208], encompasses a set of classification algorithms based on Bayes' theorem, aimed at categorising data into distinct groups under the presumption of predictor independence, irrespective of their quantity [209]. According to the theory, each predictor is posited to independently and conditionally influence the outcome for a particular class. Nevertheless, this methodology has demonstrated inefficacy and reduced accuracy in cases where attribute interdependence is breached [199]. Vadapalli [209] provides an analysis of the advantages and disadvantages of Naive Bayes with notable challenges according to Frank [199] including the learner's inability to obtain potential hidden forms from the data and reduced efficiency when the NB is applied without considering feature dependency.

2.1.1 Types of Naïve Bayes classifiers

The Python sci-kit learn library offers various classifiers, including multiple options below [210]:

1. Multinomial Naïve Bayes: The system operates on multinomially distributed categorised data. Documents are categorised into foreign news, sports, politics, and religion. It arranges texts based on how frequently certain terms are used as characteristics.

2. Bernoulli Naïve Bayes: One of the most widely used models, it functions similarly to a multinomial classifier and uses Boolean variables with a 'Yes' or 'No' value as its predictors. Its main purpose is document classification.

3. Gaussian Naïve Bayes: The model assumes continuous data, rather than discrete values, which are samples from the Gaussian distribution, based on the normal distribution.

4. Complement Naïve Bayes: This Multinomial NB modification is designed to handle imbalanced data by determining model weights based on the complement of each class.

5. Categorical Naïve Bayes: This works best when the features are categorically distributed.

6. Weighted Naïve Bayes: The method employs domain-based weights to assign varying weights to different attributes based on their prediction ability, based on expert knowledge [204].

Ruan *et-al.*[211] proposed a method to improve attribute weighting for Naive Bayes text classifiers using the improved distance correlation coefficient. Their model incorporated deep attribute weighting by combining measurement of inverse document frequency and distance correlation coefficient, demonstrating that their attribute weighting method achieves an effective balance

between classification accuracy and execution time. Their work, however, did not address multi-class classification. Wang *et-al.* [212] proposed a universal Domain Adaptation (UniDA) method called Adaptive Unknown Authentication by Classifier Paradox (UACP) to adaptively identify target unknowns based on paradoxical predictions. A composite classifier was jointly designed with two types of predictors: a multi-class and a binary predictor. A weight-adaptive multi-factor authorisation technology to enhance network security is described in Zeng *et al.* [213]. In their work, two adaptive weight algorithms were designed to meet more precise authority control in complex network security scenarios and through the construction and testing of the actual prototype system, the utility and advantages of multi-factor and weight adaptation in authorisation were verified. Their work, however, mainly focused on multi-factor authentication. A weighted Naive Bayes classification algorithm with an Adaptive Genetic algorithm (AGA_WNB) to improve image classification accuracy using initial weights of features as the initial population and adjusted crossover and mutation probabilities based on fitness functions to optimise classification accuracy was proposed in [214]. Results showed that (AGA_WNB) outperformed other models, but their work, however, did not address multi-class classification. An adaptive multi-factor authentication system that selected multiple authentication modalities based on trustworthiness values in different environments, employing a multi-user permission strategy to dynamically select approvers based on the sensitivity of the requested information and the user's work environment, was proposed in [215]. Their work mainly focused on authentication in general. A feature weighting-based Naive Bayesian microblog user classifying method to distinguish between normal microblog and malicious microblogs users was proposed in Wang *et al.* [216], where the prior probability, the conditional probability, and the information gain of each feature were calculated. Their classification, however, was binary. An adaptive user authentication system that verifies user identity using different authentication steps based on a risk score was introduced in [217]. The adaptive user authentication system implemented a sequence of authentication steps based on a risk score to verify user identity. They did not address multi-class classification. An adaptively evidential weighted classifier combination method using basic probability assignment (BPA) modelling was proposed in [218]. They determined weights for individual classifiers based on the uncertainty degree of the corresponding BPA measured by belief entropy. Their work illustrated the effectiveness of the proposed weighted combination method through numerical experimental results.

2.2 Feature-based classification and prediction

Kharya and S. Soni [204] highlighted that not all medical symptoms are equally effective in predicting a specific disease and introduced the Weighted Naive Bayes Classifier (WNBC) framework, which assigns different weights to attributes based on their predictive abilities, and consulted with domain experts. Their experiment shows that the weighted Naïve Bayes method outperforms the Naïve Bayes method. Kumar *et-al.* [208] utilised contextual factors such as money, location, MAC address, and successful attempts to identify fraudulent activities in their Naïve Bayes-based mobile banking security system. Their algorithm accurately identified the behaviour of a new transaction and classified it as either normal or unusual. In Sari *et al.* [219], Naive Bayes and Mean of Horner's Rule were used to classify users based on their keystroke dynamics, discovering that this method yielded more precise outcomes than Naïve Bayes alone. In Blue *et al.* [220] the Naive Bayes classifier was used to estimate the likelihood of a digital identity characteristic being real based on the reliability of the sources used. They utilised various digital identifying sources, such as phone numbers, email addresses, first and last names, addresses, and account numbers, and demonstrated that the Naive Bayes theorem effectively predicts the reliability of an identity source. In [206] certainty factors and the Naive Bayes classifier were used to develop an expert system that could classify stroke illnesses with 96% accuracy. A 76% accuracy rate in user face detection for an attendance system using the Naïve Bayes algorithm was achieved in Rahman *et al*. [221] but background light impacted their prototype's accuracy. Because different qualities have different levels of relevance, Zhang *et al.* [222] proposed an Attribute and Instance Weighted Naive Bayes (AIWNB) that blends attribute and instance weighting. They estimated the weights directly using training data. The same authors in [223] proposed an attribute-weighted, fine-tuned NB model, emphasising the importance of accurate conditional probability estimates and eliminating the implausible attribute conditional independence assumption. For multi-class classification, Akkaya [207] conducted a comparative study of different classification algorithms on early diagnosis of heart diseases and could only classify data into three categories: "Normal," "Suspect," and "Pathological". Based on these findings, they concluded that Random Forests had the best accuracy and F-Score. A similar experiment by Jha *et al.* [224] on breast cancer and iris datasets found that the Random Forest algorithm outperformed the Decision Tree in binary-class classification, with CTree outperforming in multi-class classification. Their research underscored the importance of considering dataset characteristics and training-testing partitions in model evaluation for a specific

task. Using Browser fingerprints, Salomatin *et al.* [225], attempted to solve the adaptive authentication problem by employing Bayes theory and weighting, observing that weighting improves the accuracy of their algorithm. Wickramasinghe *et al.* [203] argued that despite numerous studies examining Naïve Bayes' robustness, no one has proven a necessary and sufficient condition for its behaviour. They contend that while conditional independence is a prerequisite for maximum performance, it is not sufficient. This review highlighted the potential for other researchers to utilise the Naive Bayes technique, so in the next section, we will look at the research methods.

3.0 Research methods

This section delineates the proposed methodology, data aggregation, preprocessing, sampling, and construction of machine learning models, encompassing the proposed user classification technique based on Naive Bayes. The probability of a login attempt being illegitimate is computed considering various contextual data, and the selection of Naive Bayes was predicated on the conditional aspect of the issue and its expeditious problem-solving capabilities in classification. To address biases with the traditional NB, we assigned weights to our attributes guided by the literature [161][204][223] and expert knowledge, as shown in Table 2, and the scoring was out of 10.

Table 4: Proposed Contextual Factors and their weights

Contextual Factor	Weight
Mobile Device	3
Other Device	1
Network	2
Location	3
Habit	1
Total	10

The Bayes theorem is shown below.

$$P\,(c\,|a) = \frac{P(a|c)P(c)}{P(a)}, \qquad (1)$$

where 'c' represents a class, 'a' represents attributes, P(c|a) is the posterior probability, P(a) is the prior probability, P(c) is the prior probability of the class and P(a|c) is the probability of the

predictor based on the class. The weighted NB introduced to overcome the conditional independence bias is represented as equation (2)

$$P(Y = y \mid X = x) = \hat{P}(Y = y) \times \prod_{i=1}^{n} [\hat{P}(X = x_i \mid Y = y)]^{wi} \quad (2)$$

Where P(Y=y|X=x) is the posterior probability or class probability, the probability of the target variable Y belonging to a specific class y, given the observed features X with their values x. *P^(Y=y)* is the prior probability representing the estimated or observed probability of a specific

class y occurring in the dataset before considering any of the input features. *X=x* represents the input features or predictors and is a vector of all the features used to make a prediction. *Y=y* is the class variable or target label we are trying to predict, which is the risk. $\prod i=1 \ \ n$ is the product operator, which indicates that we need to multiply all the terms that follow it, from i=1 to n. In this case, it multiplies the conditional probabilities of each feature. $P\hat{}(X=x_i/Y=y)$ is the conditional probability, meaning the probability of a single feature x_i having a specific value, given that the class is y. w_i denotes each feature weight. Since we believe contextual factors influence the final risk likelihood, we want to show how *wi* affects the final risk score. Since research shows that the feature weighting approach outperforms standard NB in many of the examined datasets [203][204], we need to see how the weighting in equation (2) affects user classification beyond binary. We conducted a comparative analysis between several variations of Naive Bayes and alternative multi-class classification approaches to assess their efficacy. To mitigate inherent biases in traditional Naive Bayes, we allocated weights to our contextual variables informed by scholarly works [161][204][223] and domain expertise. These weights serve as coefficients for contextual factors, which were then multiplied based on the deviation of a feature from known values. The weights displayed in Table 2, along with a 10-point scale, would subsequently undergo normalisation to a range between 0 and 1.

The following example demonstrates how each contextual factor's contribution would be calculated. It is assumed that there is a one-to-one mapping between a user and a mobile device; hence, a user is associated with one mobile device. Also, GPS or cell data provides location information for the user and the mobile device, along with the network that connects their device. As a result, if only for instance, the device changes, the probability of the user being illegitimate based on weight only is 3/10 = 0.3 and if location also changes, contribution becomes 3/10 + 3/10 = 6/10 = 0.6. The full weighted classifier now consists of weighted data assigned to each pair of

{attribute, value} giving each tuple a set $\{a_i, v_i, w_i\}$ where an attribute a_i has a value v_i and a weight w_i where $1<=w_i<=10$, for instance, for Mobile Device Change context, which has Operating System and Browser as attributes, is expressed as follows:

$$\{a_i, v_i, w_i\} = \{\text{Mobile Operating System, Android, 1.5}\} \quad (3)$$

$$a_i, v_i, w_i\} = \{\text{Mobile Browser, Opera, 1.5}\} \quad (4)$$

$$=>\{a_i, v_i, w_i\} = \{\text{Mobile Device Change, Yes, 3}\} \quad (5)$$

The proposed solution was tested on a Windows 11 computer with an Intel Core i7@1.30 GHz processor and 16 GB RAM using Python 3.10.9 and Jupyter 6.5.2. Synthesised data was merged from various sources, including Datasets [226][227][228] due to the scarcity of datasets related to adaptive authentication. Following equation (2), our work employed the chain rule, which can be expressed as equation (6):

$$P(A_1, A_2, \ldots, A_n) = P(A_1)\, P(A_2|A_1)\, P(A_3|A_1, A_2) \ldots P(A_n|A_1, A_2, \ldots, A_{n-1}) \quad (6)$$

In equation (6), we have the formula for the joint probability of events $A_1, A_2, \ldots, A_n$, where our predictors were Mobile Device, Other Device, Location Change, Network Change, and Habit Change, with a change in any of these weighted predictors affecting the risk probability. The risk score or probability is the dependent variable, as depicted in Figure 2.

3.1 Data collection

We used synthesised data, as previously described, which included 15 features with 3,000 records. Figure 2 shows the independent and dependent variables.

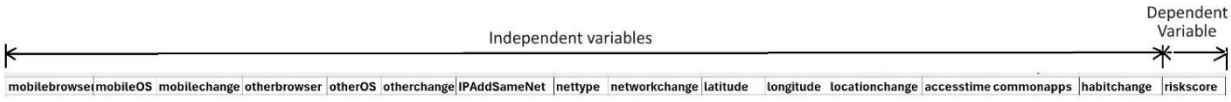


Figure 8: Independent and dependent variables in risk calculation

We used feature weightings explained in Table 2 to apply several Naive Bayes variants based on the dataset, and we compared the outcomes with other multi-class classification techniques.

The description of the data is in Table 3 below.

Table 5: The risk calculation dataset attributes detailed information

Sno	Attribute	Description	Values/Range
1.	Mobile Browser	The browser of the user's mobile phone	0 for Chrome, 1 for Opera,2 for DuckDuckGo, 3 for Firefox, 4 for Microsoft Edge,
2.	Mobile OS	Mobile phone Operating System	0 for Android, 1 for Tizen, 2 for iOS, 3 for Windows
3.	Mobile Device Change	Describes status of mobile device	0,1 for No and Yes
4.	Other Browser	Other Device browser	0 for Google Chrome, 1 for Brave, 2 for Apple Safari,3 for Firefox, 4 for Microsoft Edge
5.	Other OS	Other Device Operating System	0 for Windows 10, 1 for Linux Ubuntu, 2 for Windows 11, 3 for Mac OS, 4 for Windows 8
6.	Other Change	Other Device change	0,1 for No and Yes
7.	IP Add Same Network	Known IP Address	0,1 for No and Yes
8.	Network Type	Describes an unknown IP Address	0,1 for WiFi and Mobile
9.	Network Change	Change in the user device's network	0,1 for No and Yes
10.	Latitude	Describes latitude	0,1 for known latitude and unknown latitude
11.	Longitude	Describes longitude	0,1 for known longitude and unknown longitude
12.	Location Change	Change in location	0,1 for No and Yes
13.	Common Apps	Apps commonly used by user on the device	0 for TikTok, 1 for Facebook, 2 for SnapChat, 3 for Instagram, 4 for WhatsApp, 5 for Telegram
14.	Access Times	Usual time apps are accessed by the user	0 for 2:00, 1 for 6:00,2 for 8:00,3 for 9:00,4 for 10:00,5 for 11:00, 6 for12:00,7 for 14:00,8 for 18:00
15.	Habit Change	Change in user habits	0,1 for No and Yes
16.	Target	Categories/classes of risk	0 for Accept, 1 for Very Low, 1 for Low, 2 for Medium, 3 for High, 4 for Deny

3.2 Data pre-processing

Data pre-processing is essential to prevent misleading results due to outliers, redundant values, or missing values, and must be completed before analysis [229][230][231]. This guarantees that a reliable machine learning model is tested. Different sources' data may not be suitable for analysis due to variations in formats, missing values, or outliers. Consequently, we examined the dataset for any missing values, noisy data, or outliers, and eliminated them. We employed tools like scalers

to eliminate outliers from numerical data and hot encoders to encode categorical data, which we then replaced with encoded data.

2.2.1 Data merging

We combined multiple datasets to create a single dataset that combines weighted and non-weighted risk calculations for authentication.

3.2.2 Data cleaning and handling

This step involves removing, altering, or replacing problematic data from a dataset or record, as well as identifying incomplete, erroneous, incomplete, or irrelevant data portions [229][230]. Our instance had categorical and numerical data that required multiple strategies, despite no missing data.

3.3 Feature Selection

The initial cleaning phase involved removing irrelevant features, such as MAC Addresses to maintain 15 features.

3.4 Data Splitting

The study utilised stratified sampling to divide data into two sets: a training set and a testing set. The initial 80:20 ratio was utilised, with 3,000 records used, where 2,400 were for training and the remaining 600 for testing.

3.5 Classification

The research performed user multi-class classification for authentication using Naïve Bayes classifier and its variations on the weighted and unweighted datasets. Other multi-class classification algorithms, which include Decision Trees, ADABoost, Random Forest, XGBoost and Support Vector Machine, were also employed in testing the classification model. The experiment assessed the algorithm's ability to categorise risk probabilities into the six classes expanding from two classes by Kumar *et al.*[205], Khusnul *et al.* [206], Akkaya and Soni [207] and three classes by Mohammed Misbahuddin *et al.* [161]. The devised classes are listed in Table 4.

Table 6:Security meanings of the 6 risk classes of proposed scheme

Probabilities	0.0<=x<0.1	0.1<=x<0.2	0.2<=x<0.4	0.4<=x<0.8	0.8<=x<0.9	1
Meaning	Allow	Very Low	Low	Medium	High	Deny

Normal scores are defined as 0-0.09, requiring no further authentication, while scores between 0.9-1 are considered unacceptable and rejected. A single authenticator can be used for low-risk probability authentication, but as the risk probability increases, the difficulty of authentication shifts from single to multifactor. Table 5 presents a detailed risk classification for scores between 0 and 1 in the proposed multi-class classification.

Table 7: Proposed risk probability classes

Probability range	**Classes**	**Numbers**
'0' if 0.0<=x<0.5 else '1'	0,1	2 Classes
'0' if 0.0<=x<0.1,'1' if 0.1<=x<0.9 else '2'	0,1,2	3 Classes
'0' if 0.0<=x<0.1,'1' if 0.1<=x<0.5, '2' if 0.5<=x<0.9 else '3'	0,1,2,3	4 Classes
'0' if 0.0<=x<0.1,'1' if 0.1<=x<0.3, '2' if 0.3<=x<0.6 ,'3' if 0.6<=x<0.9 else '4'	0,1,2,3,4	5 Classes
'0' if 0.0<=x<0.1,'1' if 0.1<=x<0.2, '2' if 0.2<=x<0.4, '3' if 0.4<=x<0.8 '4' if 0.8<=x<0.9 else '5'	0,1,2,3,4,5	6 Classes

4.0 Results

The study evaluated various classifier types, including Gaussian, Categorical, Bernoulli, Hybrid, and other multi-class classification algorithms. Weighted and unweighted datasets were used to execute classification algorithms, and the outcomes were compared and evaluated using weighting and unweighting method. Figure 3 displays a risk score graph based on various weightings, with RiskScore3 being a result of unweighting contextual factors.

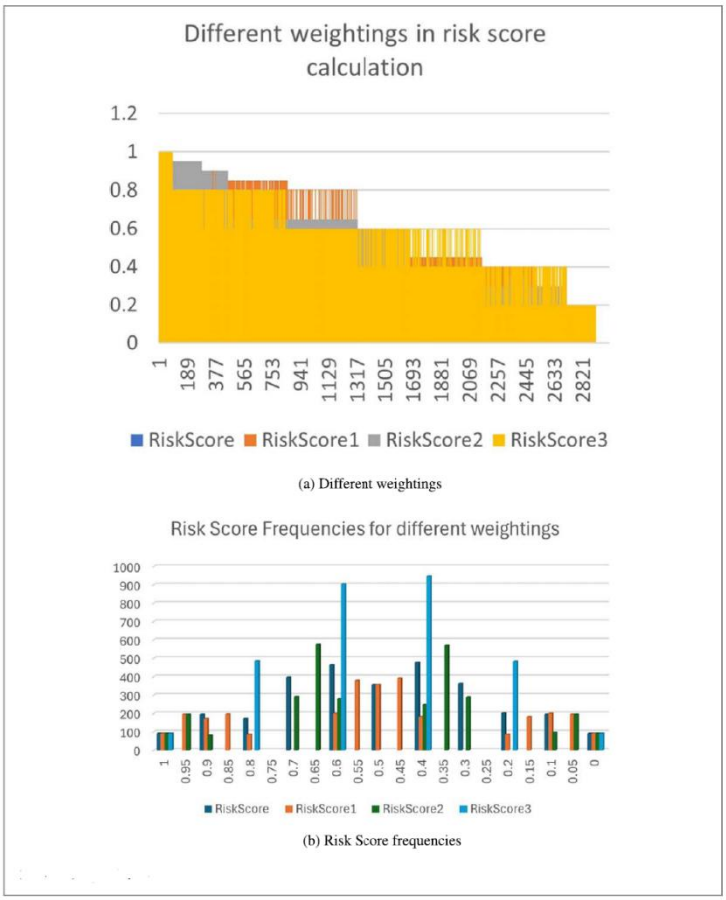


Figure 3:Weighted and unweighted context for risk score calculations

As shown, the shapes of the graphs vary with weights, and the unweighted risk score leads to generalised outcomes, introducing bias, which we aim to minimise. The unweighted approach may have adverse effects on user classification and handling during authentication, potentially resulting in their grouping together. A correlation matrix with a dendrogram overlay was created to demonstrate the similarity in correlation between contextual factors and results across weighted and unweighted datasets. Figure 4 shows the matrix.

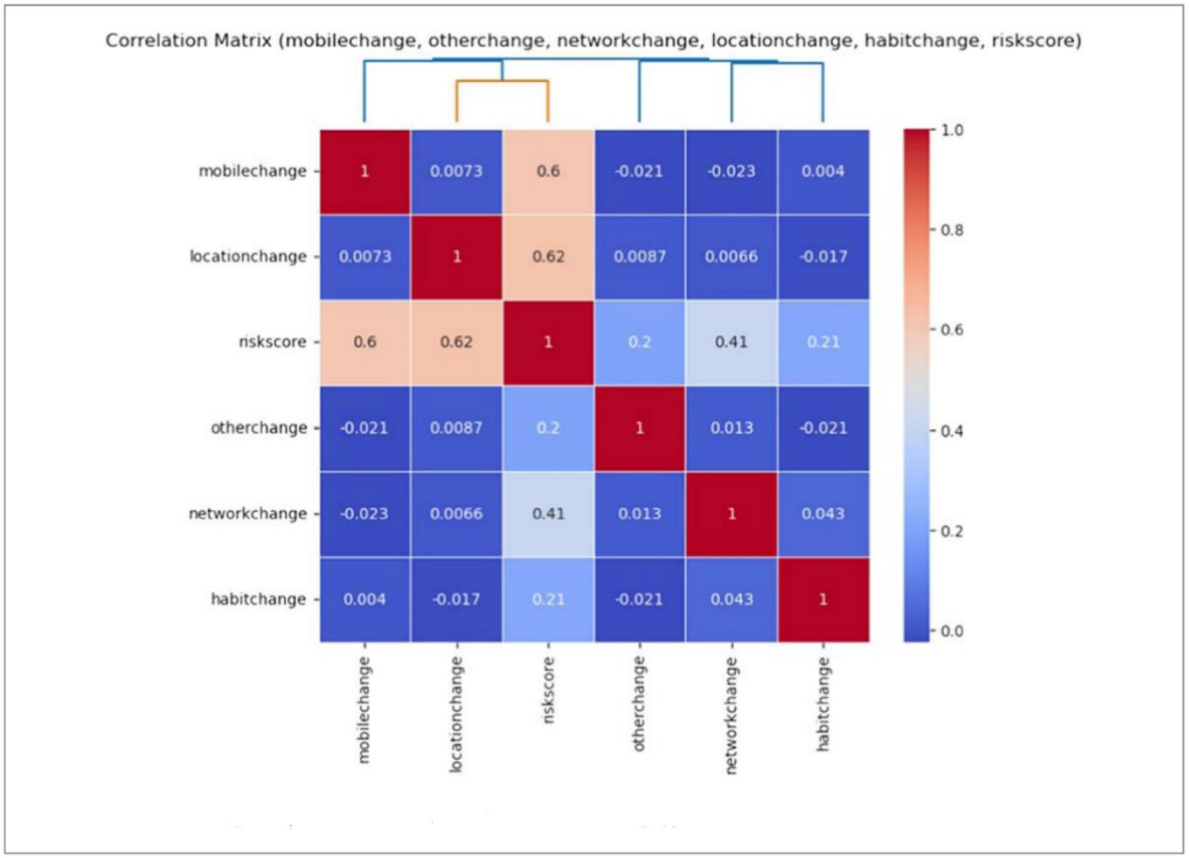


Figure 4:Correlation matrix of contextual factors contributing to final risk score

The data reveals minimal negative correlations, indicating that despite their weak nature, these correlations do not consistently recur, hence they cause minimum problems. Figure 5 displays the evaluation results of our algorithms' performance on weighted contextual features using the GaussianNB and CategoricalNB classifiers.

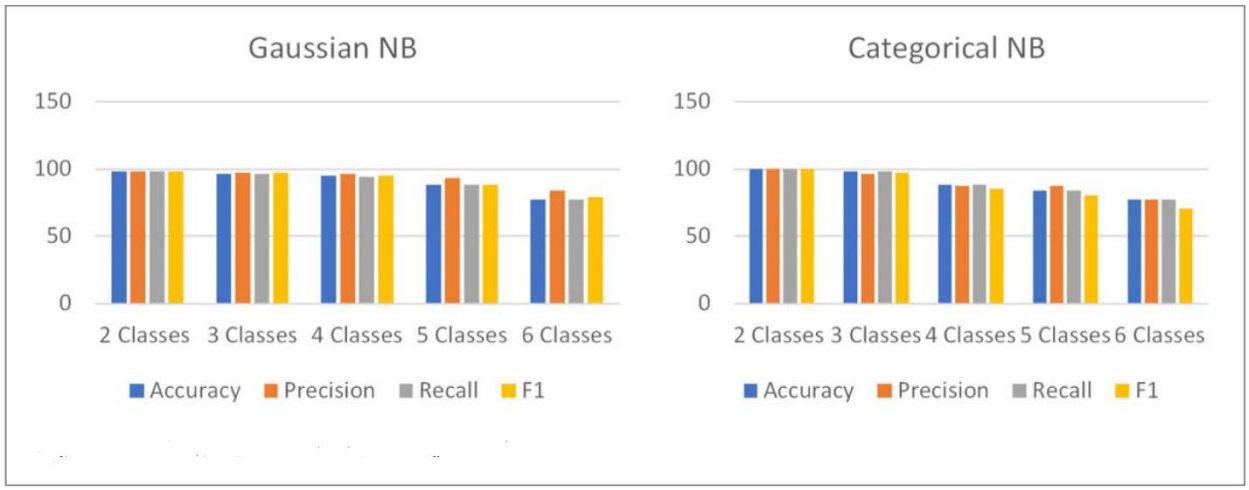


Figure 5: Weighted GaussianNB and CategoricalNB classifiers

It can be observed that there is a decrease in accuracy as classes go beyond three. Figure 6 shows the performance of the BernoulliNB and the first mixed approach, where Gaussian and CategoricalNB were mixed at once.

Figure 6:Weighted BernoulliNB and Mixed approach

A decrease in performance accuracy can also be observed as classes go beyond three. Figure 7 below shows the weighted mixed second approach.

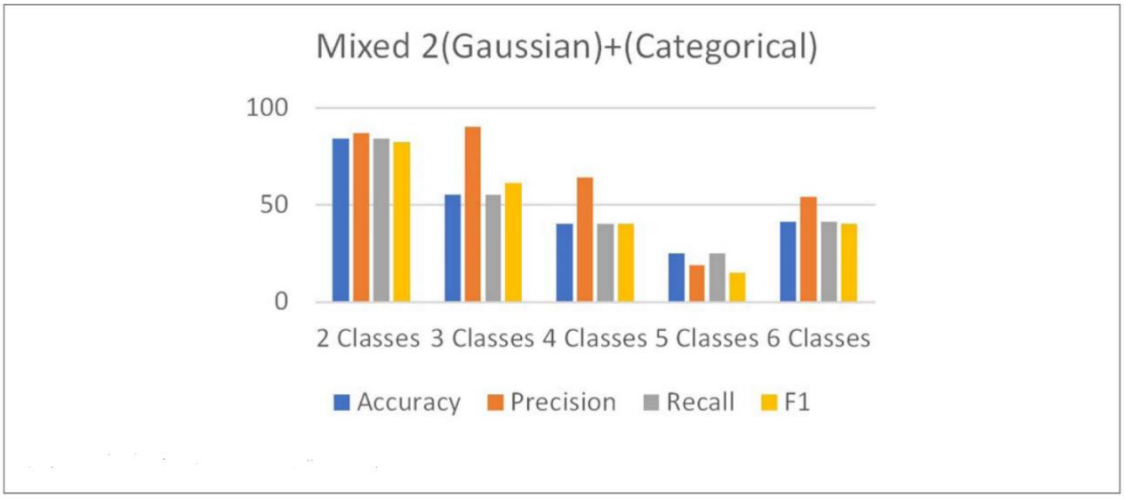


Figure 7:Weighted second mixed approach

This method involves using both approaches separately and performance can be observed to degrade starting at three classes. Results demonstrate that the Bernoulli model exhibits a slightly superior performance than the Gaussian and Categorical models for up to four classes with accuracy rate as low as 83%. The same observation extends to metrics such as precision, recall and F1-score. Conversely, the mixed methodologies yielded reduced accuracy in classification tasks relative to the aforementioned techniques. The evaluations considered the premise that the suitability of algorithms is contingent upon the nature of the dataset. The preference of a weighted

approach was justified by its consistently enhanced outcomes compared to the unweighted approach. The results of their comparisons are shown in Figure 8.

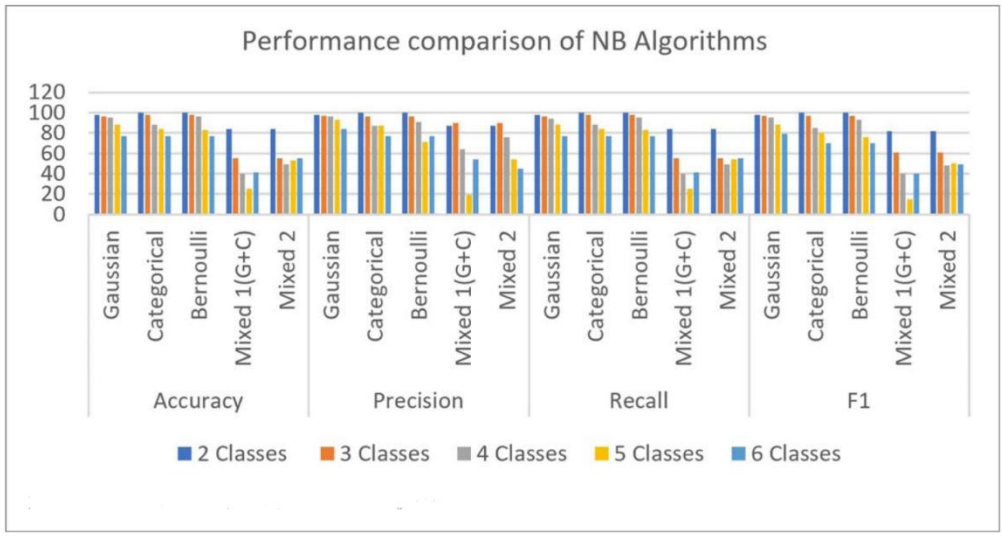


Figure 8:Comparison of NB algorithms on weighted dataset

Methodologies that combine different approaches showed decreased effectiveness compared to using individual methods, wherein Gaussian, Categorical, and Bernoulli strategies demonstrated similar levels of performance. The slight variations observed could potentially be linked to the inherent characteristics of the dataset, given that each algorithm presents unique strengths over the others. Overall performance tended to decrease as the number of categories increased. The investigation juxtaposed the outcomes of Naive Bayes multiclassification techniques against alternative algorithms, as illustrated in Figure 9.

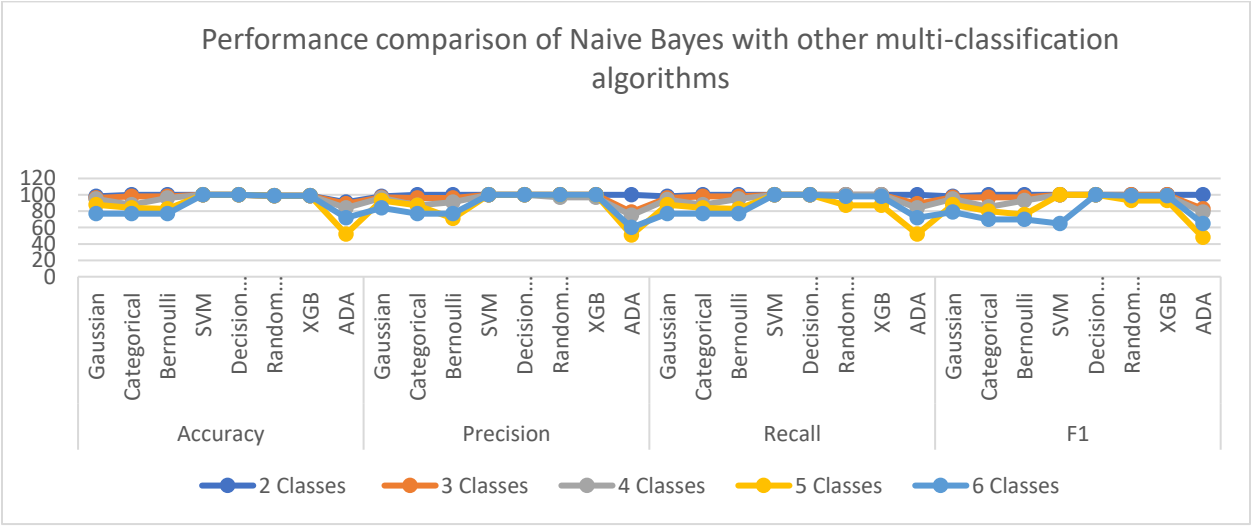


Figure 9: Performance evaluation of different multi-class classification algorithms

Decision Trees and Support Vector Machines (SVM), followed by Random Forests and XGBoost (XGB), demonstrated strong performance across all metrics when compared to Gaussian, Categorical, and Bernoulli algorithms. Conversely, ADA yielded lower performance than the other models. Despite exhibiting acceptable accuracy, Naïve Bayes algorithms did not perform as well as the alternative multi-class algorithms. A five-fold cross-validation was conducted to evaluate the model's performance across different data splits. The model's performance was assessed using 80:20, 70:30, and 60:40 data splits. The performance of the model in various machine learning multi-class classification scenarios using these splits is illustrated in Figure 10.

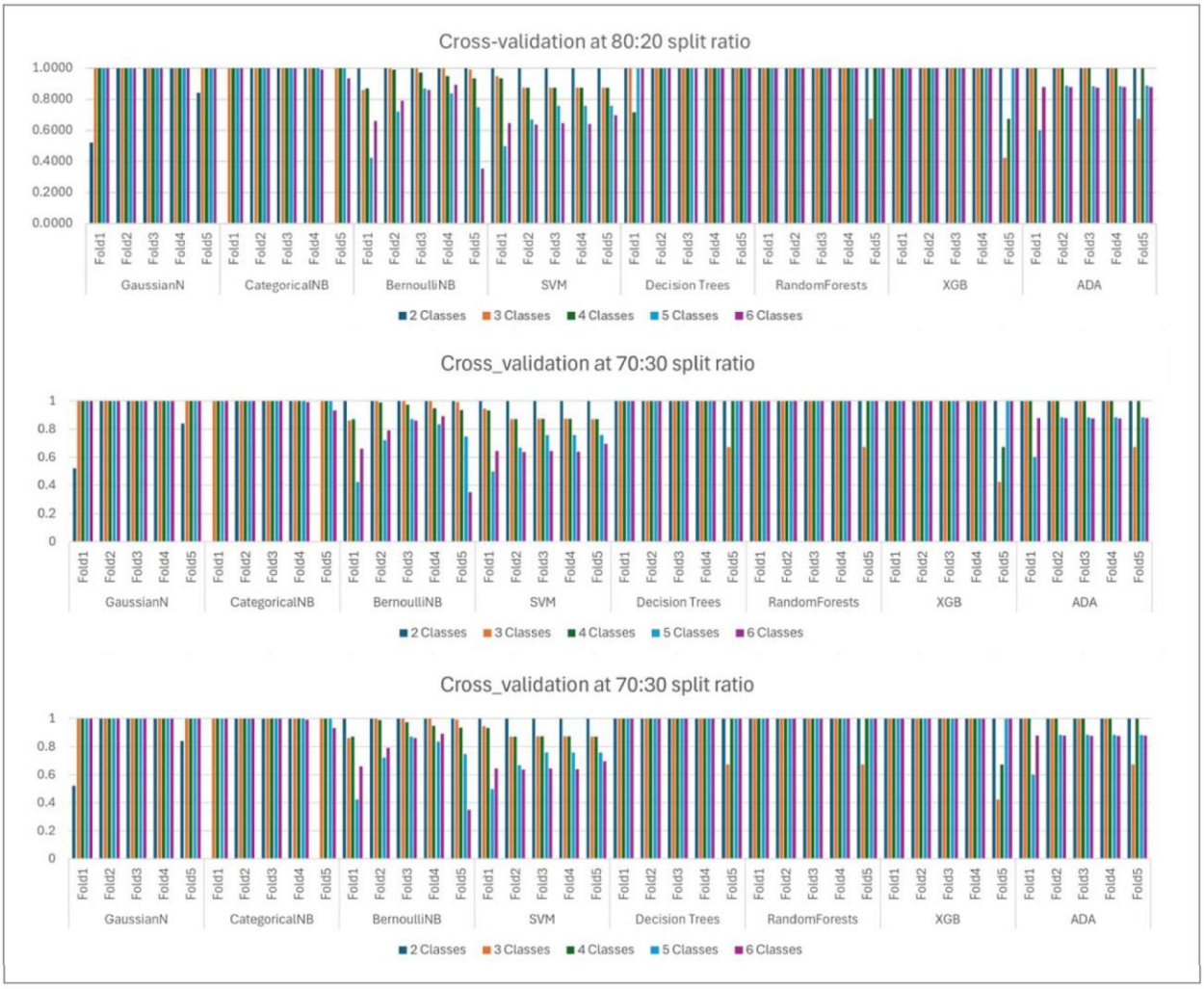


Figure 10: Performance evaluation of different multi-class classification algorithms

We created Figure 11 to illustrate how our algorithms' performance varies with changes in the number of classes in order to assist in explaining the discrepancies.

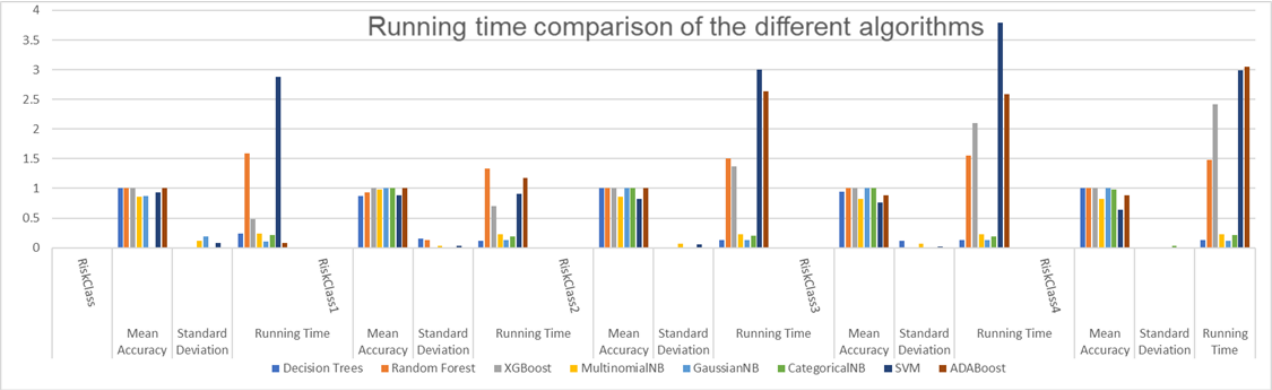


Figure 11: Running time evaluation of different algorithms

4.1 Discussion

The weighting in Table 2 proved to significantly impact the overall risk score and classes, thus enhancing the accuracy of classification models. The study tested various Naive Bayes classification methods using both weighted and unweighted training data, confirming the findings in Zhang *et al.* [222]. The study aimed to evaluate the performance of both methods beyond three classes, and the heatmap reveals a positive correlation between variables, except for mobile device and habit changes. Positive correlations have advantages that include increased risk prediction accuracy, enhanced authentication decision-making, improved usability, reduced false positives/negatives, and better adaptation to dynamic environments [231]. It is, however, worth noting that the correlation does not imply causation [232]. The study classified authentication into six classes, but there was degradation beyond four classes, which may explain why previous studies focused on models for three classes. The accuracy of NB variants and ADA increased up to three classes before declining. When more than four classes were involved, Naïve Bayes classifiers were found to produce less accurate results than other multi-class algorithms that did not depend on the number of classes. Algorithms like Decision Trees, Random Forests, and Support Vector Machines can flexibly model dependencies and interactions between variables, do not assume feature independence, have greater flexibility in model structure and parameterisation, are robust to imbalanced data, and have performance optimisation capabilities [233]. The Non-Naïve Bayes algorithms outperform other classification algorithms up to six classes. The (80:20) partition outperformed the other (70:30) and (60:40) partitions, confirming a claim by [224] that partitions significantly influence algorithm accuracy. The weighted version outperformed the unweighted version in confirming assertions made in [199][203][204][222][224]. The hybrid Naive Bayes method, which combined continuous and categorical data for training, produced more

accurate results on weighted data but generally had poor performance. The study, therefore, concludes that weighting enhances performance. The unweighted approach assumes equal weights for all attributes, leading to biases in risk scores, with odd numbers 0.3,0.45 being omitted. Akkaya [207] indicates that the type of data significantly impacts the performance of an algorithm. For example, if the data is categorical, CategoricalNB will obviously outperform other algorithms, and vice versa. The ADABoost algorithm performed poorly, with an average accuracy of 74.25%, but tuning could potentially improve its performance. On the other hand, the cross-validation using splits did not have a significant effect on the performance of our model, as can be observed in Figure 10. BernoulliNB, SVM, and ADA performed significantly less than the rest as the classes increased. Decision Trees, Random Forests, and Naïve Bayes variations GaussianNB and Categorical NB, performed well above three classes, thereby cementing our conclusion on the suitability of the non-Naive Bayes algorithms for multi-user classification. When mean accuracy was compared, as shown in Figure 11, the tree-based models (Decision Trees, Random Forest, and XGBoost) surpassed the others with perfect accuracy for binary and three classes, holding up well in several risk categories. However, several models show a decline in accuracy for five and six classes, suggesting that the classification issue for these categories might be more complicated, either as a result of feature scarcity or class overlap. Efficiency-wise, AdaBoost is a great option when efficiency is crucial because it stands out for having a shorter running time while retaining a high level of accuracy. The Naive Bayes variants show low running times compared to other models, indicating speed and probably simplicity. The study supports Brownlee [192] who claim that there's a limited theory for mapping algorithms to different problem types, suggesting controlled tests as the most effective approach in classification predictive modelling evaluation. The Naive Bayes method, even though it performed worse than alternative algorithms, is frequently used because of its simplicity and speed, as demonstrated in Figure 11 by low running time, validating [233][234], usefulness as it worked well in our case, thereby supporting [235][236], interpretability, which comes from the ease of understanding the model and result, and efficiency measured from a running time point of view, which is what we desire.

5.0 Conclusion and future work

Our research primarily focused on implementing Naïve Bayes to address user classification problems in risk-based authentication. Binary user classification is frequently used to categorise

users as valid or not, and other multi-class classifications go up to three classes [207]. However, two or three classes of users can only generalise authentication, limiting the usability of security solutions. The study proposed categorising user risk scores into six classes, with extreme classes indicating zero and one and the remaining four classes occupying the middle. The multi-class classification aims to contribute to improved usable security by adjusting authentication difficulty based on risk score. We tested both weighted and non-weighted features on various Naive Bayes algorithms on a synthetic dataset, and the weighted technique outperformed the unweighted technique, which was the overall finding across all experiments. Generally, Naïve Bayes classification algorithms' effectiveness peaks at three classes, and as class sizes increase, accuracy declines. The study also compared Naïve Bayes with other machine learning algorithms for multi-class classification, finding that SVM, Decision Trees, Random Forests, and XGB outperformed Naïve Bayes. Evaluating an algorithm using appropriate data is crucial, as different algorithms perform differently with different data, as per Ray [210]. The Gaussian, CategoricalNB, and Bernoulli algorithms performed almost similarly in the general comparison, but upon five-fold cross-validation, the BernoulliNB performed poorly. In conclusion, when compared to other multi-class algorithms, our model properly categorises users with a higher level of precision when utilising non-Naïve Bayes algorithms, namely DT and RF. GaussianNB and categoricalNB also performed well in both general comparison and cross validation. Cross-validation gave us an insight into the performance of our model as it complimented the initial performance comparison that we made, thereby reducing bias. Since not all iterations of the classification algorithm perform poorly, it is acceptable to say that some of the shortcomings of the Naive Bayes algorithm are reached from a generalised point of view. The results indicate that the Naïve Bayes rule can be used for risk calculation while other machine learning algorithms can be employed for user classification. As illustrated in Figures 5 to 9, the Naïve Bayes algorithms did not perform as well as the alternative multi-class algorithms despite displaying acceptable accuracy, but these findings explain the algorithm's interpretability and simplicity, as it can be understood on a modular level shown in Figure 4, and Table 3 to 5, demonstrating how each feature contributes to a class prediction. The probabilistic model is easy to explain and understand. Because of the Bayes theorem and the feature independence assumption, this algorithm is simpler to implement than other algorithms that are more complicated because of their underlying mathematical models, optimisation procedures, or architectural designs. Particularly during training, the algorithm runs quite quickly, and because it simply needs to calculate probabilities from the training data, the

Naive Bayes algorithm is fast and computationally efficient, supporting [233][234]. Large datasets, however, are where their speed is most noticeable [237]. Its efficiency is shown in Figure 10, where the GaussianNB and CategoricalNB compete with other Machine Learning multiclassification algorithms. The Naive Bayes doesn't need to store a lot of data in memory and has less computational overhead. Because it believes that features are independent of one another, the Naive Bayes method performs poorly in situations where the features are heavily correlated. It is therefore most appropriate for classification problems involving categorical features [238]. As can be observed in Figure 4, there is little correlation, indicating that the algorithm performs well in our multi-classification scenario. Based on the results in Figure 11, future work may involve looking at the characteristics that lead to the incorrect classifications in five and six classes through examining the model's feature relevance. The weights for our contextual factors will also be automatically determined in future work using machine learning-based techniques, which can improve risk assessment by learning the ideal weights from data. Tree-based models like Random Forests and Gradient Boosting Machines (e.g., XGBoost, LightGBM) and Genetic Algorithms will be used together with the Lasso Regression that has a penalty for the magnitude of coefficients. Feature engineering may also be tried in the future to distinguish between classes where performance is lower. It is also necessary to try an ensemble approach that combines several models' predictions to increase robustness. Fine-tuning attributes and weighted techniques in Android app construction, detecting context through device sensors, and assigning authenticators based on risk scores are also our future work. The app's deployment aims to collect complete data on user context and authenticators, as complete data is challenging to obtain. The solution's usability is expected to enhance security adherence, and full deployment will evaluate the model's viability for diverse users with diverse medical conditions that affect their use of authenticators.

Part III-A

PART III-A

An Android-Based Internet of Medical Things Adaptive User Authentication and Authorisation Model for the Elderly

Part III-A is published as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma. An Android-Based Internet Of Medical Things Adaptive User Authentication And Authorisation Model For The Elderly, J.Cybersecur. Priv. **2024**, 4, 993–1017.
https://doi.org/10.3390/jcp4040046

An Android-Based Internet of Medical Things Adaptive User Authentication and Authorisation Model for the Elderly

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, and Frederic Nzanywayingoma

Abstract

Globally, 77% of the elderly aged 65 and above suffer from multiple chronic ailments, according to recent research. However, several barriers within the healthcare system in the developing world hinder the adoption of home-based patient management, hence the need for the IoMT, whose application raises security concerns, particularly in authentication. Several authentication techniques have been proposed; however, they lack a balance of security and usability. This paper proposes a Naive Bayes based adaptive user authentication app that calculates the risk associated with a login attempt on an Android device for elderly users, using their health conditions, risk score, and available authenticators. This authentication technique guided by the MAPE-K_{HMT} framework makes use of embedded smartphone sensors. Results indicate a 100% and 98.6% accuracy in usable security metrics, while cross-validation and normalization results also support the accuracy, efficiency, effectiveness, and usability of our model with room for scaling it up without computational costs and generalising it beyond SSA. The post-deployment evaluation also confirms that users found the app usable and secure. A few areas need further refinement to improve the accuracy, usability, security, and acceptance but the model shows potential to improve users' compliance with IoMT security, thereby promoting the attainment of SDG3.

1.0 Introduction

Around 77% of the global elderly population, aged 65 and above, suffer from chronic diseases like stroke, hypertension, asthma, diabetes, and cognitive impairment [239]. In the United States, 95% of individuals over 60 years old suffer from at least one chronic illness, while 80% grapple with multiple conditions [240]. Even the elderly population in Sub-Saharan Africa (SSA), comprising 3.06% of the overall population [85][241], is vulnerable to health-related issues. At the same time, the provision of basic, high-quality, and affordable healthcare has posed a universal dilemma. The growing elderly population significantly impacts their societies and families [85][242], and inadequately staffed healthcare facilities pose challenges in accommodating all patients [243]. The recent COVID-19 pandemic has accelerated the adoption of home-based care [244][245], prompting the integration of IoMT to support healthcare stakeholders both within and outside healthcare settings. The progression of sensor technologies and mobile devices has accelerated the adoption of the IoMT [128] with smartphones being integrated into the IoMT for telemedicine applications due to their affordability and sensor availability, enabling non-invasive vital parameters monitoring, communication, and healthy behavior encouragement. However, the implementation of the IoMT faces challenges concerning the privacy and security of patient data [128][158][246][247]. Generally, IoT systems cater for both technical and non-technical users [248], but most end users, including elderly individuals, lack technological proficiency and are unlikely to implement security measures, making them susceptible to potential attacks [249]. At the same time, the development of security protocols often fails to account for the health issues prevalent in older populations [103][250],but when it comes to authentication, elderly users have their authenticator preferences [251]. Although smartphones are commonly utilized for authentication purposes, there is little empirical support regarding their effectiveness across various age demographics, including the elderly [242]. Despite ongoing research on suitable authentication techniques [239], there is a lack of extensive research on the practicality of authentication technologies for senior citizens and individuals with disabilities [252]. Most previous research has either focused on device authentication [116], security without usability and vice versa [118][119][253], physiological authentication [121], health monitoring and well-being only, and does not consider user age. As a result, there is essentially a dearth of research on IoMT user authentication that takes into account senior users' capabilities. Since smartphones are widely used devices that people of all ages can use for communication and other purposes, they make

good candidates for use in IoMT authentication. Therefore, research on smartphone-based user authentication mechanisms for the elderly is crucial.

This research aimed to improve usable security by developing and implementing an Android-based adaptive authentication system for elderly IoMT users.

The primary objectives were as follows:

(i) Develop a Naive Bayes Android-based adaptive authentication model for IoMT hardware and software that considers elderly users' medical conditions and risk scores for suitable authenticators.

(ii) Assess the effectiveness of the proposed model in authenticating elderly users.

The selection of an Android device was predicated on its widespread availability in the SSA region, with a substantial market share of 83.6%, in stark contrast to Apple's 14.35% [254]. Our proposed work is novel in that it leverages users' existing technology to authenticate them, taking into account their age, medical condition, risk score, and available authenticators to ascertain the level of difficulty of their authentication procedure based on their updated trust score. Most previous works have yielded solutions that have not been practically tested. We anticipate that this research will lead to increased user authentication compliance, which will encourage the usage of the IoMT and, in turn, encourage the use of technology to help achieve Sustainable Development Goals (SDG3), which are to improve the health and well-being of all people, regardless of age. In contrast to behavior based authentication, which primarily entails continual authentication that is difficult and expensive for elderly users, this effort concentrates on physiological-based authentication and initial login. This is because even though there exist hands-free, one-time, continuous authentication schemes [255-261], they come with additional hardware and require more movements among the elderly, thereby increasing cost and inconvenience.

2.0 Analysis of Various Authenticators

Despite widespread recognition, there is a lack of proactive measures to address emerging threats on IoMT devices, hindering the implementation of effective mHealth applications. Around 60% of smartphone users do not use security measures, and mobile platforms often use explicit authentication [178]. Elderly individuals with chronic conditions like arthritis, Parkinson's, and osteoporosis face challenges in utilizing some authentication systems [178], making them more

susceptible to security breaches [255]. Authentication is a critical component in maintaining network security [256], acting as the first line of defense against potential attacks. Multi-factor authentication (MFA) combines knowledge-based, physiological, and behavioral candidate authenticators, requiring attackers to have to break another barrier if one factor is compromised [142]. Figure 1 shows examples of factors used in MFA.

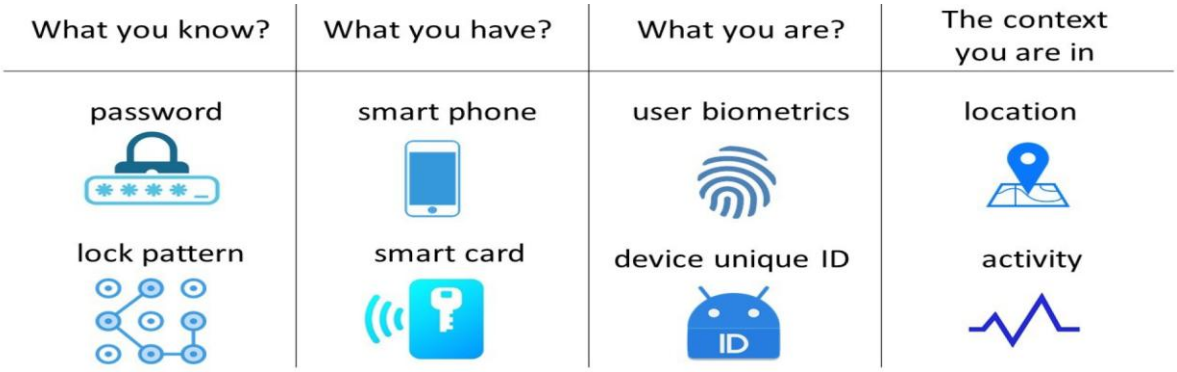


Figure 1:Examples of factors used in MFA. Reproduced with permission from Hazratifard et al. [128]

We now examine the appropriateness of the following authenticators for elderly users.

2.1 Knowledge-Based Authenticators

2.1 Knowledge-Based Authenticators

2.1.1 Personal Identification Number (PIN)

A PIN is an old, secure, maskable, and quick authentication method that uses a combination of four or six numbers [177]. It is liked by the elderly [251], can defeat shoulder surfing, but is easily forgotten, making it less suitable for the elderly.

2.1.2 Textual Password

This old authentication mechanism, which can contain special and alphanumeric symbols, is more resistant to brute-force attacks than PINs [257]. However, elderly individuals often struggle with password input due to arthritis, early-stage dementia [242], deteriorating vision [258], frustration [177], and lack of prior technology exposure [259].

2.1.3 Graphical Password

Images, instead of alphanumeric characters, are utilized for memory stimulation and are easier to remember than text [177], making them more accessible to elderly users.

2.1.4 Face Recognition

Faces serve as a verification system for senior citizens, allowing easier memory retention and selection from a set of saved faces.

2.1.5 Pattern Lock

Users draw recognizable patterns on a three-by-three grid, which is usable and less time-consuming than a PIN but may be frustrating for dexterity-deficient adults [177] and susceptible to side-channel attacks. Fingertips can leave a distinctive trace on the screen.

2.1.6 Musipass

Musipass is easy to remember, allows users to choose their preferred music as their password [259], but may not be suitable for elderly individuals with typing difficulties.

2.2 Biometric Authenticators

Biometrics identify living individuals by utilising physiological attributes as well as behavioral traits for accurate individual authentication [130]. Biometric traits are widely used as authenticators in mobile devices combining the "what you have" and "what you are" dimensions [128]. Of late, most IoT devices are improving their sensorial abilities, enabling user data collection for authentication [128], with success significantly influenced by user experience [260].

2.2.1 Physiological-Based Biometric Authenticators

Machine vision and sensor-based techniques are used in human motion behavior feature extraction; the former is difficult and subject to environmental influences, while the latter is inexpensive and not affected by them [243].

Fingerprint/Palm

Although older users prefer fingerprint authentication, they are less likely to successfully authenticate using it. Off-the-shelf smart devices now offer scanner capture technology [144][131], but factors like aging, moisture, gender, medical, and occupation can hinder its effectiveness [260].

Ocular/Eye Scanner Scanning

The eye, through the iris or retina can be used for authentication. The scanner is costly and less common, and its authentication process may be impeded by factors like spectacles [144], age, and environmental light intensity [260].

Voice Recognition

Most devices come with built-in microphones that can be utilized for voice capture and authentication. The user's state or age can significantly impact the outcome of voice capture, potentially leading to a denial of service. Despite being user-friendly, they are more susceptible to spoofing attacks than facial recognition systems [144], so they must be combined with other authenticators to enhance security.

Facial Recognition

This camera-based technique compares a user's image with the database but requires good lighting and is not suitable for low-cost wearable devices [244]. Factors like glasses, facial expressions, age, poses, and lighting influence results [242].

2.2.2 Behavior-Based Authentication

These models use machine learning (ML) to authenticate users by learning their previous access patterns. This authentication mechanism is beneficial for tracking user behavior over a specific period [240] but requires time to observe, and algorithm design is complex. Older individuals' use of behavior is difficult to capture due to their limited activities. Examples of authentication mechanisms are explained below.

Gait-Based Authentication

Modern mobile devices can effectively capture gait patterns for authentication [85], but older adults face more challenges due to walking challenges [242].

Heart Rate Biometric Identification

Heart rate signals are unique and consistent over time [243], and while smartphones with integrated sensors offer heart rate biometric authentication, research on its use in elderly individuals is still limited.

2.3 Smartphones and Wearables

Wearables have gained popularity for their use in health monitoring and authentication. However, most health-related signal proposals are based on high-end medical equipment datasets that may not accurately represent widely available devices. Smartphones and tablets are popular portable devices in the IoT [244], although they are not always considered essential components. They have the expected capabilities of the traditional IoT, and they interact with IoT devices.

2.4 Adaptive Authentication

Adaptive security is a self-monitoring security method that prevents network attacks by altering its behavior and controlling the conditions under observation [245] reducing the monotonous selection of the same authentication factors and identifying risks more effectively than the one-size-fits-all approach [128].

Risk-Based Authentication

This is an adaptive authentication method that calculates user activity risk using contextual and historical data, calculating the risk score in real time using specific rules [241]. There has been a lot of research on adaptive authentication, but not much of it has produced real-world, workable solutions [241].

2.5 Authentication and Authorisation Attacks in the IoMT

Because health data are sensitive and IoT device environments are resource-constrained, authentication and authorisation attacks in IoMT present serious security risks, particularly in smart-home applications [268-270]. Although security protocol developments are encouraging, continuous research and adaptation to new threats are necessary due to the dynamic nature of the IoMT. As a result, numerous strategies continue to be explored to mitigate these risks. IoMT devices are vulnerable to denial-of-service and man-in-the-middle attacks, which could jeopardise patient data and device functionality [85]. Physically Unclonable Functions (PUFs) are one type of authentication mechanism that can be cloned by ML-based modeling attacks, granting unauthorised access [242], but by incorporating ML techniques into authentication and authorisation procedures, the unique challenges presented by IoMT networks can be addressed and attack resistance can be increased [243]. Biometric Authenticated Key Exchange (BAKE), one of the lightweight cryptographic protocols, improves security by offering mutual authentication

and protecting against phishing attacks [244]. At the same time, IEEE 802.1X and 802.11X are playing a significant role in improving wireless network security by providing strong authentication and access control mechanisms. The 802.1x standard addresses vulnerabilities in earlier standards by implementing a centralised authentication server, which helps mitigate denial-of-service attacks. On the other hand, 802.11x introduces two-way authentication to prevent man-in-the-middle attacks, significantly improving the security posture of wireless Local Area Networks (LANs) [245]. Research is still ongoing to improve these standards, which are incorporated at the hardware level in our proposed work.

3.0 Related Work

3.1 IoMT Authentication

Vijayan *et al.* [116] proposed a secure Lightweight Authentication Scheme (LAS) for IoMT-based healthcare systems, enhancing security in healthcare systems. The proposed system required device registration and central authority approval but allowed peer-to-peer communication without central intervention during authentication and communication phases while outperforming other lightweight schemes. However, only the technical part of the scheme was evaluated. A graphical-password-based user authentication scheme for the IoMT to improve security and user experience during the COVID-19 pandemic was proposed in [117]. The proposed scheme, implemented via an Android application, was assessed for system, information, and interface quality using the Post-Study System Usability Questionnaire (PSSUQ) tool, demonstrating its potential to enhance user authentication experiences in healthcare. Similarly, some authors [118] proposed an improved lightweight user authentication scheme for the Internet of Medical Things (IoMT) in which the hash function and XOR operation were used for operation in low-spec healthcare IoT sensors. The proposed scheme outperformed other protocols in terms of security and performance but did not deal with smartphone sensors. The protection of patient information's confidentiality in IoT gadgets was proposed in [119], which used decentralised identifiers (DIDs) and verifiable credentials (VCs) together with OAuth-based authorisation framework. The proposed framework demonstrated enhanced privacy and security through a smart pill dispenser, thereby streamlining access control administration. The work, however, mainly focused on the technical part of the model rather than the user part. Bali *et al.* [120] proposed a multi-factor authentication system for IoT-based Wireless Medical Sensor Networks, enhancing security, scalability, and effectiveness

in patient care. The proposed system, while offering enhanced functionality and resistance to common attacks, did not include smartphones. The use of Artificial Intelligence (AI) to enhance authentication of IoMT users through the design of a framework using bioelectrical signals for authentication and AI with contextual data was proposed in [121]. The framework enhanced security in healthcare, maintained user trust and data integrity, balanced usability and security, and was adaptable to various devices. Their work, however, was only restricted to bioelectrical signals. Most works on the IoMT involving the elderly look at applications that monitor their health and maintain their well-being without looking at authentication. We now look at other works in the realm of the IoMT that do not necessarily look at the elderly's authentication. Khan *et al.* [253] suggested an assessment framework to offer trustworthy and safe authentication procedures based on authentication features for Internet of Health Things (IoHT) devices. Using a hybrid multi-criteria decision-making methodology, the framework assessed authentication aspects and determined which authentication scheme or method was best. The work, though adaptive, did not consider elderly users. A biometric-based authentication scheme for hospital environments where patients interacted with smart surroundings without explicit gadgets was proposed in [122]. The scheme could resist various well-known attacks showing that biometric keys were crucial for identification and authentication, but the work generalised security and did not focus on the elderly. A novel, low-complexity, and resilient remote user authentication system for Internet of Things-enabled healthcare applications was presented in [123]. A formal verification proved the security of the scheme and its applicability in real-world healthcare applications. On the other hand, the exploration of authentication techniques for IoT-enabled healthcare systems at different network levels and a taxonomy of attacks was conducted in [124]. Their work focused on user and device verification but did not focus on elderly users. Table 1 below shows a comparison of our proposed work with previous works highlighting the gaps that our work sought to close.

Table 8:Our proposed work against previous work

Item	Previous work	Our proposed work
Usable-Security	Previous works focused on security without usability and vice versa [118][119][253].	Our proposed Android app aims to balance usability and security.
Device authentication	Most previous research focused on device authentication [116][118].	Our work aims to authenticate both the user and device on medical platforms for security and usability.

Continuous authentication	A model based on app traffic patterns continuously authenticates users by analysing network traffic, achieving an impressive average F-measure of 95.5% was developed by Ashibani *et al.* [261], one that utilised touch-timing differences and hand-movement gestures [262], hands-free one-time and continuous authentication using glass wearable devices [263], hands-free authentication using glass wearable devices that enabled one-time access through voice commands and maintained continuous authentication by periodically displaying QR codes for re-authentication while the user faced the terminal [263], continuous authentication scheme using human-induced electric potential measured by wearables [264], combining trusted IoT devices and continuous authentication based on smart-home behavior [265], hands-free continuous authentication using ECG and EMG biometrics that required no human interaction [266], continuous authentication (CA) using cardiac biometrics from wrist-worn wearables [267], a single-factor authentication scheme that required only two short voice inputs [268].	Previous techniques either required additional hardware or movement of the elderly people thereby inconvenient to them. We aim to use static authentication for improved usability amongst elderly users.
Adaptive authentication	Current authentication techniques impose what users must use [269].	We aim to enable adaptive user authentication by assigning available and suitable authenticators based on a risk score and the user profile.
User consideration	Most previous IoMT works do not consider the age of users.	We factor in the user's age, health, and risk score.
App availability	Most commercial apps mainly monitor health [270][271].	We aim to use users' physiological features for health monitoring and authentication on medical platforms.
Risk score analysis	With user behavior and environmental data, a risk score was calculated via localized risk analytics to help the authentication server make decisions in [275-277].	Our work is narrowed down to risk scoring for IoMT authentication.

3.2. Adaptive Authentication

Bayesian probability in Context-Aware Scalable Authentication (CASA) was proposed in Hayashi *et al.* [156], which selected active authentication methods based on passive factors and location contexts to lock the screen based on PIN and password. The model, while reducing usability, formed the foundation for modern adaptive authentication. Forget *et al.* [126] introduced Choose Your Own Authenticator (CYOA), allowing users to choose their authentication scheme based on their inclinations, capabilities, and usage context, but restricting flexibility and introducing delays, especially for elderly users. A proposed smartphone adaptation that adjusted lock functionality between vocal sound recognition, facial scan, and fingerprint-based on usability was proposed in Wo'jtowicz *et al.* [127] but it disregarded security due to its focus on usability. In conclusion, there is no universally applicable solution for IoMT security, and thus the various authentication mechanisms can be used in conjunction to improve security at the elderly users' convenience [147].

4.0 Research Method

The proposed adaptive authentication model analyses user interaction with an Android application to create a risk profile using the Naive Bayes Model. The choice of the model was predicated upon its simplicity, speed, interpretability, usefulness in our context, and efficiency [233-236]. An Android app was developed, through which users first registered and then tried to log in to an imaginary platform. During authentication, an assessment of the context was executed to estimate the risk associated with the login request. The outcome was then categorised as a Propensity Score, which determined the level of authentication difficulty and the authenticators to be used. The goal was to create an authentication solution that was tailored to the user's visual, mental, and physical medical condition providing a user-friendly authentication experience while ensuring the security of their medical information. The steps followed the MAPE-K_{HMT} framework.

4.1. Naive Bayes Machine Learning Algorithm

This supervised machine learning algorithm employs probabilistic and statistical methods for classification. The derivation of the Naive Bayes probability from the simple Bayes Theorem is written as follows:

$$P(y|x) = \frac{P(x|y)P(y)}{P(x)}, \quad (1)$$

where $x = (x_1, x_2, \ldots\ldots\ldots, x_n)$ represent the user's context and y represents the risk probability of a user. Expanding using the chain rules gives

$$P(y|x_i, \ldots\ldots\ldots, x_n) = \frac{P(x_1|y)P(x_2|y)\ldots\ldots\ldots P(x_n|y)P(y)}{P(x_1)P(x_2)\ldots\ldots\ldots P(x_n)} \quad (2)$$

which simplifies to

$$P(y|x_1,\ldots,x_n) \propto P(y) \prod_{i=1}^{n} P(x_i|y) P(y \mid x_1,\ldots x_n) \propto P(y) \prod_{i=1}^{n} P(x_i|y) \quad (3)$$

Let $P(y|x_1,\ldots,x_n)$ be represented by $P(u)$ for simplicity purposes. The verification stage compares the user's illegitimacy probability P(u) to a predefined threshold $\alpha(0, 1)$, if it is 1, access is denied, otherwise, multiple classes are used. The following formula is
used to calculate the categorisation decision rule:

$$P(u) = \begin{cases} Legitimate, & if\ P(u) \leq 0.2 \\ Suspicious, & if\ P(u) > 0.2 \end{cases} \quad (4)$$

Contextualising Equation (2) to our case gives Equation (5):

$$P(Ill|MobChnge \ldots TimeChnge) = \frac{P(MobChnge|Ill).P(GPSChnge|Ill)\ldots.P(TimeChnge|Ill)}{P(MobChnge)P(GPSChnge)\ldots P(TimeChnge)} \quad (5)$$

where *Ill* represents Illegal, *MobChnge* represents Mobile OS Change, *TimeChnge* represents Time Change and *GPSChnge* represents GPS Change.

4.1.1 Proposed System Overview

We utilised Android smartphones with Android version 12 or higher, equipped with sensors for context identification and authentication. The research focused on the operating system rather than specific brands to cater to different users who used their devices since the research used the Bring Your Own Device (BYOD) concept. After data collection, data analysis was conducted using R Studio. The smartphone worked as a lightweight information processor, sensing and actuating, and sending data to the cloud for further processing and storage. The research introduced a new feature, human–machine collaboration, which was integrated into the framework's monitoring, analysis, and execution. This work introduced novel aspects that included assigning authenticators based on risk, user medical conditions, available authenticators, and testing outside the lab environment.

The Naive Bayes algorithm described in the previous section was used to calculate the risk associated with a login attempt. A user was defined using contextual features included in the algorithm below, namely, mobile browser, mobile operating system, IP address, network type, GPS coordinates, and access time. These features were used in the Naive Bayes chain rule to calculate the conditional probability of a login attempt being illegal based on the number of mismatches with known features. Having determined the risk score, the user's age and medical condition were used, guided by the analysis of authenticators conducted in Section 2 to determine which authenticators available on a particular device could be used to authenticate an elderly user. Algorithm 1 shows the steps that a user follows from the time of clicking the login button to the time of authorisation.

Algorithm1. Adaptive authentication and authorisation for elderly users

Input: Mobile_Browser, Mobile_OS, IPAddress, Network_Type, GPS_Coordinates, Access_Time, Knowledge_based data, Biometric_data, Age.
Output: Risk score, trust score, and authentication result.
Assumption: The usability of authenticators is significantly influenced by age and medical condition.
1. *Start adaptive app by clicking an icon.*

2. *Obtain user verification information:*
- User—begin signup if no account exists, or login if already registered.
- User—during signup, select medical condition(s) for the app to determine the usable authenticators for the user.
- App—verifies user email address/phone number and password or PIN.

3. *Define partial conditional probabilities as weights using the Naive Bayes Theorem:*
- App—use Naive Bayes to define conditional probabilities of deviation of input.
- App—capture all background and active data that define a user.

4. *Calculate first-level weighted risk score:*
- App—obtain email/username and device parameters.

If the account is verified on the device, request an adaptive authentication PIN or password
else
Call other available and usable verification methods.
5. *Calculate second-level weighted risk score:*
- Verify user against the device.

If the user and device match, call one usable authenticator and update the trust score
else

Call other available and usable authenticators.
6. *Iterate through user profiles:*
Begin: while trust score < threshold = 0.7

- Repeatedly continue through each user profile, calculating the risk score, and initial trust score.
- Authenticate with available and usable authenticators, one at a time.
- Update trust score at each iteration:

trust score += trust score
End
7. *Display Results:*
- Show each user's risk score, trust score, and whether authenticated or not.

8. *Authorise:*
- Grant access to requested resources.

The following is a summary of the algorithm: With the help of enumerators, users downloaded, installed, and registered on the adaptive app on their smartphones. The algorithm uses the Naive Bayes Theorem to define conditional probabilities and calculate risk scores, so the model operates on a probabilistic framework to determine a user's risk and trustworthiness.

How It Works:

- **Input Data**: The model takes various inputs, such as Mobile_Browser, Mobile_OS, IPAddress, GPS_Coordinates, and Access_Time, together with knowledge-based and biometric data. These are the features of a user's login attempt.
- **Training**: During the initial signup phase (Step 2), the user's "normal" behaviour is captured. The medical condition selected by the user and the age are key pieces of information that will influence the model's assumptions when assigning authenticators. The model learns the probability of these features being associated with a legitimate user.
- **Calculation**: The algorithm computes a first-level weighted risk score in Steps 3 and 4 using the Naive Bayes Theorem. The "partial conditional probabilities" of the features of the current login attempt departing from the user's pre-established profile are computed in order to accomplish this. The naive_bayes_theorem determines the likelihood of an occurrence based on past knowledge of related conditions and is predicated on the idea that features are conditionally independent.
- **Scoring**: The computation of a risk score and a trust score (Steps 4 and 5) forms the basis of the model. The probability that the login is fraudulent is indicated by the risk score, which is probably an inverse probability. On the other hand, the trust score indicates the likelihood that the user is authentic.

- **Iterative Authentication**: The risk and trust scores are continuously calculated and updated by the model using an iterative technique (Step 6). The trust score rises with each successful authentication using a usable authenticator (such as a PIN or biometric information). The process keeps going until the trust score rises over a certain level, at which time the user is given access (authorised).

By contrasting the features of the current login attempt with a baseline of "normal" behaviour, the Naive Bayes model essentially assists the system in making a judgement. The weights that go into the risk score are defined by the conditional probabilities, and they are used to assess how trustworthy or suspicious the login is.

The user would not be permitted access if the trust score was not obtained. Device-level data collection resulted in the transmission of that information to the server, where it was stored and later accessed for analysis. After that, it was subjected to ML algorithms to extract data regarding the model's efficiency, usability, and security. Users were then asked to rate the app's usability in a post-deployment evaluation, and the data were evaluated in R Studio. Figure 2 shows the general architecture of the proposed system.

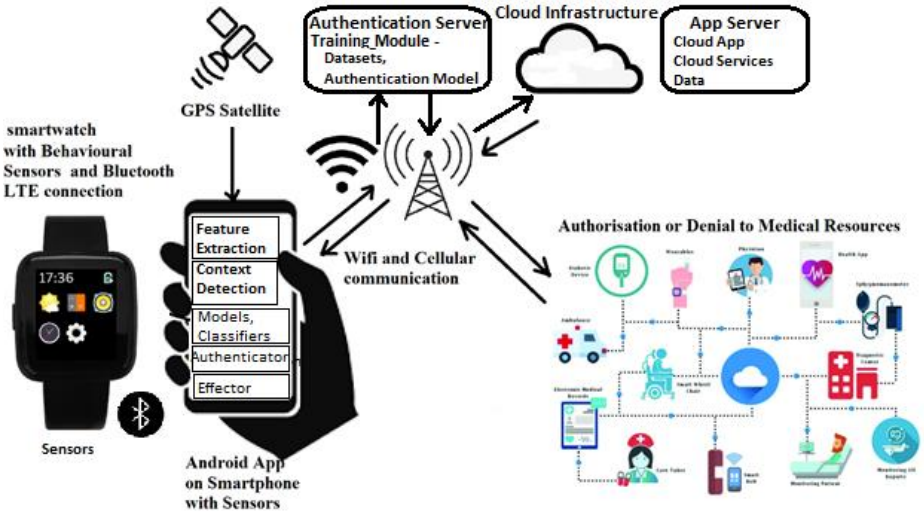


Figure 2: General architecture of the proposed system

To connect with the server for risk assessment, authenticator selection, and ultimately authorisation, the smartphone served as both a sensing and an authenticating device. Through Bluetooth, the smartwatch could optionally provide additional sensing connection with the smartphone. Since there was no specific app or resource to access our work, we used Figure 3c's

panel to represent the authorisation stage. It offered the option to search for Bluetooth devices for behavioral authentication following initial authorisation.

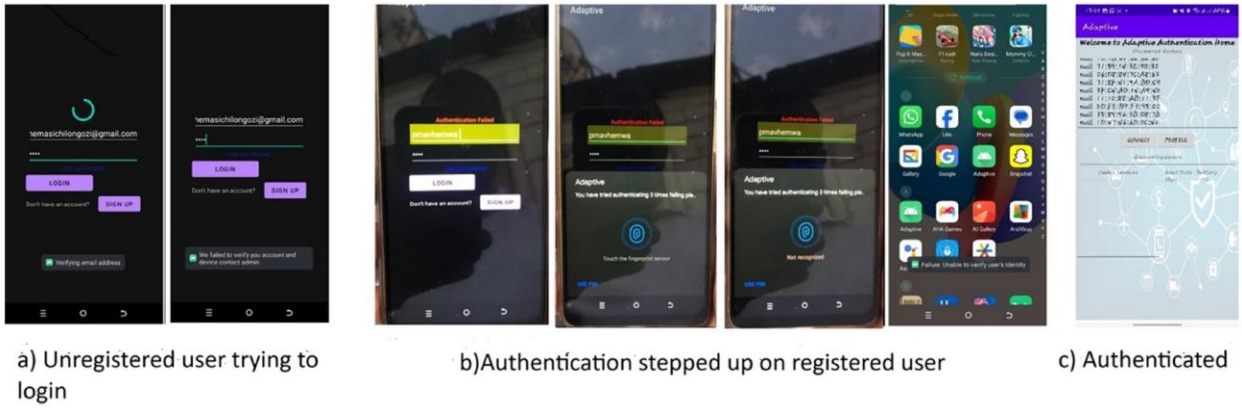


Figure 3 :Login process until authorisation

When a user uses the app for the first time, signup is initiated. Then, login followed. Figure 3 shows cases of failed login where (a) is a scenario of an unregistered user being unrecognized and (b) a registered user failing the initial knowledge-based authentication before the biometric fingerprint is called, which is again failed before a failure message is displayed signaling the end of the session. Part (c) shows the successful authentication screen where the system starts searching for nearby Bluetooth devices that can also be used for authentication. The same process described above occurs if there are changes in any other contextual factors which result in a change in risk score. Figure 4 shows the signup and login screens.

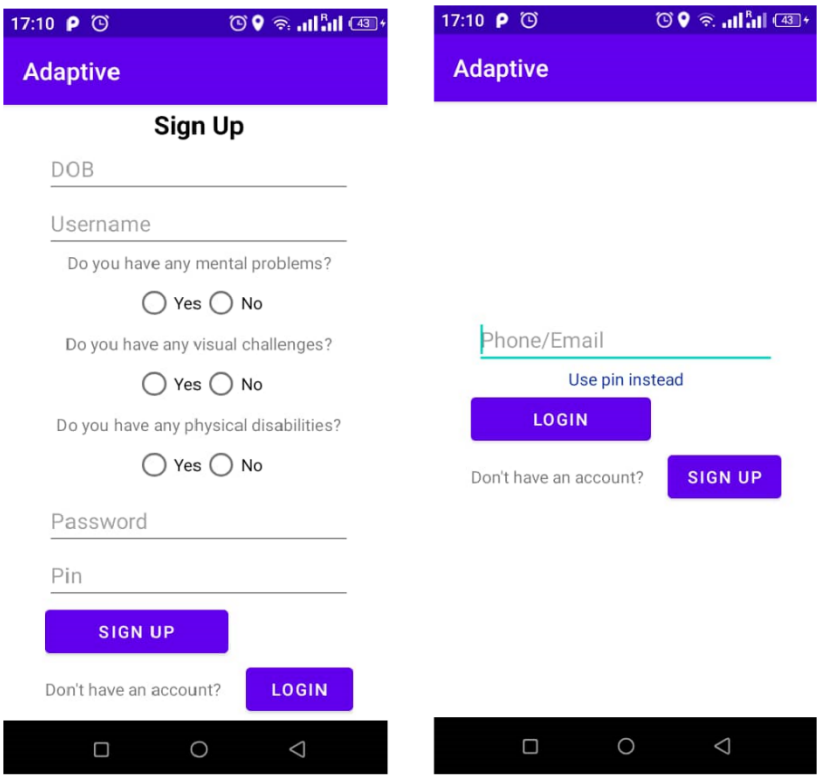


Figure 4:Signup and login screens

Pre-Study Survey

To help with prototype development, our previous study [251] examined user demographics, ICT backgrounds, disabilities, security knowledge, and preferred authentication methods. In order to find age-related changes in the aforementioned parameters, the study used participants who had completed a pre-study survey and were above the age of eighteen (18). Because of the different results and participant changes, there was no comparison with the initial survey during the information gathering stage.

Study Setup

Participants were interviewed using smartphones at workplaces, hospitals, or homes, starting with the enrollment phase where they registered, provided information, and created models. The usability of their smartphones was assumed to be enhanced due to their familiarity with them.

Tasks

Instead of visiting the actual site, participants were told to pretend they were logging into their health portal, primarily for authentication.

4.2 Participants

4.2.1 Population

Patients over the age of fifty (50) were the focus of this study, with the assumption that they were not active and were not tech-savvy, suggesting the necessity for static authentication.

4.2.2 Sample Size

Fifty-three (53) participants comprising twenty-five (25) men and twenty-eight (28) women participated in the research drawn from Rwanda and Zimbabwe. Seven (7) participants did not respond, giving an 88% response rate.

4.2.3 Dataset Size

The preceding section's sample yielded a dataset including two-hundred and thirty six (236) records, with an average of four records per user indicating distinct login attempts. The user-identifiable details, contextual elements, and variations in risk score up to the final score indicating whether or not a user was permitted access were all labeled in the dataset.

4.2.4 Sampling Technique

The research utilised stratified systematic sampling to represent both rural and urban populations.

4.2.5 Inclusion and Exclusion Criteria

The study employed smartphone ownership as an inclusion criterion and examined senior users, eliminating the upper-age limit, following the Belmont Report [272]. Elderly people without smartphones and those under 50 were not allowed to participate in the survey.

4.3 Data Collection

The data were collected through the app's registration form and user logins, with an average of four trials per participant.

5.0 Results

Following their contact, the adaptive authentication app gathered information on users' backgrounds, health issues, risk assessments, and authentication status. For each component of the adaptive authentication model, confusion matrices were among the metrics used in the analysis. The study focused on successful or failed authentication and used R Studio to analyse the data to find trends in the ease or difficulty of authentication among older participants using our proposed model. Since different devices were using the same operating system, performance tests at the device level were not carried out.

5.1 Confusion Matrix and Statistics for Overall Authorisation

The confusion matrix and statistics for the whole authentication to authorisation process are displayed in Figure 5 where the confusion matrix, the Kappa Score, and Mcnemar's test are shown in order.

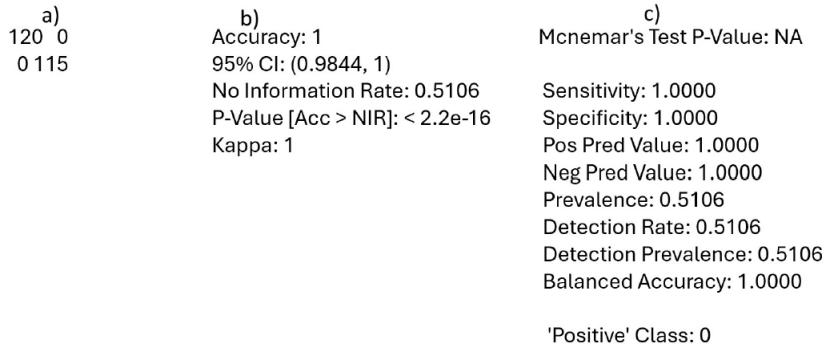


Figure 5:Overall confusion matrix and statistics of proposed system

As can be seen, the model accurately classified every instance in the dataset, with a 95% confidence interval indicating a 100% accuracy. The model's low p-value suggested superior performance compared to the baseline, with a true accuracy of at least 98.44%. The No Information Rate indicated that an estimate about the most prevalent class could be accurate 51.06% of the time. When taken as a whole, these metrics offered strong proof that the model performed extremely well on the given data, correctly classifying each event with no mistakes. Other metrics used included balanced accuracy, prevalence, detection rate, positive predictive value (PPV), negative predictive value (NPV), specificity, and sensitivity. The specificity and sensitivity were both one, indicating that the model correctly detected true negatives and positives. Similar functionality in both groups was indicated by the dataset's balanced accuracy of one, with equal prevalence, detection rate, and detection prevalence matching the real class distribution. Verifying

the model's performance using untested test data is essential to ensure that it generalises well and does not overfit the training set.

Our model, which had an Area Under the ROC Curve (AUC) value of one, showed excellent discrimination ability between the positive and negative classes. For randomly chosen positive and negative instances, the model consistently gave positive occurrences a higher score than negative instances. Figure 6 shows the ROC curve for authentication and authorisation with the Area Under the Curve (AUC) of one with control = 0 and cases = 1.

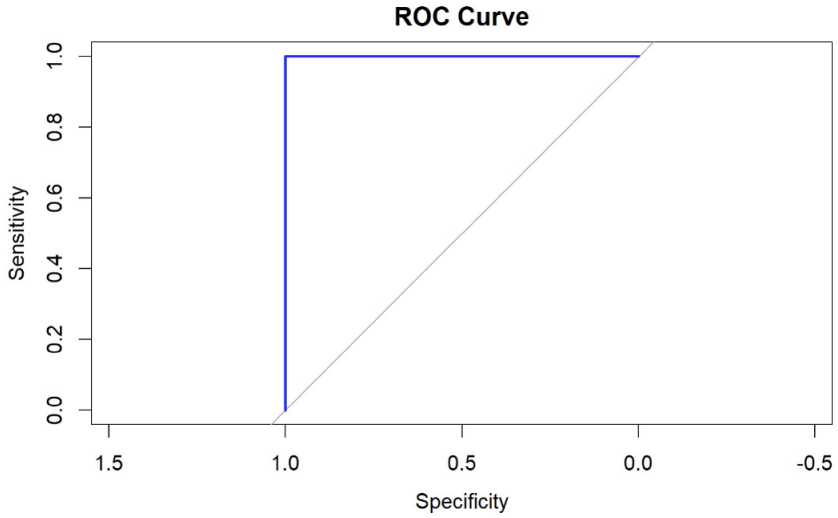


Figure 6: ROC curve for authentication and authorisation of proposed system

The results of combining the AUC with additional performance indicators derived from Figure 1 are shown in Table 2.

Table 9: Combination of AUC with other performance metrics of proposed system

Metric	**Value**
Accuracy	1
Sensitivity (recall)	1
Specificity	1
Precision (PPV)	1
NPV	1
Balanced Accuracy	1

The adaptive authentication model, with no false positives or negatives, accurately recognised all positive and negative classifications, predicting data distributions. The model accurately predicted the dataset's class distributions and consistently ranked positive examples higher than negative ones, demonstrating a flawless AUC. However, since these results may indicate overfitting, we

further performed cross-validation. Since perfect performance is uncommon, overfitting is the only explanation for these findings. Normalisation and more thorough testing with a wider variety of datasets (real-world data) are needed to make sure the model performs well outside of a controlled environment. However, since there are not many studies that directly connect to our work, real-world deployment was carried out to acquire a dataset, which was evaluated. The results of the calculations for the False Positive Rate (FPR) and False Negative Rate (FNR) were zero for each. The FPR and FNR values of zero for the provided dataset supported the accuracy and reliability of the model.

5.2 Usability Evaluation

False acceptance and rejection rates were employed to gauge the model's usability. Table 3 shows the evaluation metrics also derived from Figure 1.

Table 10: Combination of AUC with other performance metrics of proposed system

Metric	**Value**
False Rejection Rate	0
False Acceptance Rate	0

The authentication paradigm exhibited high security and usability, with zero false acceptance and rejection rates, demonstrating its exceptional performance. The model's authentication decisions were accurate and consistent, ensuring users' authenticated state was accurately matched.

5.3 User Health Impact on Authentication

Our assessment of the effect of user health on authentication was aided by post deployment evaluation, as the majority of users reported that the app considered their health. This had an impact on the selection of authenticators, as previously assumed. Our model accurately predicted 80% of the cases, with an overall accuracy of 80% as evidenced by its high recall and precision. The model's high specificity suggested that it could recognize class 1 (negative cases) instances with accuracy. Figure 7 shows the confusion matrix and statistics for health impact on authentication where (a) is the confusion matrix, (b) shows the Kappa test, and (c) shows Mcnemar's test.

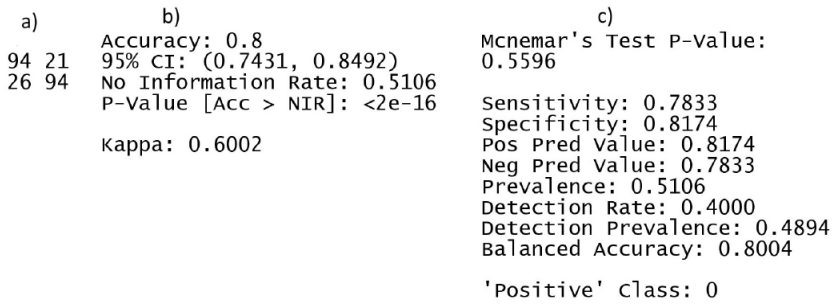


Figure 7:Confusion matrix and statistics for health impact on authentication of proposed system

Further analysis and investigation may be necessary to identify the most significant predictor features and their impact on model performance. Cross-validation is also required to validate the model on independent datasets.

5.4 Train–Test Split and Cross-Validation

The model underwent further validation through train–test split and cross-validation, utilising the confusion matrix and statistics results as shown in the tables Train–Test Split Figure 8 shows the confusion matrix and statistics for the train–test split option and the L1, L2, and Elastic Net normalisation where (a) is the confusion matrix, (b) is the Kappa test, and (c) is Mcnemar's test.

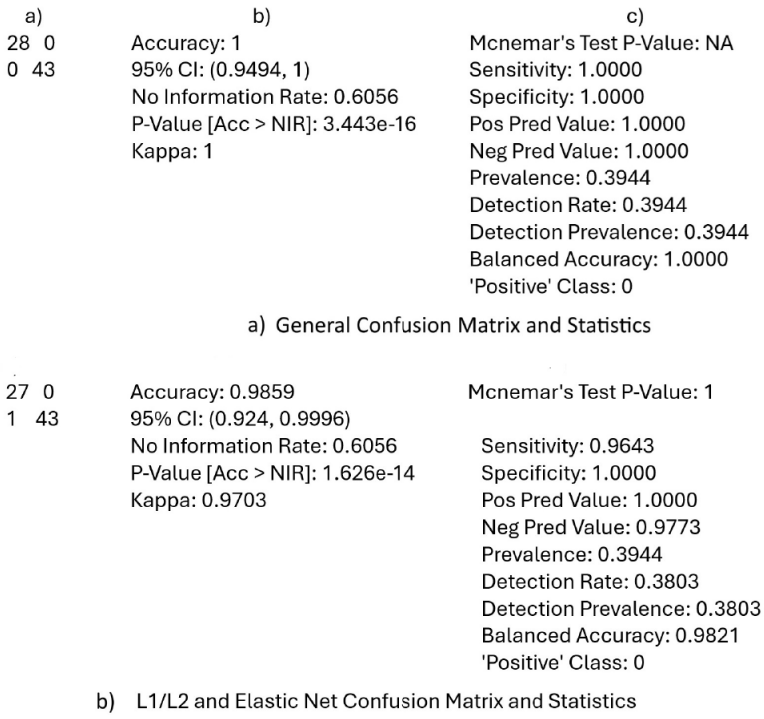


Figure 8: Confusion matrix and statistics for the train–test split and L1, L2 normalisation

The model successfully predicted every occurrence in the test set with excellent sensitivity and specificity, identifying both positive and negative events. The initial results were confirmed by the

Kappa, precision, and negative predictive values, which showed that all forecasts for each class were accurate. The model effectively generalised to the test data, as indicated by the findings. With an accuracy of 98.59%, excellent sensitivity, specificity, and balanced accuracy, the model was operating remarkably well under the Lasso and Elastic Net normalisation. The one misclassification was a minor and normal problem, but the model predicted outcomes quite well.

5.5 Cross Validation

To examine access performance metrics and the confusion matrix, the Random Forest classifier was employed for 10-fold cross-validation using 235 samples, 26 predictors, and two classes, "0" and "1". The greatest number was utilised to determine the best model using accuracy, and mtry = 133 was the final value employed for the model. For an accurate representation of each class and to increase the model's generalisability, a 10-fold cross-validation method with gender-based stratification was employed. To ensure reproducibility, a random seed was used, and it was observed that accuracy and Kappa both considerably rose when mtry rose from 2 to 133 and finally 265, suggesting that for the particular dataset and model, choosing more variables at each split improved performance. Figure 9 shows the performance metrics. In both train–test split and cross-validation results, the model demonstrated excellent accuracy and Kappa, demonstrating its effective generalisation to unknown data.

```
Access performance metrics

  mtry  Accuracy   Kappa      Accuracy SD  Kappa SD
1 2     0.8891304  0.7779628  0.05774286   0.1154879
2 133   1.0000000  1.0000000  0.0000000    0.0000000
3 265   1.0000000  1.0000000  0.0000000    0.0000000
Access confusion matrix and other metrics

          Accuracy: 1                    Mcnemar's Test P-Value: NA
          95% CI: (0.9844, 1)
    120   0 No Information Rate:         Sensitivity: 1.0000
      0 115 0.5106                       Specificity: 1.0000
          P-Value [Acc > NIR]: <         Pos Pred Value: 1.0000
          2.2e-16                        Neg Pred Value: 1.0000
                                         Prevalence: 0.5106
          Kappa: 1                       Detection Rate: 0.5106
                                         Detection Prevalence: 0.5106
                                         Balanced Accuracy: 1.0000

                                         'Positive' Class: 0
```

Figure 9: Confusion matrix and statistics for the cross-validation option on proposed system

5.6 Distance Analysis

We performed a distance analysis to determine the effect of location on authentication. The study underscored the importance of location by calculating the distance a user, presumed to be

constantly carrying their smartphone, would have travelled from a predetermined spot. This is shown in Figure 10.

```
Residuals:
    Min      1Q  Median      3Q     Max
-0.7345 -0.2008  0.1321  0.2103  0.4219

Coefficients:
                  Estimate Std. Error t value Pr(>|t|)
(Intercept)       0.912344   0.028185   32.37   <2e-16 ***
dist_from_epicenter -0.044475   0.002147 -20.71    <2e-16 ***
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1


Residual standard error: 0.2978 on 233 degrees of freedom
Multiple R-squared:  0.6481,   Adjusted R-squared:  0.6466
F-statistic: 429.1 on 1 and 233 DF, p-value: < 2.2e-16
```

Figure 10:Distance analysis of proposed system

The linear regression analysis revealed a significant negative correlation between Dist from epicentre and authorised. The likelihood of obtaining authorisation decreased as the distance from the epicentre increased. The relationship was statistically significant due to the significant variability in the authorised variable. Figure 11 shows a graphical illustration of the distance analysis where trust ranking decreased with distance from a known location.

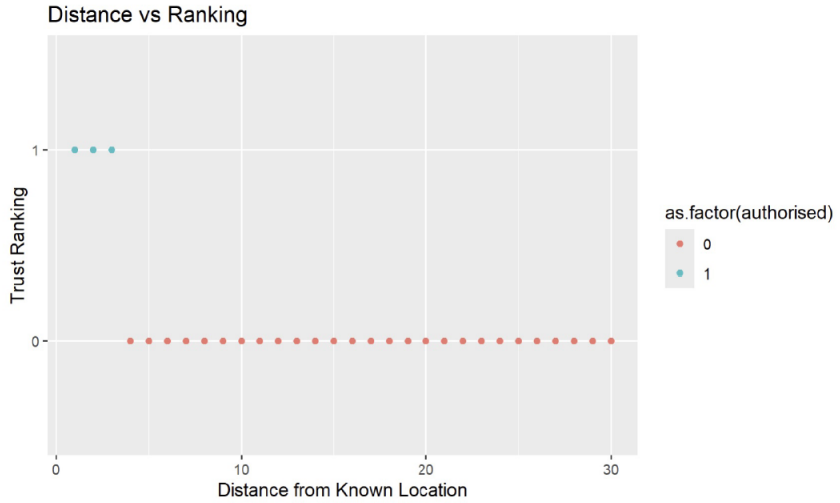


Figure 11:Distance graph of proposed system

According to the results, our model could tolerate a certain radius from a known site, but when the radius was above a certain threshold, it caused suspicion, and it was clear that our model was user-friendly, especially for older users.

5.6.1 Effectiveness

The model's effectiveness in predicting user access was assessed using a confusion matrix and related metrics. The success ratio was measured to ensure the model's reliability and usability in real-world scenarios. Figure 12 shows part of the success-ratio results derived from the total login attempts and the successful attempts.

	owner_id	total_logins	successful_logins	success_ratio
12	26	5	3	0.6
13	27	5	3	0.6
14	28	5	2	0.4
15	29	5	4	0.8
16	30	5	4	0.8
17	31	5	3	0.6
18	32	5	4	0.8
19	33	5	2	0.4
20	34	5	3	0.6

Figure 12:Snippet of success ratio on proposed system

The snapshot shows a success ratio between 0.4 and 0.8, with successful logins generally exceeding failed logins.

5.6.2 Efficiency

The efficiency of our model was assessed through the FRR and FAR measurements, both of which had zero values indicating efficient classification. The study analysed various factors such as trust ranking, success rate, completion rate, average success ratio, overall completion rate, and average success ratio. The overall values are shown in Table 4.

Table 11: Overall success and completion ratios on proposed system

	Value
Average success ratio	0.47
Overall success rate	0.49

Although the ratios were acceptable, they were not high, which showed that our model's efficiency needed to be raised. Other mechanisms that could be used to measure it include resource efficiency, risk vs. trust balance, model interpretability, scalability, performance, and the security–usability trade-off, cross-validation, and accuracy-related metrics that we utilised.

5.7 Usability Considerations

We conducted a post-deployment survey to ask users about their experiences with the app. We used the age category of fifty-one (51) years and older. Most respondents who were asked if the app considered their medical conditions indicated that it did, as seen in Figure 13.

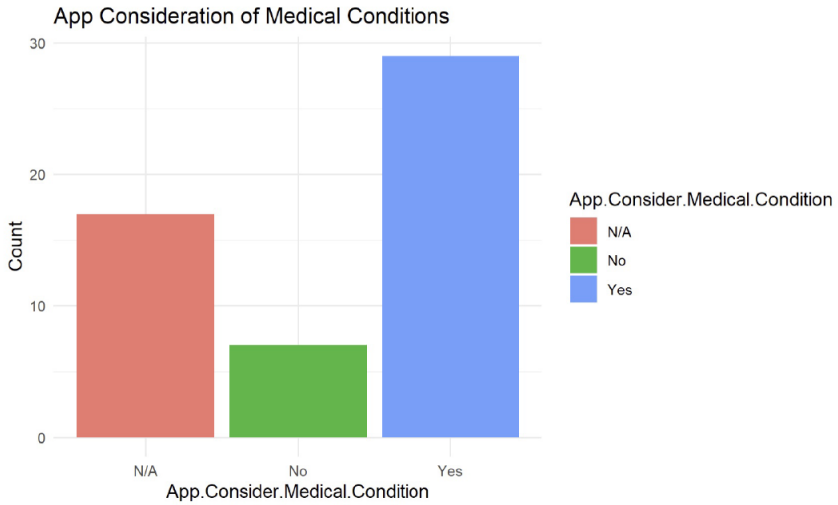


Figure 13:App consideration of user medical conditions on proposed system

Most respondents concurred that the app considered their medical issues. Regarding further usability measures, the responses were compiled as depicted in Figure 14.

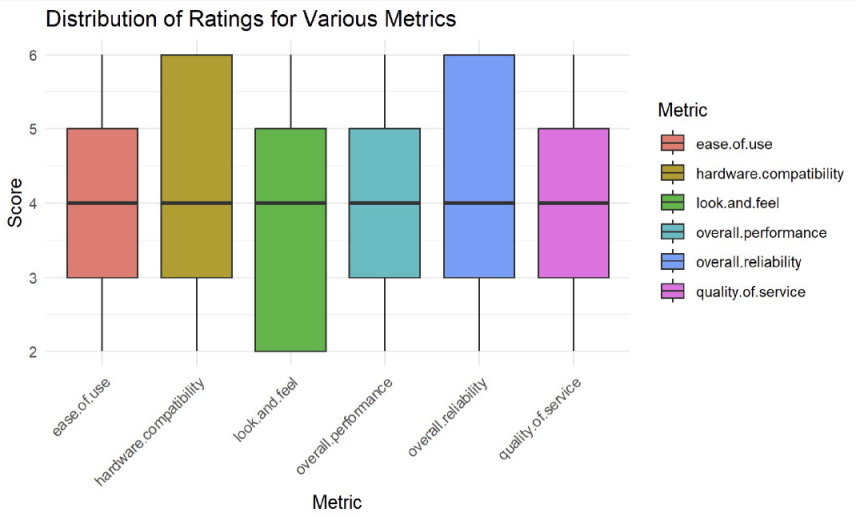


Figure 14:Usability metrics on proposed system

It is clear that most reviews were favorable to the app. On the frequency of issues with the app, users gave responses in Table 5.

Table 12:Frequencies of errors on proposed system

Metric	Value
Average success ratio	0.47
Overall success rate	0.49

As evident, 66% of the respondents responded positively in support of the app. Figure 15 summarises user responses to a question about whether they would recommend the app to others.

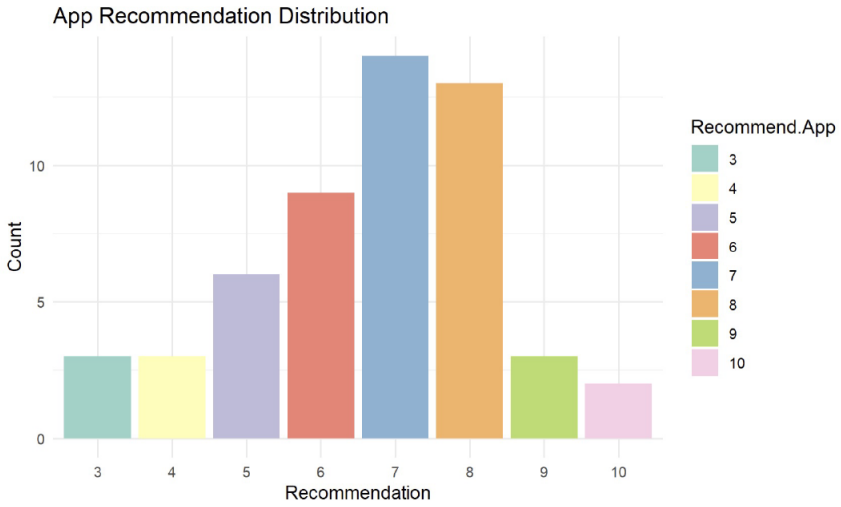


Figure 15: Proposed app recommendation to others

6.0 Discussion

We implemented an adaptive user authentication model for IoMT users with a particular focus on improving usable security. The model, which was implemented on Android smartphones, demonstrated promising results in terms of accuracy, precision, recall, and overall performance. The model calculates the initial risk score by utilising various features like user ID, device ID, network, location, and habits and performed stepwise authentication guided by the hardware of the device. The model demonstrated high accuracy in identifying authorised and unauthorised access attempts during cross-validation, indicating effective risk calculation. These ideal outcomes, however, could not always be practical and might point to possible problems like overfitting, particularly given that the evaluation was mostly focused on training data rather than a distinct test set. To ensure the model maintained its excellent performance in real-world scenarios, it was crucial to determine consistency in its performance on unobserved test data. The Kappa value of

one indicated a perfect agreement between the model's predictions and the actual values after adjusting for chance. The risk calculation mechanism accurately detected anomalies between legitimate and fraudulent access attempts, with a 1.0 sensitivity and specificity, ensuring no false positives or negatives. Combining the AUC with additional performance indicators showed that our model accurately recognised all positive and negative classifications, predicting data distributions. The results suggested that there may have been overfitting, which may necessitate cross-validation. Nevertheless, our accuracy of 98.5% after applying Lasso and Elastic Net normalisation provided us with confidence that our model was resistant to overfitting. The authentication paradigm, which had zero false acceptance and rejection rates, exhibited high security and usability. Although these results are ideal, the model's performance in real-world scenarios and against different user types is crucial for ensuring its robustness and generalisability.

The health impact accuracy rate was 80%, indicating accurate detection of positive situations with high recall and precision. We can infer that physical health conditions have an impact on the success of authenticators like a fingerprint or gait, while mental health conditions affect the success of knowledge-based authenticators that are recall-based, based on our analysis of authenticators and their suitability for elderly users. As a result, we used rule-based selection to allocate authenticators related to health conditions. Nevertheless, the impact of each health condition on the outcome of authentication was not examined in this experiment. Therefore, to strengthen our user authentication model, it is crucial to discover any particular risk factors associated with health issues that are correlated with lower trust ratings or greater failure rates. To ensure equitable treatment for older users with specific medical conditions and appropriate authentication mechanisms, the model was further tested for usability taking health conditions and distance from known locations into consideration. However, this is only applicable to specific smartphone's hardware. Further analysis and investigation may be necessary to identify the most significant predictor features and their impact on model performance. When evaluating using the train–test split, the model's Kappa, precision, and NPV showed accurate forecasts for each class, indicating good generalisation to test data. The study found a mix of high- and low-trust users, with a median trust value of 0.5, influenced by contextual factors. Health conditions, age, and location data in that case were significant predictors of trust score. In line with the logic of the model, which holds that greater distance diminishes confidence, authorisation was significantly negatively impacted by distance from the known location. To enhance the validity of the study, it is recommended to incorporate more predictors and examine multicollinearity and non-linear

relationships. The confusion matrix demonstrated 100% accuracy in training; nevertheless, the final authorisation decision based on trust score and risk assessment might be improved, as indicated by the 80% cross-validation findings. The high Kappa value indicated a strong agreement between the predicted and actual classes. Average and overall success ratios validated [178], who asserted that age and illness had a bearing on user authentication success amongst the elderly. Although our method employed risk scores to ascertain authentication challenges, each user's experience with the process would vary based on factors such as the availability of usable authenticators on their particular device. This is a result of the model's lack of device specificity and its base in the Android operating system, which works on a range of hardware. Risk-based authentication (RBA) allows our model to successfully comply with data privacy regulations such as GDPR and HIPAA since it protects user data and minimizes unnecessary data exposure. This model makes use of several authenticators and enhances security while abiding by privacy rules by modifying authentication requirements based on risk assessments. It guarantees that all risk assessments and outcomes are carried out, kept secret from the user, and that backend privacy is upheld. Additionally, using several authenticators makes the system more secure against attacks because an attacker may have to compromise multiple authenticators, increasing the likelihood that they will be discovered. According to Figure 13, which displays the metrics used to measure usability, users were generally satisfied with the app across all evaluated aspects. Overall performance, quality of service, and ease of use all pointed to most users finding the app to be mostly satisfactory. User views varied significantly when it came to hardware compatibility and overall reliability, which suggests that those aspects need to be improved to enhance the entire experience. Look and feel further revealed that some users were not at all happy with the way the app looked and felt, while others thought the design and interface were great. These findings typically point to the need for improvements to make the app more aesthetically pleasing and easier to use to boost user satisfaction.

7.0 Conclusions and Future Work

The model exhibited exceptional performance in calculating risk, trust, and authorisation decisions. The system effectively integrated user behavior, environmental context, and health conditions to provide adaptive and secure user authentication. However, the model's accuracy difference between training and cross-validation indicated the need for further testing and tuning on diverse data to ensure its generalisability across various scenarios. Low success ratios may also

be attributed to several factors like user experience, network, and medical conditions, and to capture more complex user behaviors and environmental changes, future work will require diversifying the training data to cover a wider range of user behaviors and situations. We could use contextual factors such as ambient light, social context, and network speed to estimate the risk of a login attempt. Network quality could be used to identify patterns, proximity to known devices (like Bluetooth), daily habits, and user activity and could be used to identify a particular person when analysed over time. This would also involve exploring additional features and testing performance at the device level. Additionally, it is important to keep track of the users' health status and modify authentication procedures as needed to accommodate any changes. To ensure optimal performance, we will also frequently adjust the model's parameters and validate them using fresh data. To effectively address the overfitting issue, other normalisation approaches might need to be considered in addition to the cross-validation and real-world data use that Lasso and Elastic Net suggested in this work.

Given that 80% of the participants were senior users in SSA, whose socioeconomic circumstances may differ from those of other continents, some degree of geographic and demographic generalisation may be limited. This is due to potential variations in financial status, amount of technological expertise, perceived usability, and overall security awareness. Nonetheless, it is possible that the findings, independent of geography or upbringing, can be applied to other demographic groups. On health conditions, future work needs to investigate if some health conditions have more effects on authentication outcomes than others. Additionally, longitudinal studies need to be conducted in the future to monitor user behavior, and health changes over time would provide deeper insights into improving model accuracy. Regarding scalability, we believe our model can only perform very well with small datasets like the one that we used in our experiment as it has few features, but we believe that since we used the algorithm for risk calculation and not the classification tasks, we can expand it by adding more features to the risk calculation engine without significant performance costs. However, as Veziroğlu [233] and Kumar *et al.* [234] have noted, the Naive Bayes algorithm performs best on small datasets but not datasets that require intricate feature interactions on classification tasks. Because of its computational efficiency, Naive Bayes can still perform well on simple datasets that only grow in size while the non-existence of large datasets in our specific scenario prevented us from testing its effectiveness on a sizable dataset. If the dataset becomes more complex and has more feature interactions, Random Forest or Gradient Boosting are likely to perform better predictively, though they will

demand more computational power. The model can be scaled for real-world deployment, especially in a healthcare setting with thousands of users; however, given that end-user devices are mobile, attention should be kept on the computational resources needed for such scalability so that the technology cost remains low. On usability, future work needs to look at areas that need improvement, which include hardware compatibility, look and feel, as well as overall reliability.

Part III-B

PART III-B

Naive Bayes-Based Android Adaptive User Authentication

Prototype for Young Internet of Medical Things Users

Part III-B was accepted as:

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, Frederic Nzanywayingoma. Naive Bayes-Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users. Publisher: IET Communications, **Print ISSN:** 1751-8628,**Online ISSN:** 1751-8636,**Article ID:** CMU270082

Naive Bayes-Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users

Prudence M. Mavhemwa, Marco Zennaro, Philibert Nsengiyumva, and Frederic Nzanywayingoma

Abstract

The increasing use of IoMT in healthcare highlights privacy and security concerns surrounding sensitive health data. This research focuses on enhancing the security and usability of IoMT for young users through a robust, adaptive, continuous authentication model using physiological biometrics on Android devices and heart rate data from smartwatches. By integrating user behaviour, environmental context, and health conditions, the model dynamically determines risk, trust, and authorisation decisions. Machine learning techniques analyse data related to devices, networks, locations, and user habits while considering demographics like age and medical conditions to assign suitable authenticators. The model balances accuracy and usability, favouring correct positive predictions, but faces limitations such as class imbalance, feature selection, and overfitting, with a false rejection rate (FRR) of 19%. Behavioral biometrics, personalised authentication, and continuous authentication enhance security and accessibility. However, moderate sensitivity affects its ability to capture all positive cases. Age-group analysis reveals varying engagement with technology, emphasising tailored authentication flows. Future work will explore explainable AI, context aware analytics, and advanced risk assessments, integrating complementary smartwatch data like step count for improved accuracy. This research demonstrates the potential of risk-based adaptive authentication to deliver secure, user-friendly solutions in complex healthcare environments.

1.0 Introduction

The Internet of Medical Things (IoMT) has significantly impacted healthcare care by allowing remote control and real-time monitoring of resources [1][281], particularly during the COVID-19 pandemic [282][283]. However, this increase in IoT (IoT) devices has prompted increased information exchange [284] and cybercrime [267], necessitating innovative security measures such as authentication [285] and customised user experiences [286][287]. Research on user authentication for mobile devices and IoMT has been extensive, with one-time authentication being the predominant method [288]. Traditional security systems based on initial login lack the intelligence required to detect and block suspicious behaviour [289], yet session hijacking can compromise these systems [290]. Typical authentication, which involves one-to-one mapping for individual devices and one-to-many mapping for group-owned devices, is vulnerable, discrete, obtrusive, costly, and not user-friendly [253][287]. Credential reuse across services exposes users to cyberattacks [15][291], while at the same time, IoMT security is crucial due to unique threat landscapes and malicious motives [292], often overlooked by device manufacturers [293]. Research on smartphones and wearables for user authentication is evolving but still limited in scope and application [294][295][296], necessitating self-adaptive and user-friendly security that can autonomously adjust parameters at runtime. There is an increased need for cybersecurity awareness in developing countries, particularly Africa [297], largely due to IoT initiatives primarily targeting developed countries [298]. This research aims to design and implement an adaptive user continuous authentication prototype for young users in healthcare utilising heart-rate data. The prototype uses IoT, the Naive Bayes algorithm, and smartphone and smartwatch sensors to detect illegal login attempts and assign authenticators based on perceived risk, user age, medical condition, and available authenticators. This prototype aims to validate our adaptive user authentication model, which offers a pleasant experience for low risk users and rigorous authentication for high-risk users. The process involves continuously monitoring the user's heart rate for any potential changes that may raise suspicion.

2.0 Related Work

2.1 Continuous Authentication

Continuous authentication (CA) enhances security [291] and user experience [287] by simultaneously identifying and authenticating users while running in the background [299]. Continuous authentication systems offer high accuracy, low battery usage, and security without human intervention [300]. This system is still in its early stages due to implementation challenges such as power, processing, and sensor limitations [301]. Deepthi *et al.*[302] suggest a shift from one-time authentication to continuous user authentication using behavioural biometrics, utilising data from inertial sensors in smart devices and machine learning algorithms. Heart rate sensors are being utilised in continuous user authentication to improve wearable device security by providing efficient and user-friendly authentication. A low-cost system was proposed in Zhao *et al.* [273] that uses users' pulsatile signals from photoplethysmography (PPG) sensors in wearable devices for CA. The system prompts users to temporarily verify their identity using traditional authentication methods before updating itself using adaptive learning, effectively detecting random attacks with a low false detection rate (4%) and high accuracy of over 90%. However, continuous near wrist activity and sudden illness can significantly impact performance. A context-dependent soft-biometric-based authentication system using breathing, gait, and heart rate audio signals was presented in Cheung *et al.* [303] demonstrating the potential for creating a secure, implicit, and continuous authentication system for the wearables market. The study was hindered by limited datasets and audio breathing recordings, necessitating further research on behaviour changes and user variability. A wearable chest strap that employs dry electrodes for single-lead electrocardiography (ECG) signal for continuous authentication was employed in Smyth *et al.* [301] but faced limitations such as short sample size, device dependence, robustness against intrusion attempts, algorithm complexity, and emphasis on verification over-identification. Smartbands can also be utilised efficiently for continuous implicit authentication, as shown by Ekiz *et al.* [304] who highlight the potential of physiological signals, specifically heart rate variability (HRV), as distinct identifiers for continuous authentication in cloud services and IoT devices. The proposed measures can reduce the risk of spoofing attacks but have drawbacks such as placement-related artefacts and poor signal quality. Heart rate data from smart watches can provide continuous user authentication with an Equal Error Rate (EER) of 11.25% [305] but the method may not be robust enough for high-security applications and also, the paper does not

address the potential challenges, such as battery life and user comfort. The use of heart rate sensors through ECG and Blood Volume Pulse (BVP) signals for continuous user authentication was explored in [306], achieving approximately 2% exercise-induced oxygen desaturation (EID) in within-session tests. The study revealed that while varying window lengths can improve ECG performance, the BVP signal did not significantly enhance the multimodal approach's performance. A novel authentication framework for IoT communication models in Nishat *et al.* [307] utilised gait data, achieving a 95% accuracy rate, a lower error rate, and optimised execution time. Machine learning was utilised to analyse user login patterns over time, assigning risk scores based on current behaviour compared to previous patterns, including typical login time, weekdays, last-hour activity, failed logins, and successful logins [308]. The approach initially has a high-risk score, gradually decreasing as the user develops a normal pattern, but this proprietary platform lacks evaluation. Table 1 shows a comparison of our proposed work with previous works on the use of heart rate signals for Continuous Authentication (CA), highlighting the gaps that our work sought to close.

Table 13: Our proposed work against previous work

Item	**Previous work**	**Our proposed work**
Risk Score calculation for static authentication and continuous authentication.	Zhao *et al.*[273] sought to improve the resilience of continuous authentication systems by using cardiac biometrics, providing consistent performance even in the face of motion-induced disturbances. The authors developed a low-cost system that uses pulsatile data from photoplethysmography (PPG) sensors in wearable devices to conduct CA. The authors used Bandpass Filtering to isolate cardiac signals, Independent Component Analysis (ICA) to separate the signal from motion artefacts, and Adaptive Filtering to reduce residual motion artefacts by adjusting parameters in real-time based on characteristics.	Our prototype uses adaptive authentication to balance security and usability. Contextual factors are predefined, and an initial risk score is produced using the Naive Bayes Algorithm. Changes in context are used to determine the risk score. The second stage employs a low-cost, off-the-shelf smartwatch in which heart rate is used to differentiate one user from another via Heart Rate Variability (HRV) for continuous authentication.
Physiological data from wearables.	Ekiz *et al.*[304] demonstrated that HRV-based authentication from smartbands is feasible for real-world continuous authentication, but	Our prototype balances usability and security by establishing an initial risk score for authentication using

	performance depends on sensor accuracy, user activity, and environmental conditions. Enamamu *et al.* [305] emphasise the feasibility of using physiological data from wearable devices for transparent and continuous authentication, while also admitting the difficulties associated with the unpredictability of heart rate readings. The researchers used the Discrete Wavelet Transform (DWT) to break down the bioelectrical signal into n-level detail and approximation coefficients. They then used the Biorthogonal Wavelet (bior 4.4) to extract features from the four levels of detail coefficients. Each sub-band level was classified using a Feedforward Neural Network (FF-NN). Their research likewise focused mostly on the heart rate signal itself and not the authentication process.	the Naive Bayes algorithm. It then adds continuous authentication after initial authentication to provide an additional degree of protection, utilising Heart Rate Variability (HRV). Combination with static authentication makes up for the potential weaknesses in [304][305].
Adaptive security in e-health	Gebrie [309] tackles security concerns in smart home eHealth environments by introducing a risk-based adaptive authentication system for IoT devices. The framework performs Risk Assessment, Adaptive Authentication, Smart Home e-Health Application, and Artificial Intelligence Integration to improve the accuracy of risk assessments and the adaptability of authentication methods, ultimately improving the overall security posture of IoT systems in smart home environments.	Our prototype balances usability and security by establishing an initial risk score for authentication using the Naive Bayes algorithm. It then adds continuous authentication after initial authentication to provide an additional degree of protection, utilising Heart Rate Variability (HRV).

From the above table, we can note the differences between the main adaptive authentication systems that are closely related to our work.

2.2 Adaptive Authentication in Healthcare

A Naive Bayes method for monitoring and analysing user and device activities to decide whether to authenticate or re-authenticate based on risk was proposed in Gebrie [309]. The study in a smart

home setup evaluated risks and verified device authenticity in resource-limited environments, but the model lacked validation. An enhanced MQTT protocol authentication method that incorporates a contextual risk model for continuous risk quantification on a fog node was proposed in Selvan *et al.* [289] which was for the Fog layer, focusing on risk calculation only. DuoPass, an innovative patient-centric authentication paradigm, was introduced in healthcare organisations to improve security and usability [310], with findings expected to guide the development of patient-centric, knowledge-based authentication mechanisms. Krishnan *et al.* [311] introduced an open standards-based authentication method that can be seamlessly integrated with an adaptive authentication system, enabling client identity confirmation. The study indicates that the proposed authentication method is both secure and user-friendly, making it suitable for healthcare settings. A new adaptive identification-based authentication framework was proposed in Henaien *et al.* [312] for healthcare applications in predictive, preventive, and personalised medicine, with an ontology developed for various patient abilities and capabilities. However, no formal evaluation was conducted.

2.3 Biometric Authentication

Fitbit users were tested on step count, heart rate, hybrid calorie burn, and metabolic equivalent of task, and it was concluded that behavioural biometrics do not work well during sedentary periods [313]. A mobile-based One Time Password (OTP) using a heart pulse sensor for user authentication was proposed in Deepak *et al.* [314] where the sensed pulse values were processed in the IoT 100 cloud via a Wi-Fi module. However, the work is only static and not adaptive. Adaptive in this context refers to the authentication scheme's ability to respond to perceived threats. The study by Karanikiotis *et al.* [315] suggested gestures for implicit continuous authentication on mobile devices, noting potential weaknesses in recognising new behaviours and not addressing attacking scenarios. AuthDNA adaptive authentication, as proposed in Silva *et al.* [253] uses geo, network, device, and risk to authenticate users, but is limited to keystroke dynamics and does not consider device impact on time and efficiency. A device-free authentication method using WiFi signals to capture behavioural and physiological characteristics during daily activities was proposed in Shi *et al.* [316] but its applicability may be limited to smart homes, which may not be feasible in most developing countries.

Behavioural Biometrics

Behavioural biometrics rely on user actions such as typing or gait, while physiological biometrics rely on body characteristics [317]. The former is significant in continuous authentication to enhance security by automatically identifying people and devices based on dynamic features, thereby creating an additional security layer [43]. These biometrics enable continuous user behaviour analysis, modelling, and profiling to create a profile for authentication, determining a user's legitimacy effortlessly [317][291], reducing discomfort and burden [318] providing security, continuity, transparency, and cost-effectiveness [43][287]. Intelligent adaptive authentication uses various environmental and behavioural features to identify login risk and dynamically customise the authentication process [253]. Previous research on access control has several shortcomings in the IoT landscape. Static access control mechanisms, like Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC), may not adapt to changing IoT environments, while dynamic access control, on the other hand, uses contextual features for real-time threat response [289]. Authentication includes knowledge-based, physiological-based, and behavioural-based, as illustrated in Figure 1.

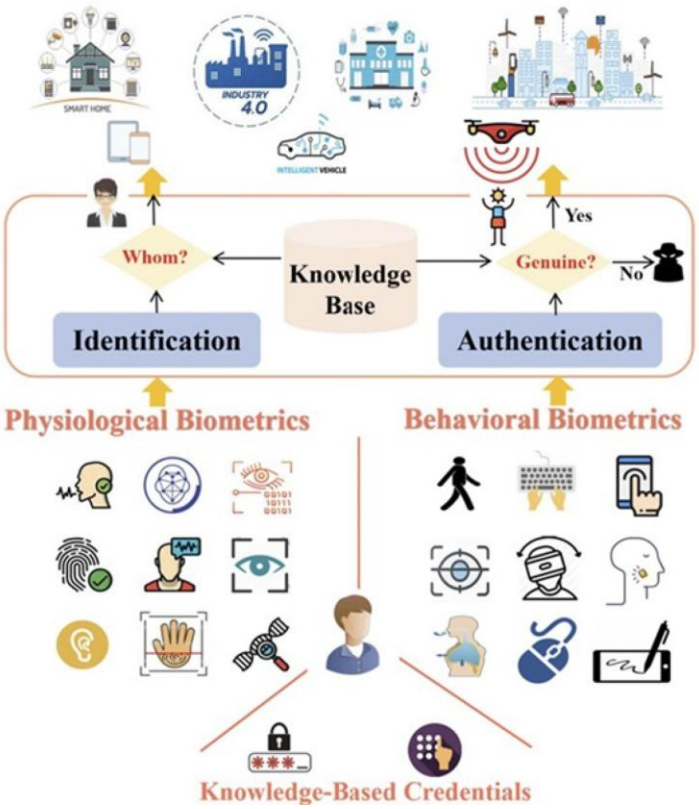


Figure 1:Three classes of user authentication. Adapted with permission from [287]

2.4 IoT Enablers: Smartphones and wearables

Smartphones, tablets, and wearables are popular IoT devices with affordable mobile sensors permeating everyone's everyday lives [253][318]. Smartphone sensors, which include motion, environmental, and position sensors [319], are widely used to monitor users' neuromotor skills, cognitive functions, and behaviours [46], and smartphones are ideal for user authentication due to their embeddedness, overcoming resource constraints and sensor deployment costs [320]. The sensors can identify individuals based on physiological and behavioural features [285], although the commonly used authentication mechanisms are explicit, making the process cumbersome and inconvenient [301]. At the same time, smartwatches use motion sensors (gyroscopes and accelerometers) to track user movements and categorise them into normal and suspicious categories. Additionally, optical sensors confirm the user's presence by determining whether the device is still worn, all while maximising energy consumption [302][321][322].

2.5 Analysis of contextual factors

Context is a set of parameters that define an entity's status, encompassing factors such as user activities, physical environment, location, time, social network situations, and network states. Adaptive authentication can be triggered by the above factors, among others. Table 2 lists contextual factors used by various researchers.

Table 14: Contextual factors used by different researchers in adaptive authentication

Contextual Factor	**Mentions**
Location (GPS), including Geo-velocity	[253][323][324][325][326]
Time (Duration) / Since last successful authentication	[289][325][326][299][327][328]
Role	[324][299][327]
Network	[286][253][325][299][327][328]
Behaviour	[253][323][325]
Resource Sensitivity	[253][323][325][299]
User Experience/speed	[286][326][299]
History	[289]
Action	[289]
Past Risk	[289]
Mobile App usage	[267][329]
User preference	[299]
Unknown or known device or browser	[326]

2.6 Risk-Based Access Control Model

A risk factor is crucial in adaptive or risk-based authentication, enabling estimation of the cost of granting or denying access for each request [289]. Because there is no explicit user interaction, risk-based authentication is widely acknowledged to provide the best balance of security and usability [323]. To determine the process of risk calculation, we analysed some risk calculation approaches used by various researchers.

2.7 Analysis of Risk Calculations

Researchers [330] calculated risk score for security as

$$Risk\ Score = \frac{total\ weight\ of\ mismatched\ attributes}{(total\ weight\ of\ all\ attributes - total\ weight\ of\ indeterminate\ attributes)} * 100 \quad (1)$$

An assessment of the security risks associated with the security triad on Fog devices was done in [289] with the outcome cost calculated based on the specific action and device context as

$$RV = \frac{(W_1 RV_C + W_2\ RV_I + W_3\ RV_A + W_4 RV_T + W_5\ RV_N + W_6 RV_D + W_7\ RV_L)}{W_i} \quad (2)$$

where Wi ∈ N, i = 1, 2, 3, 4, 5, 6, 7, 8 and RV is the Risk Value. The authors employed Fuzzy Logic, which can be enhanced by risk assessment to compute risk factors. Three machine learning algorithms: SVM, One-class SVM, and Naive Bayesian, were used in Silva *et al.* [253] for calculating risk scores.

$$Risk\ Score = \left(\left(BP + DP + PP + NP + \frac{NBP + SVMP}{2}\right) * 100\right) + parameter\_weight, \quad (3)$$

where BP = behaviour probability/percentage, DP = device probability/percentage, PP = plugin probability/percentage, NP = network probability/percentage, NBP = Naive Bayesian probability/percentage, SVMP = Support Vector Machine probability percentage, parameter_weight = updated from the static policies.

Location, MAC address, and time to calculate trustworthiness scores for implementing resiliency in adaptive multi-factor authentication systems were used in Phan [327]. The allocation of authenticators was done manually, but they calculated the trustworthiness score as

$$Trustworthiness = (IP\ Scores * Weight_{IP\ Address}) + \left(Time\ Scores * Weight_{Login\ Time}\right) + (MAC\ Address * Weight_{MAC\ Address}) \quad (4)$$

In summary, there is currently no universally applicable authentication solution for IoMT environments. The IoT environment is dynamic, interconnected, and heterogeneous, necessitating the development of mechanisms that adapt to changing context conditions, particularly without context-aware access control schemes [324]. The theoretical security offered by security mechanisms is insufficient in practice due to poor usability [253] , but the integration of various authentication mechanisms can enhance user convenience and security [58].

3.0 Proposed Approach

The proposed method utilised a hybrid mode that combined static and continuous authentication, as well as machine learning, with a particular focus on young users. The choice of continuous authentication was based on the availability of authenticators, their perceived ease of use for young users, and the need for enhanced security on young users' data. The research utilised Android smartphones with version 12 and above, along with Pine-Time smartwatches. The study did not concentrate on specific smartphone brands for app portability across various user devices. The app utilised a heart rate sensor on the smartwatch for continuous authentication, allowing real user data to be collected and analysed. The contextual features in equations 6 to 8 resulted in a conditional probability of a user being illegitimate. The smartwatch transmitted heart rate data to the smartphone via a Bluetooth connection after the initial login. This could result in either authorisation or denial of the user. This work is a continuation of our previous work [331] where we investigate continuous authentication among young users. The proposed architecture follows the framework in [250] . Users on their smartphones enrolled in the mobile application installed on their devices. The following algorithm shows the steps followed from clicking the login button to authorisation through continuous authentication.

Algorithm1. Adaptive authentication and continuous heartrate monitoring

Input: Mobile_Browser, Mobile_OS, IPAddress, Network_Type, GPS_Coordinates, Access_Time, Knowledge_based data, Physiological biometric_data, HRV Metrics, Pulse Waveform Features.

Output: Risk Score, Trust Score, Authentication Result, HRV Analysis.

1. *Start adaptive app by clicking an icon.*
2. *Start heart rate recording on the smartwatch.*
3. *Obtain user verification information:*

- User—begin signup if no account exists, or login if already registered.
- App—verifies user email address/phone number and password or PIN.

4. *Define partial conditional probabilities as weights using the Naive Bayes Theorem:*
   - App—use Naive Bayes to define conditional probabilities of deviation of input.
   - App—capture all background and active data that define a user.
5. *Calculate first-level weighted risk score:*
   - App—obtain email/username and device parameters.

   If the account is verified on the device, request an adaptive authentication PIN or password
   else
   Call other available and usable verification methods.
6. *Calculate second-level weighted risk score:*
   - Verify user against the device.

   If the user and device match, call one usable authenticator and update the trust score
   else
   Call other available and usable authenticators.
7. *Open Bluetooth on your smartphone and connect to your smartwatch once authenticated:*

   - Open Bluetooth and connect with the smartwatch if present.
8. *Baseline profiles:*
   - While the smartwatch is connected, begin profiling the user and establish baseline HRV metrics and wavelet coefficients for each user.
   - End profiling after a specific time interval.
   - Repeat the process several times to create a robust profile for the user.
9. *Thresholds and alerts:*
   - Define thresholds for acceptable deviations in HRV metrics and waveform features.
10. *Realtime monitoring:*
    - During continuous authentication in the background, compare real-time HRV metrics and pulse waveform features with baseline profiles.
    - Allow connection with consistent patterns and trigger re-authentication where deviations occur.
11. *Machine Learning Models:*
    - Use the combined data to train machine learning models that can classify or predict user identity based on HRV metrics and pulse waveform features.
12. *Iterate Through User Profiles:*

    Begin: While Trust Score < Threshold
    - Continue iteratively through each user profile, calculating the risk score and initial trust score.
    - Authenticate with available and usable authenticators, one at a time.
    - Update trust score at each iteration:
      Trust Score += Trust Score
      End

Our proposed system utilises user medical conditions to select one or more knowledge based, physiological, and behavioural authenticators based on risk scores. The collected data was then

used to test our model for usable security. Our proposed Naive Bayes based Risk Calculation is as shown in equations 6 to 8.

$$P(MDC|MOS,MB) = \frac{P(MOS|MBC,MB)P(MDC|MB)}{P(MOS|MB)} * Weight_{MDC} \quad (6)$$

Where MDC represents Mobile Device Change, MOS represents Mobile Operating System, MB represents Mobile Browser. The equation calculates the weighted scores of contextual factors based on deviation from the learned values. The same goes for Network Change, Location Change and User Change. The final risk score is the weighted sum of the contextual factors deviation scores with trust score being inverse of risk score.

$$P(S|MC,NC,LC,UC) = weighted \sum P(MC,NC,LC,UC) \quad (7)$$

$$Trust = 1 - P(S|MC,OC,NC,LC,UC) \quad (8)$$

where S = Suspicion, MDC = Mobile_Device_Change, OC = Other Device Change, NC = Network_Change, LC = Location_Change, UC = User_Change.

3.1 Population

The study aimed to assess the effectiveness of continuous authentication in patients and medical staff under the age of 50, assuming they are technologically proficient and active. However, the number of smartwatch users was limited by the availability of smartwatches.

3.1.1 Sample Size

A total of one hundred and eighty-two (182) participants were used in the study. They were made up of 108 males and 74 females. Out of 200, this represented 91% of the responses.

3.1.2 Sampling technique

The stratified systematic sampling was employed because it ensures both representation and efficiency.

3.1.3 Inclusion criteria

We included medical staff and patients who had access to smartwatches, as they were limited. The upper age limit for the young participants was 50, and smartphone ownership among patients was also an inclusion criterion.

3.1.4 Exclusion criteria

We excluded participants below the age of 18 due to diminished autonomy and those who did not own smartphones. Users interacted with the app, changing location and other contextual factors. During interaction, the app would calculate the risk score and adapt accordingly.

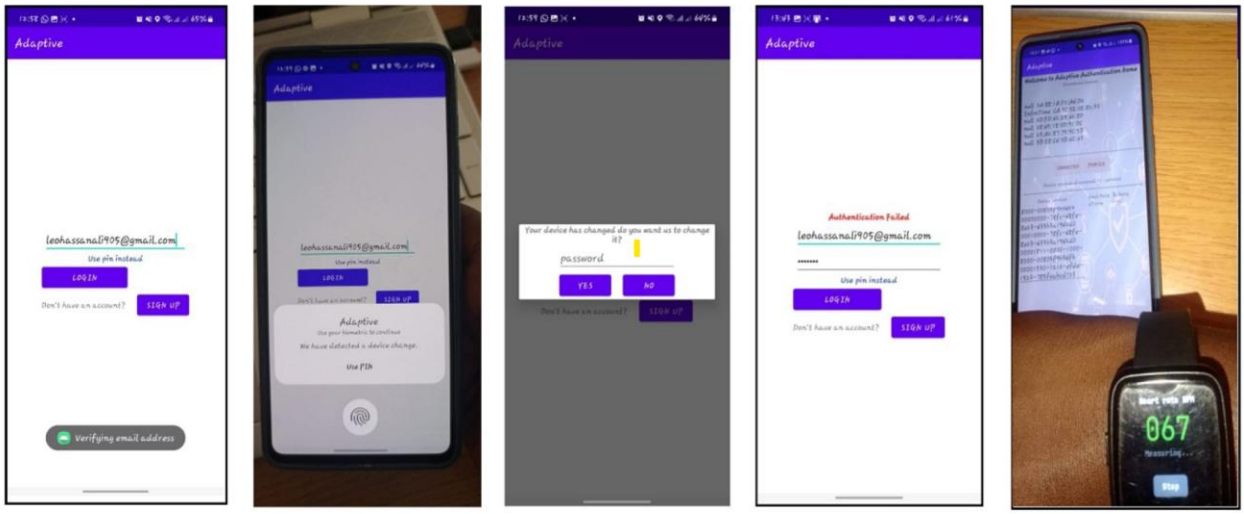
4.0 Results

4.1 Prototype

An Android App named Adaptive was developed and installed on participants' Android smartphones, which collected user contextual information from its sensors and Pine-Time smartwatch sensors. The App was created using Java, Android, Laravel Framework (PhP), MySQL, and Xampp. Fairhaven provided web hosting services using the Google Location API, as indicated by the provided URL .*http://www.adaptiveauthentication.co.zw:2082/cpsess1630754293/frontend/jupiter/index.html?login=1&post_login=18197609683.*

The Domain IP was*: {"158.220.118.132":"fairhaven.co.zw"}*

The screenshots for the mobile app interface and the smartwatch are shown in Figure 2.



a) E-mail verification b) Biometrics request c) Password change on device change detection d) Authentication failed e) Phone and watch connected

Figure 2:Proposed adaptive app screenshots

4.2 Evaluation

As mentioned in the previous section, we used the Naive Bayes algorithm in equations 6 to 8 to calculate the initial risk associated with a login attempt. Parameters in Figure 1 served as prior and derived probabilities respectively in the dynamic risk calculation. The risk score was the first component where the user was subjected to static authentication. Following the successful login, the user was then continuously authenticated using heart rate data.

4.2.1 Feature Extraction

Feature extraction was performed in python. Table 5 displays the Heart Rate Variability (HRV) estimated using SDNN and RMSSD Pulse waveform. The features include amplitude and wavelet coefficients. Figure 11 shows how a user's HRV and pulse waveform were integrated to identify them uniquely. Contextual authentication factors were recorded, including device ID, network type, and GPS position. The retrieved features were normalised and preprocessed using z-score normalisation.

4.2.2 Model training

To prevent overfitting, we separated the dataset into training (80%) and testing (20%) sets and used 5-fold cross-validation. This will be explained later. The study also utilised multi-class classifiers with evaluation metrics such as confusion matrix, accuracy, FAR, FRR, and receiver operating characteristics. Performance requirements were prioritised, focusing on reducing authentication time while maintaining security and usability. Figure 3 shows the confusion matrix and statistics for the authentication to authorisation process.

```
          Reference  Accuracy: 0.8995              Mcnemar's Test P-Value:
Prediction   0   1   95% CI: (0.8808, 0.9161)     < 2.2e-16
         0 542 118   No Information Rate: 0.5383
         1   0 514       P-Value [Acc > NIR]: <   Sensitivity: 1.0000
                     2.2e-16                      Specificity: 0.8133
                                                  Pos Pred Value: 0.8212
                     Kappa: 0.8009                Neg Pred Value: 1.0000
                                                  Prevalence: 0.4617
                                                  Detection Rate: 0.4617
                                                  Detection Prevalence: 0.
                                                  5622
                                                  Balanced Accuracy: 0.906
                                                  6

                                                  'Positive' Class: 0
```

Figure 3: Overall Confusion Matrix and Statistics of proposed system

The model exhibited good accuracy in detecting positive cases (sensitivity = 1), outperforming random guessing, and performing reliably, as confirmed by the significant McNemar's test p-value and the Kappa score of 0.8009. The authentication decision binary classification model demonstrated superior performance near 1 when considering usage context and performance measures, as evaluated using the Area Under the Receiver Operating Characteristic Curve.

Figure 4 shows the ROC curve for authentication and authorisation with the Area under the Curve (AUC) of 1.

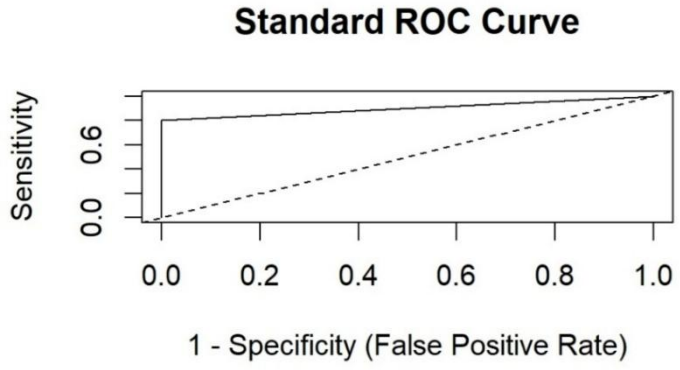


Figure 4: ROC Curve for authentication and authorisation of proposed system

The model performs very well, demonstrating robustness, excellent specificity, and moderate sensitivity, particularly in detecting actual positives, though there is a minor trade-off with precision, likely due to some false positive cases. The results of combining the AUC with additional performance indicators are shown in Table 3.

Table 15: Combination of AUC with other performance metrics on proposed system

Metric	**Value**
Sensitivity(Recall)	1
Precision (PPV)	0.81
F1_Score	0.90

4.3 Usability Evaluation

To evaluate usability, users were given a post-deployment questionnaire that they completed.

Figure 5 shows the age distribution of respondents.

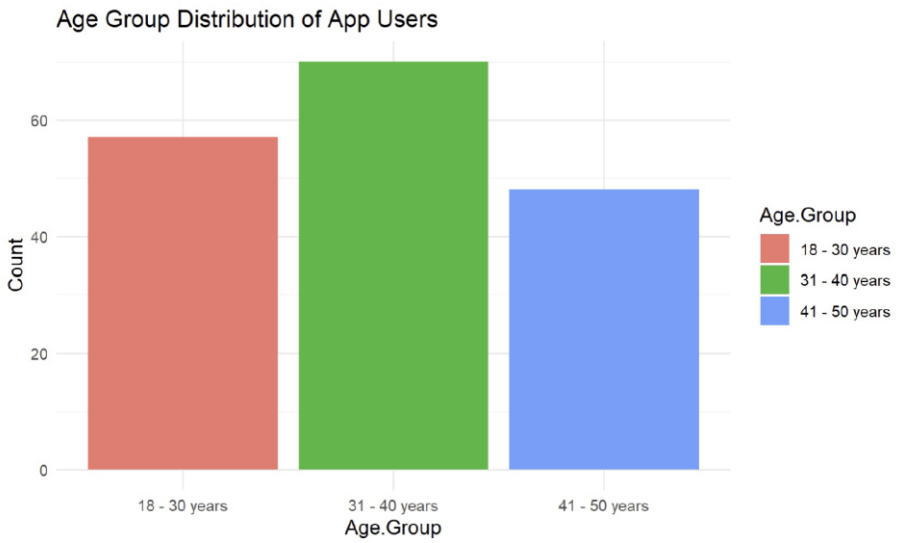


Figure 5:Age distribution of the research participants on proposed system

The 31-40 year old age group has the highest count, with slightly over 60 users, followed by the 18-30 year old age group with just below 60 users, and lastly the 41-50 year old age group with around 50 users. Several Metrics were used to assess usability.

When asked if they would recommend the app to other users, the majority of users gave it an overall satisfaction rating of between 6 and 8, suggesting that they are generally happy with it. A small percentage of users gave the app an exceptionally low rating (3 and 4), while a small number of users gave it an extremely high rating (9 and 10). A pleasant user experience is indicated by the concentration of ratings between 6 and 8, which suggests that many users, albeit not overwhelmingly, so are likely to recommend the app. False Acceptance and Rejection Rates were used to measure the usability of the model. Table 4 shows the evaluation metrics.

Table 16: Combination of AUC with other performance metrics on proposed system

Metric	**Value**
False Rejection Rate	0.19
False Acceptance Rate	0

The results indicate a trade-off between security and usability, where high security is shown by the 0% FAR, suggesting that the system is highly effective at preventing unauthorised access. However, with an FRR of 19%, the system shows moderate usability where the system might inconvenience legitimate users, which could reduce the overall user satisfaction or trust in the system. The model's 19% False Rejection Rate (FRR) suggests potential bias toward positive predictions and to address class imbalances, overfitting, and FRR reduction we employed the

Synthetic Minority Over-sampling Technique (SMOTE) and Random Over-Sampling Examples (ROSE) packages to oversample the minority class.

4.3.1 User Health Impact on authentication

Most respondents did not have any medical issues, so the question about the app's consideration of their medical problems did not apply to many. A small number of responses suggested that the app does not consider their medical conditions, but a significant portion of responses suggested that the app considers their medical conditions; however, this group is substantially smaller than those that found the question inapplicable. The model, however, reveals that visual and mental conditions have higher sensitivity than physical conditions, making authenticators more effective in identifying authorised situations.

4.4 Train Test Split and Cross-Validation

The model underwent further validation through train test split and cross-validation, utilising Confusion Matrix and Statistics.

4.4.1 Train Test Split

Figure 6 shows the confusion matrix and statistics for the train-test split option.

```
Reference          Accuracy: 0.7198             Mcnemar's Test P-Value:0.00291
Prediction 0   1   95% CI: (0.6931, 0.7453)
        0 405 192  No Information Rate:0.5383   Sensitivity: 0.7472
        1 137 440  P-Value [Acc > NIR]:< 2e-16  Specificity: 0.6962
                                                Pos Pred Value: 0.6784
                   Kappa: 0.4403                Neg Pred Value: 0.7626
                                                Prevalence: 0.4617
                                                Detection Rate: 0.3450
                                                Detection Prevalence:0.5085
                                                Balanced Accuracy:0.7217

                                                'Positive' Class: 0
```

Figure 6: Confusion matrix and statistics for the train-test split option on proposed system

The model exhibits moderate performance, with an accuracy of 71.98% and a Kappa value indicating moderate agreement beyond chance. The model's sensitivity is higher than its specificity, suggesting it is slightly better at identifying actual positives than negatives. The precision and negative predictive values suggest a reasonable balance between false positive and false negative rates.

4.4.2 Cross Validation

Access performance metrics, as well as the confusion matrix were used in cross-validation using the Random Forest classifier. Figure 7 shows the performance metrics.

```
Access performance metrics

      mtry      Accuracy       Kappa           AccuracySD      KappaSD

1     2         0.5715848      0.02410257      0.01379978      0.03177979

2     35        1.0000000      1.00000000      0.00000000      0.00000000

3     635       1.0000000      1.00000000      0.00000000      0.00000000

Access confusion matrix and other metrics

Reference          Accuracy:1                      Mcnemar's Test P-Value: NA
Prediction 0  1    95% CI:(0.9969, 1)
        0 660 0    No Information Rate:0.5622      Sensitivity:1.0000
        1 0 514    P-Value [Acc > NIR]:< 2.2e-16   Specificity:1.0000
                                                   Pos Pred Value:1.0000
                   Kappa:1                         Neg Pred Value:1.0000
                                                   Prevalence:0.5622
                                                   Detection Rate:0.5622
                                                   Detection Prevalence:0.5622
                                                   Balanced Accuracy:1.0000

                                                   'Positive' Class:0
```

Figure 7: Confusion matrix and statistics for the cross-validation option on proposed system

The model achieved perfect performance on the training data with accuracy, sensitivity, specificity, and predictive values at 100%, with a Kappa value of 1, indicating perfect agreement beyond chance, despite possible overfitting, requiring cross-validation on an independent dataset. To ensure overfitting was minimised and simplified the model, we used Random Forest with cross-validation and parameter tuning and performed early stopping-like behaviour.

4.5 Distance Analysis

We performed distance analysis to determine the effect of location on authentication. This is shown in Figure 8.

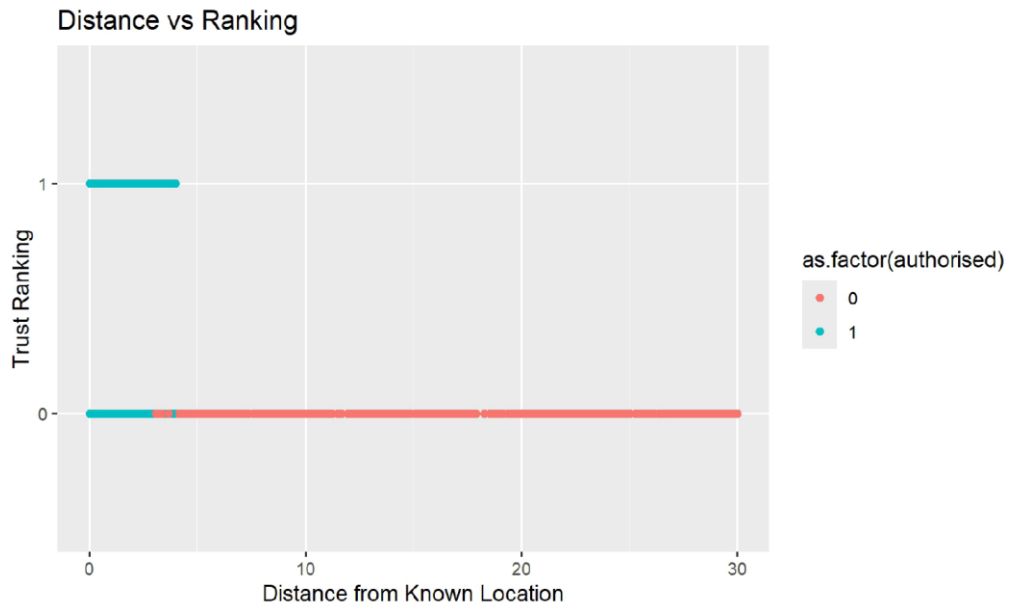


Figure 8: Distance Analysis on proposed system

Dist_ from _ epicentre and *authorised* have a statistically significant negative correlation, according to the linear regression model. The average drop in approved score is 0.045 units for each unit increase in *dist_from_epicenter*. A strong fit is shown by the model's ability to explain roughly 66.21% of the variability. According to the model and the importance of the coefficients, *dist_from_epicenter* is a significant predictor of authorised.

4.6 Heart Rate Variability for Continuous Authentication

Sample data for five users is shown with two Heart Rate Variability metrics named Standard Deviation of normal RR (NN) Intervals (SDNN) and Root Mean Square of Successive Differences (RMSSD). Table 5 shows the variability metrics.

Table 17: Heart Rate Variability Metrics

Owner_id	SDNN	RMSSD
1	12.2	12.1
2	13.2	13.1
3	13.5	13.5
4	15.6	15.5
5	13.1	13.1

These two metrics are generally associated with better heart health and lower stress, but can also be used to identify a person over a period of time. This method leverages the unique HRV patterns of each user to provide a dynamic and potentially secure authentication mechanism. Combining HRV with Pulse waveform features produced Figure 9.

	owner_id	SDNN	RMSSD	W11	W12	W13	W14	W15	W16
1	1	12.15314	12.09192	-8.5501601	3.487835	9.2573517	-0.9054282	-3.641019	3.574322
2	2	13.17839	13.11243	-0.7799733	5.899263	10.1371406	4.2152075	-12.731117	-10.196677
3	3	13.53142	13.46387	-2.8826965	1.228991	-0.5803651	16.2869242	-5.451302	-5.482752
4	4	15.61502	15.53596	7.5286172	14.820693	-0.5044298	13.5100803	2.491591	-6.438566
5	5	13.14534	13.08095	-5.8272078	1.067368	-10.9530799	-6.5224948	-8.198776	1.221769

Figure 9:Heart Rate Variability and Pulse Waveform features from proposed system

Consistent and well-known HRV patterns are required for continuous authentication, and wavelet coefficients depict the different frequency components of the pulse waveform. Because each user differs physiologically, each has a distinct pattern in their wavelet coefficients; hence, consistent and recognisable wavelet patterns can be utilised to differentiate users. This gives a bar plot showing the magnitude of each wavelet coefficient for a particular user as shown in Figure 10 a) and the summarised HRV metrics in Figure 10 b).

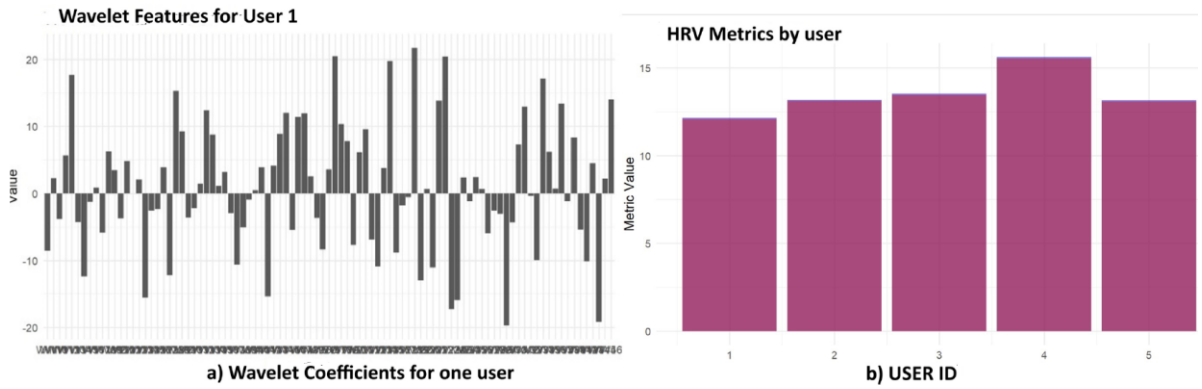


Figure 10: Wavelet Coefficients for one user and Heart Rate Variability for 5 users

4.7 Effectiveness

Our model's effectiveness in predicting user access was evaluated using a confusion matrix and metrics for the initial login attempt before continuous authentication, with low, medium, and high success ratios, ensuring the representation of different users. This evaluation is crucial for ensuring the model's reliability and usability since it aims to balance both usability and security. This work also used continuous authentication, which ran in the background, making it difficult to measure completion time. Instead, we used the success ratio to measure effectiveness and system intrusion, though there may have been errors in incorrectly classifying legitimate users as intruders. Figure 11 shows part of the success ratio results.

	owner_id	total_logins	successful_logins	success_ratio
1	1	10	7	0.7
2	2	6	1	0.167
3	3	7	6	0.857
4	4	6	2	0.333
5	5	5	4	0.8
6	6	6	3	0.5
7	7	6	2	0.333
8	8	6	2	0.333
9	9	6	3	0.5
10	10	7	5	0.714

Figure 11: Snippet of success ratio

Task completion time was also utilised to assess effectiveness, which was calculated from the moment of login to approval. This included both static and continuous authentication for 8364 records, with minimum and maximum timings provided in Table 6.

Table 18:Task Completion Times

Minimum Time (s)	8
Maximum Time (s)	38

4.8 Efficiency

We measured the efficiency of our model by calculating the FRR and FAR, which both had low values of 0.19 and 0, respectively, as shown in Table 4, implying efficient classification. We also used trust ranking, average success ratio, overall completion rate, and the average success ratio.

4.9 Dynamic trust and reputation management

To handle dynamic trust and reputation management in our model, we introduced adaptive trust scoring based on user conduct, device reputation, and contextual factors. We assigned trust scores. based on historical authentication success, behaviour, and security incidents, these scores were dynamically updated with each authentication attempt. In reputation management, we tracked device reputation based on anomalies and punished suspicious behaviours as seen in Figure 9, where trust decreased with distance from a known location. Failed attempts would result in the app locking. The trust score was updated automatically based on new evidence using the Bayes rule. Figure 12 shows the sample data collected by the prototype that was calculated based on device, context and trust.

record	p_device	p_other_de	p_network	p_location	p_habit	risk	trust	prob_devic	has_menta	has_visual	has_physic	prob_user_	prob_user_	prob_user_	ranking	authorised	dist_from_epicenter
79	0	0	0.1	0	0	0.1	0.9	0	1	0	1	0.15	0.3	0.05	0.5	1	3.138175
73	0.15	0	0.2	0.3	0	0.65	0.35	0	1	0	1	0	0.25	0.05	0.3	0	9.812652
67	0.15	0	0	0.15	0.2	0.5	0.5	0	1	0	1	0.05	0.25	0.45	0.75	1	0.951686
65	0.15	0	0	0.3	0.2	0.65	0.35	0	1	0	1	0.15	0.25	0.45	0.85	1	0.621069
64	0.3	0	0.2	0	0.1	0.6	0.4	0	1	0	1	0	0.1	0.1	0.2	0	28.00314
63	0.15	0	0.1	0.15	0.2	0.6	0.4	0	1	0	1	0.2	0.1	0.05	0.35	0	14.83331
62	0.3	0	0.2	0.15	0.1	0.75	0.25	0	1	0	1	0.2	0	0.4	0.6	1	3.212223
61	0.15	0	0	0	0.2	0.35	0.65	0	1	0	1	0.2	0.25	0.25	0.7	1	0.408075
60	0	0	0.1	0.15	0.2	0.45	0.55	0	1	0	1	0.05	0.2	0.4	0.65	1	1.495232

Figure 9: Authentication data collected by the prototype

5.0 Discussion

The overall results in terms of accuracy were within an acceptable range, and the model is generally robust with a modest bias towards accurately predicting positive cases in both static and continuous authentication. Class imbalance, feature selection, model complexity, sampling techniques, training data quality, and data preprocessing could all have contributed to this bias. To curb this bias, we performed cross-validation, although there is a need to assess the distribution of classes, carry out feature importance analysis, model re-calibration, and alternative algorithm consideration to lessen the issue. From the AUC analysis, we observed that while the model excels at ensuring that negative instances are correctly identified, it has some shortcomings in capturing all positive instances. Further tuning, retraining, using more features, or adjusting the decision threshold might be necessary to improve precision. In the usability evaluation, we observed that the model exhibits excellent specificity with moderate sensitivity. However, while it excels at ensuring that negative instances are correctly identified, it has some shortcomings in capturing all positive instances. Efforts might be needed to reduce the false rejection rate, potentially by retraining the model, using more features, or adjusting the decision threshold. With an FRR of 19% in Table 4, the model shows moderate usability, where the system might inconvenience legitimate users, which could reduce the overall user satisfaction or trust in the system. The modal age group of 31 to 40 years most likely strikes a balance between job, personal health, and family obligations, which increases the use of technology for productivity and health tracking.

On the other hand, people in the 18 to 30 age range are more likely to utilise technology frequently but may not be as engaged in the specific app or system under consideration. Those between the ages of 41 and 50 might be less likely to acquire newer technologies, depending on how comfortable and familiar they are with current apps. Lower usability metrics scores like ease of use, overall performance, and quality of service indicate that user satisfaction in these areas varies more than in other areas. The trust and acceptance test shows that the model authenticated most of

the users tested, and the presence of the minimum (0) and maximum (1) values indicates that there are instances of both complete lack of trust and complete trust, which is typical of the cases tested. These results validate the idea behind the model that authentication must not be binary but must be based on the actual trust score to determine how difficult the authentication process must be for a particular user. The health impact test shows mental and physical medical conditions exhibiting higher sensitivity, suggesting that authenticators based on these conditions are more effective at accurately identifying authorised situations. Further evaluation using the train-test split shows that there is a significant difference in the types of errors made by the model. Cross-validation shows that while these results indicate that the model performs exceptionally well on the given data, it is important to consider the possibility of overfitting. Therefore, it's crucial to validate the model on an independent test set to ensure its generalisability and robustness. Distance analysis shows a significant negative correlation between Dist_ from _ epicentre and authorised, hence, the former is a significant predictor of authorised. When measuring effectiveness, as shown in Figure 12, there is a mix of success rates classified as high, moderate, and low. The low success ratios may also be attributed to several factors, like user experience, network, and medical conditions, among other things. The reasons for unsuccessful logins must be investigated, and when the success rate is low, the appropriateness of the authentication techniques must be assessed. Any physical or medical conditions that may pose problems must be identified so that system improvements can be made. Heartrate Variability also showed the potential to uniquely identify users; therefore, it can be used for continuous authentication. However, for continuous authentication or any health-related applications, it is necessary to complement heart rate data with other data, such as step count and gyroscope data for more accurate evaluations, as variations in HRV may be due to different factors like time of day, activity level, and health conditions.

It is important to note that while our algorithm correctly identifies the need for thresholds, from similar research [324][325] these are not static, predefined numbers. Instead, they are dynamic, personalised values that are either statistically calculated from an individual's baseline data or learned by a machine learning model to achieve an optimal balance between security and user convenience.

Given that the modal age group is 31 to 40 years old, the main drawbacks of the sample strategies used on our dataset are the possibility of selection bias and the lack of generalisability. This suggests that the young users' age demographics are not evenly represented in the sample, and

that the other age groups (18–30 and 41–50) may use technology in various ways. Because the sample isn't a realistic representation of the user base as a whole, the model's performance and conclusions could not translate well to younger or older groups due to selection bias. The model's impressive performance on the tested people might not translate to a more varied user base. Bias may also have resulted from class disparities, as was mentioned earlier. The observed bias towards "accurately predicting positive cases" may result from the model's learning to predict the majority class more frequently, but it may also have "shortcomings in capturing all positive instances" and a "modest bias." Determining whether the sample is representative of the target population may be impossible due to the sampling used in the study and the inclusion criteria for the participants.

Additionally, overfitting could be introduced by the absence of an independent validation set. Most likely, a straightforward train-test split of the same dataset or cross-validation on the same dataset were used for the present validation. Even cross-validation will carry the bias if the dataset was sampled biasedly in the first place. One significant drawback that hinders a thorough evaluation of the model's performance on the general population is the absence of a fully independent, unseen test set (gathered from a different sample). Finally, health condition sampling may introduce bias. This calls into question the sampling strategy used for those with medical issues. The results pertaining to their authentication performance may not be representative if the sampling was biased. The creation of a probabilistic trust score [332], which generates a posterior probability score rather than a binary "authenticated/not authenticated" output, is one of the main benefits of the Naive Bayes-based adaptive authentication method for Android user identification. This enables a flexible, adaptive authentication process in which a user's access level or required authentication strength is determined by a continuous value rather than a simple pass/pass/failure [333]. The app is for Android, a platform for mobile devices where processing speed and battery life are essential [334]. Another benefit is computational efficiency for mobile devices. Naive Bayes is renowned for its quick training and classification times and little computational overhead. Because of its straightforward design, it is ideal for deployment on a device with limited resources, such as a smartphone, guaranteeing that the static or continuous authentication procedure won't drain the battery too much or degrade the user experience. Higher "ease of use" and "overall performance" scores are a direct result of this. Additionally, the method can handle continuous and high-dimensional data to identify users in a unique way [335]. Naive Bayes' simplicity and interpretability are additional benefits that make it a preferred tool [336]. Compared to more

complicated models like neural networks, Naive Bayes is a transparent, straightforward model that is simpler to comprehend and debug. Tasks like feature importance analysis and model recalibration are made easier by this interpretability. Robustness to overfitting is an additional benefit [337]. Naive Bayes is less likely to overfit than more intricate models with several parameters because of its "naive" independence assumption, particularly when there is a lack of data.

6.0 Conclusion and future work

The model demonstrates strong performance in terms of calculating risk, trust, and authorisation decisions. It effectively integrates user behaviour, environmental context, and health conditions to provide adaptive and secure user authentication. However, the observed difference in accuracy between training and cross-validation suggests that the model should be further tested and possibly tuned on more diverse data to ensure it generalises well across different scenarios. There is a need for future model development to address the trade-offs of false positives based on the overall confusion matrix. To capture more complex user behaviours and environmental changes, future work will look at integrating machine learning models and context-aware analytics to dynamically adapt the authentication process in real-time. This will involve enhanced risk scoring models, explainable AI in risk assessment, and personalisation and accessibility. On health impact, further analysis and investigation of features that contribute most to predictions and their impact on model performance may be required. Cross-validation may also be required to validate the model on independent datasets, together with diversifying the training data to cover a wider range of user behaviours and situations. It will also involve exploring additional features while keeping an eye on users' health status and modifying authentication procedures as needed to accommodate any changes. To ensure optimal performance, we will also routinely adjust the model's parameters and validate them using fresh data. To integrate multi-party data collaboration and privacy-preserving techniques into our IoMT authentication model in order to reduce data centralisation, we will use techniques such as federated learning and differential privacy, but further research will be required for optimisation on an Android smartphone. There is also a need to improve model training by using an appropriate classifier, such as RF for interpretability and robustness, XGBoost for high-performance risk assessment, and LSTM for time series HRV patterns. Although the integration of smartphone and smartwatch sensors for continuous authentication shows promise; to fully realise its potential in IoMT, it is imperative to address the inherent obstacles.

4 Overall Conclusion

We designed and developed an ML-based adaptive user authentication framework that adapts to user profiles and context during login to determine the likelihood of an attempt being illegitimate before assigning appropriate authentication mechanisms. This edge-centric framework fuses the Naive Bayes classifier and CoFRA model to determine the risk associated with a login attempt based on biometric wearable sensor data, non-biometric smartphone sensor data, and some predefined data. This research contributes to the academic body of knowledge on usable security and has been disseminated through seminars and conferences.

We then went on to refine the risk classification framework, using the Naïve Bayes Theorem to calculate the risk associated with login attempts. Unlike most authentication mechanisms that classify users as either legitimate or not (with a few extending to three classes), we noted that current authentication tends to generalise users, treating them equally. This often leads to highly suspicious users being "punished" with the same authentication rigor as medium-risk users, making the process less user-friendly. To address this, we proposed assigning weights to contextual factors and calculating the risk of a login attempt based on the deviation of these factors from known profiles. We tested our risk calculation model using Naïve-Based and non-Naïve-Based multiclass classification algorithms via PYTHON simulation. Our findings indicate that the Naïve Bayes Theorem is suitable for risk calculation, while for multiclassification, some non-Naïve Bayes algorithms perform best. We also concluded that some weaknesses of Naïve Bayes stem from a generalised point of view.

Having modelled and evaluated the risk calculation mechanism through simulations, we then evaluated the framework in a mobile Android App outside the lab environment with real test subjects from both young and old age groups.

4.1 Key Contributions and Findings

This research directly addresses critical gaps in IoMT security and usability by presenting a novel framework for adaptive user authentication based on Machine Learning (ML). This framework, meticulously broken down into three separate sections, represents a major step towards safe and easy access to medical IoT resources.

Part I: User-Centred Design and Prototype Development

Part I established the groundwork with the User-Centred Design (UCD) of the ML-based adaptive user authentication framework. This human-centric approach guaranteed that the proposed solution would be both technically robust and intuitively usable. This section also resulted in the creation of an Android application that used a PineTime smartwatch to demonstrate the framework's functionality in practice.

Part II: Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication

In Part II, "Weighted Naïve Bayes Multi-User Classification for Adaptive Authentication," we explored the fundamental machine learning element. The edge-centric approach of the framework was emphasised, combining the CoFRA model and the Naive Bayes classifier to dynamically evaluate the risk and legitimacy of every login attempt. Our comparisons of several machine learning algorithms, such as Decision Trees, SVM, XGBoost, Random Forests, and various Naive Bayes variants, showed that weighted datasets produced better results. This demonstrated the crucial role of data properties and splitting techniques in obtaining precise classification. Naive Bayes proved to be the best classifier for up to three authentication classes, but other classifiers performed exceptionally well in multi-classification cases.

Part III: Android-Based IoMT Adaptive User Authentication Prototypes for Diverse Age Groups

Part III provided two specialised implementations of the framework: "Naïve Bayes Based Android Adaptive User Authentication Prototype for Young Internet of Medical Things Users" and "An Android-Based Internet Of Medical Things Adaptive User Authentication And Authorisation Model For The Elderly." These applications demonstrated how the framework may be tailored to a wide range of user types. A crucial conclusion from our user research showed that, irrespective of age, experience, or level of ICT ability, users consistently preferred using simple physiological biometrics for authentication. The Android application, which uses a wide range of inputs such as biometric wearable sensor data, non-biometric smartphone sensor data, and predefined user contextual information, was designed and implemented with this insightful knowledge in mind. Despite some noted shortcomings, such as class imbalance and a 19% false rejection rate during simulations, post-deployment evaluations confirmed excellent accuracy (100% and 98.6% in useful security metrics) and high user acceptability.

4.2 Overall Evaluation

When compared to existing solutions, the proposed adaptive authentication system for IoMT exhibits notable performance gains and adaptability. Its capacity to deliver sophisticated risk assessment, balance usability and security, and leverage of a variety of contextual data for personalisation are the main enhancements.

Quantitative Performance Evaluation

Several specific metrics that quantify the system's performance and superiority have been presented:

- *Usable Security Accuracy*: The prototype demonstrated an impressive 100% and 98.6% accuracy in useful security metrics in the post-deployment evaluation for the elderly users. This shows that the proposed framework can accomplish both, which is a significant advance over conventional systems that frequently compromise usability for security or vice versa.
- *False Rejection Rate (FRR):* The model's 19% false rejection rate (FRR) during simulations is a significant quantitative constraint, despite the fact that it prioritises accurate positive predictions. This indicates that in its current condition, the system improperly rejects a genuine user almost one out of every five attempts, a problem that needs to be fixed in the future to increase accuracy and usability.
- *Performance with Weighted Data*: The research found that employing a weighted dataset regularly outperformed its unweighted equivalent. This indicates a measurable increase in algorithmic effectiveness, which is directly related to the novel hybrid algorithm that combines contextual and feature weights.
- *Multi-Class Classification Performance*: The thesis notes that the Naïve Bayes method works well for up to three authentication classes and is appropriate for risk calculation. But after five or six lessons, its performance declines. Other algorithms, such as Random Forests, SVM, XGBoost, and Decision Trees, performed better in these multi-class settings. This offers a straightforward comparison and a clear route for further optimisation, indicating that other classifiers are more appropriate for more general multi-classification tasks, even though the Naïve Bayes model works well for conditional risk computation.

4.3 Adaptability of the Algorithm

The main advantage of the proposed algorithm is its flexibility, which enables it to move beyond the limitations of static authentication methods.

- *Personalised Authentication*: Based on individual attributes like age, health, and user profiles, the framework constantly modifies its authentication procedure. The creation of two separate prototypes—one for young users and one for older users—that recognise their varying degrees of technological involvement serves as the greatest example of this. Each group's authentication flows are customised by the system, guaranteeing a safe but user-friendly experience.
- *Contextual-Awareness*: The risk of a login attempt is determined by the algorithm using deviations of contextual factors from the known that occur at login time. This comprises predetermined contextual data, non-biometric smartphone sensors, and biometric wearable sensor data. This enables the system to react instantly to modifications in the user's surroundings.
- *Nuanced Risk Classification*: In contrast to binary or three-class solutions [42–45], the suggested framework divides login attempts into six risk categories. The algorithm can apply different levels of authentication rigour depending on the real danger associated with a user by allocating people on a scale from zero to one, which makes the procedure more adaptable and user-friendly.

4.4 Novel Scientific Aspects and Significance

This research addresses important limitations in the current landscape of IoMT authentication by presenting several novel scientific facets. This study is significant because it redefines the balance between security and usability using a user-centric, context-aware approach.

Novel Scientific Aspects

The most significant contributions of this work are the innovative methods and frameworks proposed to enhance IoMT security.

- *Adaptive, Multi-Class Authentication Framework*: This study presents an edge-centric paradigm that divides users into six different risk classes, in contrast to the majority of current solutions that employ binary (legitimate or not) or up to three-class classifications.

- A more sophisticated and "friendly" authentication procedure is made possible by this granular approach, in which the level of authentication rigour is proportionate to the predicted risk.
- *Hybrid Algorithm for Risk Calculation*: The study proposes a novel hybrid algorithm that incorporates feature and contextual weights into the Naïve Bayes algorithm. In order to integrate feature and contextual weights into the Naïve Bayes algorithm, the paper suggests a novel hybrid approach. This is a direct attempt to address the Naïve Bayes model's well-known conditional independence bias. The system gives contextual factors weights according to how much they deviate from a known user profile, which results in a more reliable and accurate risk assessment.
- *Fusion of Models for Edge-Centric Design*: The framework fuses the Naïve Bayes classifier and the CoFRA model to dynamically evaluate the risk associated with a login attempt. This edge-centric approach processes data from biometric wearables and smartphones directly on the device, reducing latency.
- *User-Centric Design and Demographic Tailoring*: The research's application of a User-Centred Design (UCD) approach to include user preferences and backgrounds is a novel aspect in this discipline. The work explicitly develops and evaluates a number of prototypes for both young and old users, acknowledging that a one-size-fits-all strategy is pointless. A research gap on the usability of security for a variety of demographics is immediately addressed by this tailored approach.

4.5 Significance in the Current Research Landscape

This work is significant because it directly addresses critical trade-offs and overlooked aspects in the field of IoMT security.

- **Redefining the Security-Usability Balance:** The research's core objective is to strike a delicate balance between security and usability, a challenge that is frequently a source of friction in system design. By demonstrating high accuracy in usable security metrics and adapting to user preferences (e.g., preference for simple physiological biometrics), the framework shows that strong security does not have to come at the expense of a poor user experience.
- **Advancing the Usable Security Body of Knowledge:** This research contributes to the academic understanding of "usable security," particularly in a sensitive and critical field

like healthcare. It provides a new model and empirical evidence that can be used by other researchers to design more effective and accepted security solutions for IoMT.

- **Promoting Health and Well-being:** By developing a secure and user-friendly system, the research aims to increase user compliance with security protocols. This, in turn, promotes the adoption of IoMT in healthcare, which can improve patient care, lessen the burden on caregivers, and ultimately contribute to the achievement of Sustainable Development Goal (SDG) 3, which focuses on ensuring healthy lives and promoting well-being for all.

4.6 Limitations

We observed several limitations in the overall research, particularly concerning the performance of the machine learning models and the practical implementation of the prototypes. About model performance and classification, the following limitations exist:

- *Performance with Multiple Classes:* While the Naïve Bayes theorem proved suitable for risk calculation and performed commendably for up to three risk classes, its performance declined when classifying users into five or six distinct risk classes. For multi-classification tasks, other algorithms such as Random Forests, SVM, XGBoost, and Decision Trees performed better. In order to increase classification accuracy for a greater number of classes, the researchers intend to investigate feature relevance and engineering in their next work.
- *Naive Bayes Conditional Independence Bias:* There is he inherent conditional independence bias in the Naïve Bayes algorithm, which we tried to address by developing a hybrid algorithm incorporating feature and contextual weights.
- *Class Imbalance and Overfitting:* The model for young IoMT users faced limitations such as class imbalance, feature selection issues, and overfitting, which led to a false rejection rate (FRR) of 19%.

On prototype implementation and usability, the following limitations exist:

- *Limited Scope of Testing:* Although the prototypes were tested in a laboratory environment and outside the laboratory, testing was not in a large-scale, real-world healthcare environment with thousands of users. Future work needs to scale up the model for real-world deployment and evaluate its computational resource needs.

- *Hardware and Design Issues:* From the users' perspective, a few areas need further refinement to improve the Android app's accuracy, usability, and security. These areas include hardware compatibility, the app's look and feel, and overall reliability.
- *Limited Data and Context:* The ability of the model to catch all positive cases is impacted by its moderate sensitivity. Future research must use more advanced machine learning models and context-aware analytics to capture increasingly complex user behaviours and environmental changes.

Other limitations relate to data privacy and security emanating from:

- *Centralised Data:* The current model relies on a more centralised data approach, which can pose privacy risks. Future work should integrate multi-party data collaboration and privacy-preserving techniques, such as federated learning and differential privacy, to reduce data centralisation.
- *Generalisability:* While the model shows potential for generalisation beyond the initial test regions, there is a need for further refinement to ensure this.

This page has been intentionally left blank.

5 Future Work

Ultimately, this research provides a context-aware and user-centric authentication solution that dynamically adjusts to personal characteristics such as age, risk scores, and medical problems. This flexibility is essential for striking a vital balance between strong security and smooth use, two goals that frequently clash in system design. This adaptive authentication strategy greatly improves patient care, lessens carer burdens, and advances the achievement of Sustainable Development Goal (SDG) 3 ("Ensure healthy lives and promote well-being for all at all ages") by increasing technology adherence and building trust in digital health solutions. This thesis demonstrates that a safe, useful, and adaptive authentication system is not only possible but also necessary for successfully integrating IoMT into global healthcare and paving the path for a healthier and more connected future.

On the risk calculation component, future work will involve looking at the characteristics that lead to incorrect classifications in five and six classes through examining the models' feature relevance. Feature engineering will also be explored to distinguish between classes where performance is lower. Efforts can also be made to try an ensemble approach that combines several model predictions to increase robustness with fine-tuning attributes and weighted techniques in Android app construction.

On the actual prototype evaluation, future work will encompass scaling up the model for real-world deployment, especially in a healthcare setting with thousands of users. Given that end-user devices are mobile, attention will be kept on the computational resources needed for such scalability so that the technology cost remains low. On usability, future work will look at areas that need improvement, which include hardware compatibility, look and feel, as well as overall reliability.

To capture more complex user behaviours and environmental changes, future work will focus on integrating machine learning models and context-aware analytics to dynamically adapt the authentication process in real-time. This will involve enhanced risk scoring models, explainable AI (XAI) in risk assessment, and personalisation and accessibility. Future work will also integrate multi-party data collaboration and privacy-preserving techniques into our IoMT authentication model to reduce data centralisation, using techniques such as federated learning and differential privacy, though further research will be required for optimisation on an Android smartphone. Work

will also be done to improve model training by using appropriate classifiers, such as Random Forest for interpretability and robustness, XGBoost for high-performance risk assessment, and LSTM for time series HRV patterns. Additionally, investigating sophisticated risk assessment techniques will enhance the framework's functionality and enable even more proactive and detailed security measures.

6 References

[1] A. A. Shaikh, N. S. Gupta, A. Din, M. Khan, and H. T. Artist, "Android and Internet of Things (IOT) Based Alzheimer Care / Rehabilitation System to Moniter," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 3, pp. 5531–5539, 2017, doi: 10.15680/IJIRCCE.2017.

[2] WHO, "Sustainable Development Goals," 2022. [Online]. Available: https://www.who.int/health-topics/sustainable-development-goals#tab=tab_1

[3] F. Alsubaei, A. Abuhussein, and S. Shiva, "Ontology-Based Security Recommendation for the Internet of Medical Things," *IEEE Access*, vol. 7, pp. 48948–48960, 2019, doi: 10.1109/ACCESS.2019.2910087.

[4] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards Security on Internet of Things: Applications and Challenges in Technology," *Procedia Comput Sci*, vol. 141, pp. 199–206, 2018, doi: https://doi.org/10.1016/j.procs.2018.10.168.

[5] P. Keikhosrokiani, "Introduction to Mobile Medical Information System (mMIS) development," in *Perspectives in the Development of Mobile Medical Information Systems*, Academic Press, 2020, ch. Chapter 1, pp. 1–22.

[6] M. Banda, "IoT adoption in Africa - Intelligent CIO Africa," 2021. [Online]. Available: https://www.intelligentcio.com/africa/2021/03/03/iot-adoption-in-africa/

[7] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain," *Journal of Communications*, vol. 12, no. 4, pp. 240–247, 2017, doi: 10.12720/jcm.12.4.240-247.

[8] I. Niyonambaza, M. Zennaro, and A. Uwitonze, "Predictive maintenance (Pdm) structure using internet of things (iot) for mechanical equipment used into hospitals in Rwanda," *Future Internet*, vol. 12, no. 12, pp. 1–23, 2020, doi: 10.3390/fi12120224.

[9] K. Bhupinder, "How Can AI and IoT Help in the Fight Against the COVID-19 Pandemic? | InnovationManagement," 2020. [Online]. Available: https://innovationmanagement.se/2020/06/10/how-can-ai-and-iot-help-in-the-fight-against-the-covid-19-pandemic/

[10] WHO, "Robots use in Rwanda to fight against COVID-19 | WHO | Regional Office for Africa," WHO. Accessed: Mar. 31, 2021. [Online]. Available: https://www.afro.who.int/news/robots-use-rwanda-fight-against-covid-19

[11] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[12] H. Zakaria, N. Azaliah, A. Bakar, N. H. Hassan, and S. Yaacob, "ScienceDirect ScienceDirect IoT Security Risk Management Model for Secured Practice in IoT Security Risk Management Model for Secured Practice in Healthcare Environment Healthcare Environment," *Procedia Comput Sci*, vol. 161, pp. 1241–1248, 2019, doi: 10.1016/j.procs.2019.11.238.

[13] A. Elshimi, "Using IoT to Fight COVID-19 Pandemic - EE Times Asia," 2020. [Online]. Available: https://www.eetasia.com/using-iot-to-fight-covid-19-pandemic/

[14] Rahman and Shaban, "Escape from COVID-19 quarantine: Uganda convicts six Chinese | Africanews," 2020. [Online]. Available: https://www.africanews.com/2020/04/22/uganda-arraigns-chinese-quarantine-escapees-after-treatment//

[15] Grand View Research, "Internet of Medical Things Market | Industry Report, 2030," Market Analysis Report. Accessed: May 19, 2025. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/internet-of-medical-things-iomt-market-report

[16] A. A. Atayero, S. O. Oluwatobi, and P. O. Alege, "An Assessment of the Internet of Things (IoT) Adoption Readiness of Sub-Saharan Africa," *Journal of South African Business Research*, vol. 2016, 2016, doi: 10.5171/2016.321563.

[17] E. Nigussie, T. O. Olwal, A. Lemma, F. Mekuria, and B. Peterson, "IoT architecture for enhancing rural societal services in sub-Saharan Africa," *Procedia Comput Sci*, vol. 177, pp. 338–344, 2020, doi: 10.1016/j.procs.2020.10.045.

[18] CSIR and Erricson, "Making 5G a reality for Africa," 2018.

[19] C. C. Dupont, M. Vecchio, C. Pham, B. Diop, C. C. Dupont, and S. Koffi, "An open IoT platform to promote eco-sustainable innovation in Western Africa: Real urban and rural testbeds," *Wirel Commun Mob Comput*, vol. 2018, 2018, doi: 10.1155/2018/1028578.

[20] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu§, N. Constant, and and K. Mankodiya, "Towards Fog-driven IoT eHealth : Promises and Challenges of IoT in Medicine and Healthcare," *Future Generation Computer Systems,659-676.*, vol. 78, no. 2, pp. 659–676, 2018, doi: doi: 10.1016/j.future.2017.04.036.

[21] A. Bisi, "Evaluating the Relationship Between Information Technology Adoption and Healthcare Outcomes in Sub-Saharan Africa," *African Journal of Information and Knowledge Management*, vol. 2, no. 1, pp. 37–48, Jan. 2024, doi: 10.47604/ajikm.2267.

[22] G. S. Kuaban *et al.*, "An IoT Course Program to Foster the Adoption of IoT Driven Food and Agriculture in Sub-Saharan Africa (SSA)," in *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2022, pp. 1–7. doi: 10.1109/ICECET55527.2022.9872825.

[23] Huawei, "iot_security_white_paper_2018_v2(huawei).pdf," 2018.

[24] D. G. Aneela, I. A. Anusha, K. Malavika, and R. Saripalle, "Research Trends of Network Security in IoT," *International Journal of Innovative Studies in Sciences and Engineering Technology*, vol. 3, no. 9, pp. 6–10, 2017.

[25] S. Al-Isma'ili, G.-Z. Lo, B. P., Thiemjarus, S., King, R., and Yang, and A. Al Isma'ili, S., Li, M., Shen, J., He, Q. & Alghazi, "African Societal Challenges Transformation through IoT," in *21st Pacific Asia Conference on Information system(PACIS 2017)*, 2017, pp. 1–9.

[26] Y. Acar, S. Fahl, and M. L. Mazurek, "You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users," *Proceedings - 2016 IEEE Cybersecurity Development, SecDev 2016*, pp. 3–8, 2017, doi: 10.1109/SecDev.2016.013.

[27] L. Coll and R. Simpson, "The Internet of Things and Challenges for Consumer Protection," *consumersinternational*, no. April, pp. 1–122, 2016.

[28] S. Boudko and H. Abie, "Adaptive Cybersecurity Framework for Healthcare Internet of Things," *International Symposium on Medical Information and Communication Technology, ISMICT*, vol. 2019-May, no. 1, pp. 1–6, 2019, doi: 10.1109/ISMICT.2019.8743905.

[29] R. Chow, "The last mile for IoT privacy," *IEEE Secur Priv*, vol. 15, no. 6, pp. 73–76, 2017.

[30] M. S. Gaur, S. Kumar, N. K. Gaur, and P. S. Sharma, "Persuasive Factors and Weakness for Security Vulnerabilities in BIG IOT Data in Healthcare Solution," *J Phys Conf Ser*, vol. 2007, no. 1, 2021, doi: 10.1088/1742-6596/2007/1/012046.

[31] I. Tot, K. Lalović, and M. Brzaković, "Security Mechanisms in Iot," in *The 9th International Conference on Business Information Security BISEC 2017At: Belgrade*, 2017.

[32] A. A. Mawgoud, A. I. Karadawy, and B. S. Tawfik, "A secure authentication technique in internet of medical things through machine learning," 2019. doi: 10.6084/m9.figshare.13311479.v2.

[33] J. Maloff, "Perceptions of Responsibility for Remote Implantable or Wearable Medical Device Network Security: A Qualitative Analysis," Colorado Technical University, 2022.

[34] Ordr, "IoMT and its Transformative Impact on Healthcare Security - Ordr," What is IoMT? Accessed: May 21, 2025. [Online]. Available: https://ordr.net/article/what-is-iomt

[35] "Cybersecurity Risks With Internet Connected Medical Devices | Enlyte." Accessed: May 21, 2025. [Online]. Available: https://www.enlyte.com/insights/article/specialty-physical-medicine/specialty-solutions-spotlight-cybersecurity-risks

[36] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, "A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches," *PeerJ Comput Sci*, vol. 7, p. e414, Mar. 2021, doi: 10.7717/PEERJ-CS.414.

[37] M. Alalhareth and S. C. Hong, "Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems," *Sensors (Basel)*, vol. 24, no. 11, p. 3519, Jun. 2024, doi: 10.3390/S24113519.

[38] "Why medical equipment vulnerability remediation is not one-size-fits-all - TRIMEDX." Accessed: May 21, 2025. [Online]. Available: https://www.trimedx.com/blog/why-medical-equipment-vulnerability-remediation-is-not-one-size-fits-all-trimedx

[39] "IoMT | IoT in healthcare | PTC." Accessed: May 21, 2025. [Online]. Available: https://www.ptc.com/en/industries/medtech/medical-device-industry/iomt

[40] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions," *Sensors (Basel)*, vol. 22, no. 15, p. 5517, Aug. 2022, doi: 10.3390/S22155517.

[41] "Exposing vulnerabilities: How hackers could target your medical devices | AAMC." Accessed: May 21, 2025. [Online]. Available: https://www.aamc.org/news/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices

[42] C. Science, O. Mavropoulos, H. Mouratidis, and A. Fish, "A conceptual model to support security analysis in the internet of things," *Computer Science and Information Systems*, vol. 14(2), no. June, pp. 557–578, 2017, doi: 10.2298/CSIS160110016M.

[43] E. Gelenbe *et al.*, *Security in Computer and Information Sciences*. London: Springer, 2018. doi: 10.1007/978-3-319-95189-8.

[44] Dutta S, "Striking a balance between usability and cyber-security in IoT devices Saurabh Dutta Striking a balance between usability and cyber-security in IoT Devices," Massachusetts Institute of Technology, 2017. [Online]. Available: http://hdl.handle.net/1721.1/113508

[45] E. Leloglu, "A Review of Security Concerns in Internet of Things," *Journal of Computer and Communication*, vol. 5, no. 1, pp. 121–136, 2017, doi: 10.4236/jcc.2017.51010.

[46] T. Shuvo *et al.*, "eHealth innovations in LMICs of Africa and Asia: a literature review exploring factors affecting implementation, scale-up, and sustainability," *Innov Entrep Health*, vol. 2, p. 95, Oct. 2015, doi: 10.2147/ieh.s88809.

[47] M. N. S. Miazi, Z. Erasmus, M. A. Razzaque, M. Zennaro, and A. Bagula, "Enabling the Internet of Things in developing countries: Opportunities and challenges," in *2016 5th*

International Conference on Informatics, Electronics and Vision, ICIEV 2016, 2016, pp. 564–569. doi: 10.1109/ICIEV.2016.7760066.

[48] A. Al Isma'ili, S., Li, M., Shen, J., He, Q. & Alghazi, "African Societal Challenges Transformation through IoT," in *African Societal Challenges Transformation through IoT*, 2017, pp. 1–9.

[49] ITU, "Measuring digital development. Facts and figures 2020," *ITU Publications*, pp. 1–15, 2020, [Online]. Available: https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU Facts and Figures 2019 - Embargoed 5 November 1200 CET.pdf

[50] Vizocom, "6 IoT Applications that Improved People's Lives in Africa – A Story of 6 Countries - Vizocom - Leading IT & ELV Company in the Middle East and Africa," Vizocom. Accessed: Apr. 15, 2021. [Online]. Available: https://www.vizocom.com/ict/6-iot-applications-that-improved-peoples-lives-in-africa-a-story-of-6-countries/

[51] O. Yakubu, O. Adjei, and N. Babu, "A Review of Prospects and Challenges of Internet of Things," *Int J Comput Appl*, vol. 139, no. 10, pp. 33–39, 2016, doi: 10.5120/ijca2016909390.

[52] Fraunhofer FIT, "CONNECTING THE UNCONNECTED – TACKLING THE CHALLENGE OF COST-EFFECTIVE," 2019.

[53] IETF, "IETF | Internet of things," 2019.

[54] M. Gunturi, H. D. Kotha, and M. Srinivasa Reddy, "An overview of internet of things," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 9, pp. 659–665, 2018.

[55] Oracle, "What Is the Internet of Things? | Oracle." Accessed: May 18, 2025. [Online]. Available: https://www.oracle.com/internet-of-things/

[56] Knud Lasse Lueth, "State of IoT: 10 emerging IoT trends driving market growth." Accessed: May 18, 2025. [Online]. Available: https://iot-analytics.com/state-of-iot-10-emerging-iot-trends-driving-market-growth/

[57] F. Paul, "Gartner ' s top 10 IoT trends for 2019 and beyond Gartner shares its key trends and technologies for the Internet of Things . Social issues and user experience are the most intriguing Social issues will be pivotal in the world of IoT," Network World.

[58] B. Flaherty, "What is IoT Connectivity? | IoT Connectivity Guide | Very," The Ultimate Guide to IoT Connectivity. Accessed: May 18, 2025. [Online]. Available: https://www.verytechnology.com/whitepapers/what-is-iot-connectivity-guide

[59] Brad Griffith, "What Is IoT Integration? A Comprehensive Guide." Accessed: May 18, 2025. [Online]. Available: https://www.workato.com/the-connector/iot-integration/

[60] Arm, "What are IoT Devices – Arm®," IoT Devices. Accessed: May 18, 2025. [Online]. Available: https://www.arm.com/glossary/iot-devices

[61] Halodetect, "IoT Sensors: Everything You Need to Know," The 2025 guide to IoT sensors. Accessed: May 18, 2025. [Online]. Available: https://halodetect.com/blog/iot-sensors/

[62] UNU, "5 Benefits of Innovative IoT Irrigation in a Changing Climate | United Nations University," News. Accessed: May 18, 2025. [Online]. Available: https://unu.edu/vie/news/5-benefits-innovative-iot-irrigation-changing-climate

[63] IBM, "What is the Internet of Things (IoT)? | IBM." Accessed: May 18, 2025. [Online]. Available: https://www.ibm.com/think/topics/internet-of-things

[64] Guowei Li, "8 IoT Protocols and Standards Worth Exploring in 2024 | EMQ," 8 IoT Protocols and Standards Worth Exploring in 2024. Accessed: May 18, 2025. [Online]. Available: https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m

[65] "Characteristics of Internet of Things | GeeksforGeeks." Accessed: May 18, 2025. [Online]. Available: https://www.geeksforgeeks.org/characteristics-of-internet-of-things/
[66] L. Xing, "Internet of Things architecture," 2024, pp. 63–69. doi: 10.1016/B978-0-443-15610-6.00009-8.
[67] K. S. Satish Kumar Maurya, Om Prakash Pal, "Layered Architecture of IoT," in *Secure and Intelligent IoT-Enabled Smart Cities*, IGI Global, 2024.
[68] Md. A. Haque, D. Sonal, S. Ahmad, and K. Kumar, "Enhancing Security for Internet of Things Based System," Springer Nature, 2023, pp. 869–878. doi: 10.1007/978-981-99-3485-0_68.
[69] A. Bhardwaj, "Building a Smart Security Framework for IoT/IIoT," IGI Global, 2024, pp. 102–127. doi: 10.4018/979-8-3693-3451-5.ch005.
[70] A. Srivastava and U. R. Jain, "Securing the Future of IoT: A Comprehensive Framework for Real-Time Attack Detection and Mitigation in IoT Networks," pp. 1–6, 2023, doi: 10.1109/icccnt56998.2023.10307306.
[71] C.-K. Wu, "IoT Security Architecture," Springer Singapore, 2021, pp. 27–44. doi: 10.1007/978-981-16-1372-2_3.
[72] A. Zanella *et al.*, "Internet of Things for Smart Cities," *IEEE Internet Things J*, vol. 1, no. 1, pp. 22–32, 2014, doi: 10.1109/JIOT.2014.2306328.
[73] S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers, "A review of wearable sensors and systems with application in rehabilitation," pp. 1–17, 2012.
[74] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021, doi: 10.1109/ACCESS.2021.3073408.
[75] S. Zaidi, A. S. A. F. Alam, and Mohd. Y. Khan, "Enhancing Efficiency in Advanced Manufacturing through IoT Integration," *Engineering Headway*, 2024, doi: 10.4028/p-4hbpgf.
[76] S. Wolfert, L. Ge, C. Verdouw, and M.-J. Bogaardt, "Big Data in Smart Farming – A review," *Agric Syst*, vol. 153, pp. 69–80, 2017, doi: https://doi.org/10.1016/j.agsy.2017.01.023.
[77] V. Mekala, S. Abinaya, M. R. Abinivesh, and B. Surya, "Cargo Monitoring and Tracking Based on IoT," 2023, pp. 1–5. doi: 10.1109/ICCCNT56998.2023.10308117.
[78] A. Syaputra and T. Sutabri, "Perancangan Sistem Monitoring Barang Logistik Berbasis IoT," *Switch : Jurnal Sains dan Teknologi Informasi*, vol. 2, pp. 102–111, 2024, doi: 10.62951/switch.v2i5.288.
[79] S. Banoth, A. Agrawal, G. K. Sharma, B. Sharma, and A. Kumar, "Monitoring of Patient Health Using IoT and Machine Learning Based on Vital Signs," *Nanotechnol Percept*, pp. 3305–3312, 2024, doi: 10.62441/nano-ntp.vi.3460.
[80] A. Dubey and U. S. R, "Revolutionizing Healthcare with Intelligent Remote Health Monitoring," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 28–32, 2024, doi: 10.48175/ijarsct-22507.
[81] P. A. Lakra, "The Role of Internet of Things (IoT) in Healthcare," B P International, 2024, pp. 71–76. doi: 10.58532/v3bbio9p2ch4.
[82] David & Kyle, "The Digital Revolution comes to US Healthcare," 2015.
[83] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[84] O. Taiwo and A. E. Ezugwu, "Smart healthcare support for remote patient monitoring during covid-19 quarantine," *Inform Med Unlocked*, vol. 20, no. June, p. 100428, 2020, doi: 10.1016/j.imu.2020.100428.
[85] T. W. Bank, "The World Bank. Population Ages 65 and Above (% of Total Population)—Sub-Saharan Africa|Data. 2021." Accessed: Aug. 19, 2024. [Online]. Available: https://data.worldbank.org/indicator/SP.POP.65UP.TO?locations=ZF
[86] WHO, "Non Communicable Diseases," NCD.
[87] J. C. Rusatira *et al.*, "Enabling Access to Medical and Health Education in Rwanda Using Mobile Technology: Needs Assessment for the Development of Mobile Medical Educator Apps," *JMIR Med Educ*, vol. 2, no. 1, 2016, doi: 10.2196/MEDEDU.5336.
[88] M. Ndiaye, S. S. Oyewobi, A. M. Abu-Mahfouz, G. P. Hancke, A. M. Kurien, and K. Djouani, "IoT in the Wake of COVID-19: A Survey on Contributions, Challenges and Evolution," *IEEE Access*, vol. 8, pp. 186821–186839, 2020, doi: 10.1109/access.2020.3030090.
[89] A. Chacko and T. Hayajneh, "EAI Endorsed Transactions Security and Privacy Issues with IoT in Healthcare," *Ghent*, vol. 4, no. 14, pp. 1–7, 2018.
[90] L. Price, "Rwanda : The Digital Health Pioneer," healthcare digital.
[91] D. Al-Qurabat, A. Al-Ansi, and A. Elshiekh, "The challenges and future trends of IoT in healthcare: A review," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 5, pp. 1836–1847, 2022.
[92] R. Khan, M. A. Khan, and I. Ahmad, "Internet of Medical Things (IoMT): A survey on current trends, challenges, and future prospects," *Future Generation Computer Systems*, vol. 107, pp. 468–483, 2020.
[93] G. Rathee, M. Iqbal, and A. Singh, "IoT based smart healthcare system," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, pp. 54–62, 2020.
[94] N. M. Ghazaly and N. Jain, "IoT-Based Health Monitoring System: Design, Implementation, and Performance Evaluation," *Research Journal of Computer Systems and Engineering*, 2023, doi: 10.52710/rjcse.84.
[95] L. Dzamesi and N. Elsayed, "A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS," Jan. 2025, Accessed: May 13, 2025. [Online]. Available: https://arxiv.org/pdf/2501.07703
[96] "Authentication in the Internet of Medical Things | Encyclopedia MDPI," What is IoT? Accessed: May 13, 2025. [Online]. Available: https://encyclopedia.pub/entry/27919
[97] N. Alsaeed and F. Nadeem, "Authentication in the Internet of Medical Things: Taxonomy, Review, and Open Issues," Aug. 01, 2022, *MDPI*. doi: 10.3390/app12157487.
[98] M. S. Aslam *et al.*, "Novel model to authenticate role-based medical users for blockchain-based IoMT devices," *PLoS One*, vol. 19, no. 7, p. e0304774, Jul. 2024, doi: 10.1371/JOURNAL.PONE.0304774.
[99] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview , Emerging Technologies , and Case Studies," *IETE Technical Review*, vol. 0, no. 0, pp. 1–14, 2021, doi: 10.1080/02564602.2021.1927863.
[100] B. D. Glass, G. Jenkinson, Y. Liu, M. A. Sasse, F. Stajano, and M. Spencer, "The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions," no. July, 2017, doi: 10.14722/eurousec.2016.23007.
[101] S. M. Furnell and N. L. Clarke, "Balancing usability and security in authentication," *Comput Secur*, vol. 88, p. 101617, 2020.
[102] J. Yan, P. Yang, K. Ma, and X. Ju, "Usability of user authentication methods on mobile phones," *Int J Hum Comput Stud*, vol. 70, no. 10, pp. 809–827, 2012.

[103] S. Das, B. Wang, A. Kim, and L. Camp, "MFA is A Necessary Chore!: Exploring User Mental Models of Multi-Factor Authentication Technologies," 2020. doi: 10.24251/HICSS.2020.669.
[104] L. O. A. Wahid and A. R. Pratama, "Factors Influencing Smartphone Owners' Acceptance of Biometric Authentication Methods," *Ilkom Jurnal Ilmiah*, vol. 14, no. 2, pp. 91–98, 2022, doi: 10.33096/ilkom.v14i2.1114.91-98.
[105] V. Zimmermann, P. Gerber, and A. Stöver, "That Depends -- Assessing User Perceptions of Authentication Schemes across Contexts of Use," Sep. 2022, Accessed: May 14, 2025. [Online]. Available: https://arxiv.org/pdf/2209.13958
[106] C. S. Pilson and J. C. McElroy, "A Typology of Authentication Systems," 2015, *arXiv*.
[107] A. Oluwafemi and J. Feng, "How Users Perceive Authentication of Choice on Mobile Devices," in *Advances in Computer-Human Interaction*, ThinkMind, 2020, pp. 345–351.
[108] S. Gupta, A. Buriro, and B. Crispo, "Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access," *Mobile Information Systems*, vol. 2018, pp. 1–16, 2018, doi: 10.1155/2018/2649598.
[109] A. Sehrawat and K. Singh, *Security and Privacy in the Internet of Medical Things (IoMT)*. in Advances in Healthcare Information Systems and Administration Book Series. IGI Global, 2023. doi: 10.4018/978-1-6684-5422-0.ch001.
[110] B. Santhosh, "Internet of Medical Things in Secure Assistive Technologies," IGI Global, 2023, ch. 11, pp. 244–270. doi: 10.4018/978-1-6684-8938-3.ch011.
[111] J. L. McLaren, D. R. I. William, and J. M. Toups, "Multi-Level Authentication for Medical Data Access," 2010, *Google Patents*. [Online]. Available: https://patents.google.com/patent/US20100306858A1/en
[112] K. Kim, J. Ryu, Y. Lee, and D. Won, "An Improved Lightweight User Authentication Scheme for the Internet of Medical Things," *Sensors*, vol. 23, no. 3, p. 1122, 2023, doi: 10.3390/s23031122.
[113] CyberSec4Europe, "Usable security & privacy methods and recommendations," 2020.
[114] Thomas Onuoha Michael, O. Amunga, and L. Rajasvaran, "Usability Evaluation Criteria for Internet of Things," *International Journal of Information Technology and Computer Science*, vol. 8, no. 12, pp. 10–18, 2016, doi: 10.5815/ijitcs.2016.12.02.
[115] M. Bures and T. Cerny, "Internet of Things : Current Challenges in the Quality Assurance and Testing Methods," in *International Conference on Information Science and Applications*, 2018, pp. 625–634.
[116] P. Vijayan, R. M. L. George, M. Mathews, and S. Justine, "A Provably Secure,Privacy-Preserving Lightweight Authentication Scheme for Peer-to-Peer Communication in Healthcare Systems based on Internet of Medical Things," *Comput Commun*, vol. 212, 2023, doi: 10.1016/j.comcom.2023.07.042.
[117] M. A. Khan, I. U. Din, and A. Almogren, "Securing Access to Internet of Medical Things Using a Graphical-Password-Based User Authentication Scheme," *Sustainability*, vol. 15, no. 6, pp. 1–23, 2023, Accessed: May 13, 2025. [Online]. Available: https://ideas.repec.org/a/gam/jsusta/v15y2023i6p5207-d1098055.html
[118] K. Kim, J. Ryu, Y. Lee, and D. Won, "An Improved Lightweight User Authentication Scheme for the Internet of Medical Things," *Sensors 2023, Vol. 23, Page 1122*, vol. 23, no. 3, p. 1122, Jan. 2023, doi: 10.3390/S23031122.
[119] M. Farhan, A. Salih, and U. Butt, "Enhancing Secure Access and Authorization in Healthcare IoT through an Innovative Framework: Integrating OAuth, DIDs, and VCs," in *Proceedings of the 2023 6th International Conference on Information Science and*

Systems, in ICISS '23. New York, NY, USA: Association for Computing Machinery, 2023, pp. 254–261. doi: 10.1145/3625156.3625193.

[120] M. Bali and A. Yenkikar, "IOT-BASED SECURE WIRELESS MEDICAL SENSOR NETWORKS USING MULTIFACTOR AUTHENTICATION," 2024, pp. 146–162. doi: 10.58532/V3BIIO2CH12.

[121] T. S. Enamamu, "Intelligent Authentication Framework for Internet of Medical Things (IoMT)," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 109, pp. 97–121, 2022, doi: 10.1007/978-3-030-93453-8_5.

[122] M. Y. T. Kumar, A. Braeken, M. Liyanage, "Identity privacy preserving biometric based authentication scheme for Naked healthcare environment," in *Proceedings of the IEEE International Conference on Communications*, 2017.

[123] G. Sharma and G. Singh, "Robust User Authentication Scheme for IoT-Based Healthcare Applications," in *Recent Advancements in Smart Remote Patient Monitoring, Wearable Devices, and Diagnostics Systems*, F. Zeshan and A. Ahmad, Eds., IGI Global Scientific Publishing, 2023, pp. 170–182. doi: 10.4018/978-1-6684-6434-2.ch008.

[124] M. A. Khan, I. U. Din, T. Majali, and B.-S. Kim, "A Survey of Authentication in Internet of Things-Enabled Healthcare Systems," *Sensors*, vol. 22, no. 23, p. 9089, 2022, doi: 10.3390/s22239089.

[125] E. Hayashi, J. Hong, S. Das, S. Amini, and I. Oakley, "CASA : Context - Aware Scalable Authentication," in *Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.*, 2013, pp. 1–10.

[126] A. Forget, S. Chiasson, and R. Biddle, "Choose Your Own Authentication," in *NSPW*, 2015.

[127] A. Wójtowicz and J. Chmielewski, "Technical feasibility of context-Wójtowicz, A., & Chmielewski, J. (2017). Technical feasibility of context-aware passive payment authorization for physical points of sale. Pers Ubiquit Compu, 21, 1113–1125. https://doi.org/10.1007/s00779-017-1035-zaware p," *Pers Ubiquit Compu*, vol. 21, pp. 1113–1125, 2017, doi: 10.1007/s00779-017-1035-z.

[128] M. Hazratifard, F. Gebali, and M. Mamun, "Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial," *Sensors*, vol. 22, 7655., pp. 1–20, 2022.

[129] X. Su and Y. Xu, "Secure and Lightweight Cluster-Based User Authentication Protocol for IoMT Deployment," *Sensors (Basel)*, vol. 24, no. 22, p. 7119, Nov. 2024, doi: 10.3390/S24227119.

[130] B. Gurnani, K. Kaur, T. Sharma, and V. Sharma, "Commentary: Unfolding the role of biometric identification procedures in the current digital era," *Indian J Ophthalmol*, vol. 71, no. 1, pp. 61–62, Jan. 2023, doi: 10.4103/IJO.IJO_2239_22,.

[131] Z. Zheng, T. Pan, and Y. Song, "Research Article Development of Human Action Feature Recognition Using Sensors," *Information Technology Journal*, no. 21, pp. 8–13, 2022, doi: 10.3923/itj.2022.8.13.

[132] S. Alder, "More Than Half of All Healthcare IoT Devices Have a Known, Unpatched Critical Vulnerability." Accessed: May 21, 2025. [Online]. Available: https://www.hipaajournal.com/more-than-half-of-all-healthcare-iot-devices-have-a-known-unpatched-critical-vulnerability/

[133] "What Is a Man-in-the-Middle (MITM) Attack? | IBM." Accessed: May 21, 2025. [Online]. Available: https://www.ibm.com/think/topics/man-in-the-middle

[134] K. Kim, J. Ryu, Y. Lee, and D. Won, "An Improved Lightweight User Authentication Scheme for the Internet of Medical Things," *Sensors (Basel)*, vol. 23, no. 3, p. 1122, Feb. 2023, doi: 10.3390/S23031122.

[135] "What security threats are targeting IoMT devices (and how to prevent being hacked) | PDI Security and Network Solutions." Accessed: May 21, 2025. [Online]. Available: https://security.pditechnologies.com/blog/what-security-threats-are-targeting-iomt-devices-and-how-to-prevent-being-hacked/

[136] "Getting authentication right – considerations for medical device security | Imprivata UK." Accessed: May 21, 2025. [Online]. Available: https://www.imprivata.com/uk/node/27681

[137] "Medical Device Cybersecurity: Strategies to Minimise Risks and Enhance Safety - Device Authority." Accessed: May 21, 2025. [Online]. Available: https://deviceauthority.com/medical-device-cybersecurity-strategies-to-minimise-risks-and-enhance-safety/

[138] "A Comprehensive Guide to Healthcare Data Security | Metomic." Accessed: May 21, 2025. [Online]. Available: https://www.metomic.io/resource-centre/a-comprehensive-guide-to-healthcare-data-security

[139] "Multifactor Authentication | Cybersecurity and Infrastructure Security Agency CISA." Accessed: May 21, 2025. [Online]. Available: https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication

[140] A. Aljaedi, A. R. Alharbi, A. Aljuhni, M. K. Alghuson, S. Alassmi, and A. Shafique, "A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization," *Sci Rep*, vol. 15, no. 1, p. 14050, Dec. 2025, doi: 10.1038/S41598-025-97822-6.

[141] "The Ultimate Guide to IT, OT, IoMT and SOC Team Alignment: Best Practices." Accessed: May 21, 2025. [Online]. Available: https://www.elisity.com/blog/the-ultimate-guide-to-it-ot-iomt-and-soc-team-alignment-best-practices-for-2025

[142] K. Azmi, A. Bakar, and N. I. Daud, "Adaptive Authentication:A Case Study for Unified Authentication Platform," in *CS & IT-CSCP 2015*, 2015, pp. 61–72.

[143] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Comput Secur*, vol. 63, pp. 85–116, 2016, doi: 10.1016/j.cose.2016.09.004.

[144] A. Ometov, V. Petrov, and S. Bezzateev, "Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications," *IEEE*, no. March, 2019, doi: 10.1109/MNET.2019.1800240.

[145] L. Khajehzadeh, H. Barati, and A. Barati, "L2AI: lightweight three-factor authentication and authorization in IOMT blockchain-based environment," Jul. 2024, Accessed: May 13, 2025. [Online]. Available: https://arxiv.org/pdf/2407.12187

[146] P. Arias-cabarcos, "A Survey on Adaptive Authentication," *ACM Comput. Surv. Article 80 Article 80*, vol. 52, no. 4, 2019.

[147] P. Arias-Cabarcos and C. Krupitzer, "On the design of distributed adaptive authentication systems," *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017.

[148] F. H. Hawkins, *Human Factors in Flight*. Gower Technical Press, 1987.

[149] Hafidh Masoud, "(37) Shell Model allows you to think about all different human factors influences on your performance . | LinkedIn." Accessed: Feb. 12, 2022. [Online]. Available: https://www.linkedin.com/pulse/shell-model-helps-you-think-all-human-factors-influence-hafidh-masoud/

[150] S.A Shappel and D.A Wiegmann, "The human factors analysis and classification system," 2000.

[151] B. Craggs and A. Rashid, "Smart cyber-physical systems: beyond usable security to security ergonomics by design," in *2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, 2017, pp. 22–25.

[152] S. Al-Isma'ili, G.-Z. Lo, B. P., Thiemjarus, S., King, R., and Yang, and A. Al Isma'ili, S., Li, M., Shen, J., He, Q. & Alghazi, "African Societal Challenges Transformation through IoT," in *21st Pacific Asia Conference on Information system(PACIS 2017)*, 2017, pp. 1–9.

[153] T. Pinch, "The Social Construction of Technology(SCOT):The Old,the New and the Nonhuman," in *Material Culture and Technology in Everyday Life: Ethnographic Approaches*, 2009, ch. 3.

[154] T. Lindgren, "Using IoT to Fight Covid-19," Unissu. Accessed: Mar. 31, 2021. [Online]. Available: https://www.eetasia.com/using-iot-to-fight-covid-19-pandemic/

[155] H. Fang, A. Qi, and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," *IEEE Netw*, vol. 34, no. 3, pp. 24–29, 2020, doi: 10.1109/MNET.011.1900276.

[156] E. Hayashi, J. Hong, S. Das, S. Amini, and I. Oakley, "CASA : Context - Aware Scalable Authentication," in *Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.*, 2013, pp. 1–10.

[157] A. Steger, "What Makes IoMT Devices So Difficult to Secure Against Cyberthreats," Health Magazine. Accessed: Mar. 25, 2021. [Online]. Available: https://healthtechmagazine.net/article/2020/02/what-makes-iomt-devices-so-difficult-secure-perfcon

[158] P. C. Santana-Mancilla, L. E. Anido-Rifón, J. Contreras-Castillo, and R. Buenrostro-Mariscal, "Heuristic evaluation of an IoMT system for remote health monitoring in senior care," *Int J Environ Res Public Health*, vol. 17, no. 5, 2020, doi: 10.3390/ijerph17051586.

[159] D. Hintze, S. Scholz, E. Koch, and R. Mayrhofer, "Location-based risk assessment for mobile authentication," *UbiComp 2016 Adjunct - Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, no. September 2016, pp. 85–88, 2016, doi: 10.1145/2968219.2971448.

[160] M. T. Gebrie and H. Abie, "Risk-Based Adaptive Authentication for Internet of Things in Smart Home eHealth," in *Proceedings of ECSA'17, September 11–15, 2017, Canterbury, United Kingdom, 7 pages.*, 2017. doi: https://doi.org/10.1145/3129790.3129801.

[161] B. D. Mohammed Misbahuddin, BS Bhindumadhava, "Design of a Risk Based Authentication System using Machine Learning Techniques," *IEEE*, 2017.

[162] S. Vhaduri and C. Poellabauer, "Biometric-Based Wearable User Authentication During Sedentary and Non-sedentary Periods," *ArXiv:1811.07060v1*, pp. 1–4, 2018, [Online]. Available: http://arxiv.org/abs/1811.07060

[163] W. He *et al.*, "Rethinking access control and authentication for the Home Internet of Things (IoT)," in *Proceedings of the 27th USENIX Security Symposium*, 2018, pp. 255–272.

[164] S. Batool, N. A. Saqib, M. K. Khattack, and A. Hassan, *Identification of remote iot users using sensor data analytics*, vol. 69, no. January. Springer International Publishing, 2020. doi: 10.1007/978-3-030-12388-8_24.

[165] A. Bumiller, O. Barais, S. Challita, B. Combemale, N. Aillery, and G. Le Lan, "A Context-Driven Modelling Framework for Dynamic Authentication Decisions," in *48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, IEEE, 2022, pp. 398–405. doi: 10.1109/seaa56994.2022.00069.

[166] N. Jeyanthi, R. Thandeeswaran, and IGI Global, *Security Breaches and Threat Prevention in the Internet of Things*, vol. i, no. February. 2017. [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-2296-6

[167] O. Gordieiev, V. Kharchenko, and K. Vereshchak, "Usable Security Versus Secure Usability: an Assessment of Attributes Interaction," in *ICTERI*, 2017.

[168] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Big data privacy in the internet of things era," *IT Prof*, vol. 17, no. 3, pp. 32–39, 2015, doi: 10.1109/MITP.2015.34.

[169] I. Greenberg, "Fifth-generation cyberattacks are here. How can the IT industry adapt?," 2021. [Online]. Available: https://www.weforum.org/agenda/2021/02/fifth-generation-cyberattacks/

[170] J. Chavula, A. Phokeer, and N. Feamster, "Insight Into Africa ' s Country-level Latencies," *IEEE Africon*, pp. 938–944, 2017.

[171] E. Nizeyimana, "Design of a Decentralized and Predictive Real- Time Framework for Air Pollution Spikes Monitoring," in *IEEE6 th International Conference on Cloud Computing and big Data Analytics*, 2021, pp. 8–11.

[172] Macrotrends, "Sub-Saharan Africa Literacy Rate 1985-2021 | MacroTrends," 2021. [Online]. Available: https://www.macrotrends.net/countries/SSF/sub-saharan-africa-/literacy-rate

[173] J. Cleland-huang, M. Vierhauser, and M. Murphy, "Extending MAPE-K to support Human-Machine Teaming," in *17th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS '22), May 18â•fi23, 2022, PITTSBURGH, PA, USA*, Association for Computing Machinery, 2022. doi: 10.1145/3524844.3528054.

[174] T. Digital, "What are Smartwatch Sensors and How do they function?" Accessed: Mar. 12, 2023. [Online]. Available: https://www.taggdigital.com/blog/what-are-smartwatch-sensors-and-how-do-they-function#

[175] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, "Active user authentication for smartphones: A challenge data set and benchmark results," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, pp. 1–8, 2016, doi: 10.1109/BTAS.2016.7791155.

[176] G. Association, "State of Mobile Internet Connectivity 2018," *GSM Association*, pp. 1–64, 2018.

[177] M. Ehatisham-ul-Haq *et al.*, "Authentication of smartphone users based on activity recognition and mobile sensing," *Sensors (Switzerland)*, vol. 17, no. 9, 2017, doi: 10.3390/s17092043.

[178] K. Grindrod *et al.*, "Evaluating authentication options for mobile health applications in younger and older adults," *applications in younger and older adults. PLoS ONE 13(1): e0189048*, vol. 13, no. 1, pp. 1–16, 2018, doi: https://doi.org/10.1371/journal.pone.0189048 Editor:

[179] H. AMROUN and M. AMMI, "Who used my smart object ? a flexible approach for the recognition of users," *IEEE*, vol. 3536, no. c, pp. 1–12, 2017, doi: 10.1109/ACCESS.2017.2776098.

[180] K. Helkala and E. Snekkenes, "A Method for Ranking Authentication Products," in *Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)*, 2008, pp. 81–93.

[181] Y. M. Hausawi and W. H. Allen, "Usable-security evaluation," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and*

Lecture Notes in Bioinformatics), 2015, pp. 335–346. doi: 10.1007/978-3-319-20376-8_30.

[182] K. Chebib, "GSMA | IoT applications in the fight against COVID-19 | Mobile for Development," GSMA. Accessed: Apr. 01, 2021. [Online]. Available: https://www.gsma.com/mobilefordevelopment/blog/iot-applications-in-the-fight-against-covid-19/

[183] M. M. Kermani, R. Azarderakhsh, and M. Mirakhorli, "Multidisciplinary Approaches and Challenges in Integrating Emerging Medical Devices Security Research and Education," in *2016 ASEE Annual Conference \& Exposition*, New Orleans, Louisiana: ASEE Conferences, Jun. 2016. [Online]. Available: https://peer.asee.org/25761

[184] L. Coll and R. Simpson, "The Internet of Things and Challenges for Consumer Protection," *consumersinternational*, no. April, pp. 1–122, 2016.

[185] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): a comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, p. 383, 2017.

[186] I. Tot, K. Lalović, and M. Brzaković, "Security Mechanisms in Iot," in *The 9th International Conference on Business Information Security BISEC 2017At: Belgrade*, 2017.

[187] S. Oranski, "Why Strong Healthcare IOT Security Requires Specialized Solutions," cybermdx.

[188] M.-K. Mehran, AzarderakhshReza, R. Kui, and B. Jean-Luc, "Introduction to the special section on emerging security trends for biomedical computations, devices, and infrastructures: guest editorial," *IEEE/ACM Trans. Comput. Biol. Bioinformatics*, vol. 13, no. 3, pp. 399–400, May 2016.

[189] K. M. Mozaffari, A. Reza, and J. Xie, "Error detection reliable architectures of Camellia block cipher applicable to different variants of its substitution boxes," in *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, 2016, pp. 1–6. doi: 10.1109/AsianHOST.2016.7835560.

[190] A. Anita, M. K. Mehran, and A. Reza, "Fault Diagnosis Schemes for Low-Energy Block Cipher Midori Benchmarked on FPGA," *IEEE Trans Very Large Scale Integr VLSI Syst*, vol. 25, no. 4, pp. 1528–1536, 2017, doi: 10.1109/TVLSI.2016.2633412.

[191] United Nation, "17 goals to transform the world for persons with disabilities | United Nations Enable," un.org. [Online]. Available: https://www.un.org/development/desa/disabilities/envision2030.html

[192] J. Brownlee, *Master Machine Learning Algorithms: Discover how they work and implement them from scratch.* 2016. [Online]. Available: http://machinelearningmastery.com/a-tour-of-machine-learning-algorithms/

[193] S. Abokadr, A. Azman, H. Hamdan, and N. A. Nasharuddin, "Handling Imbalanced Data for Improved Classification Performance: Methods and Challenges," 2023, pp. 1–8. doi: 10.1109/eSmarTA59349.2023.10293442.

[194] O. Subasi, S. Ghosh, J. Manzano, B. Palmer, and A. Marquez, "Analysis and Benchmarking of feature reduction for classification under computational constraints," *Mach Learn Sci Technol*, vol. 5, no. 2, p. 20501, Apr. 2024, doi: 10.1088/2632-2153/ad3726.

[195] F. Di Nocera and G. Tempestini, "Getting Rid of the Usability/Security Trade-Off: A Behavioral Approach," *Journal of Cybersecurity and Privacy*, vol. 2, no. 2, pp. 245–256, 2022, doi: 10.3390/jcp2020013.

[196] W. Fallatah, S. Furnell, and Y. He, "Refining the Understanding of Usable Security," 2023, pp. 49–67. doi: 10.1007/978-3-031-35822-7_4.

[197] I. Karamahmutoglu and M. Gokturk, "A Systematic Approach to Measure Usability and Security Trade-off," 2024, pp. 1–4. doi: 10.1109/HORA61326.2024.10550727.

[198] Ucsc, "Choosing A Default Authentication Method," 2019. [Online]. Available: https://its.ucsc.edu/mfa/default-auth.html
[199] E. Frank, M. Hall, and B. Pfahringer, "Locally Weighted Naive Bayes."
[200] N. A. Zaidi, J. Cerquides, M. J. Carman, and G. I. Webb, "Alleviating Naive Bayes attribute independence assumption by attribute weighting," *Journal of Machine Learning Research*, vol. 14, no. Jul, pp. 1947–1988, 2013.
[201] D. Prabha, J. Aswini, B. Maheswari, R. S. Subramanian, R. Nithyanandhan, and P. Girija, "A Survey on Alleviating the Naive Bayes Conditional Independence Assumption," in *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 2022, pp. 654–657. doi: 10.1109/ICAISS55157.2022.10011103.
[202] R. S. Subramanian, P. Girija, K. Sudha, J. Aswini, S. SivaKumar, and N. V. S. Nattesan, "Alleviating the Naive Bayes Assumption using Filter Approaches," in *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2023, pp. 1430–1436. doi: 10.1109/ICSSIT55814.2023.10061030.
[203] I. Wickramasinghe and H. Kalutarage, "Naive Bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation," *Soft comput*, vol. 25, no. 3, pp. 2277–2293, 2021, doi: 10.1007/s00500-020-05297-6.
[204] S. Kharya and S. Soni, "Weighted Naive Bayes Classifier: A Predictive Model for Breast Cancer Detection," 2016. [Online]. Available: http://archive.ics.uci.edu/ml/machine-
[205] G. Kumar, A. R. Chaudhary, and K. Kumar, "Internet banking security enhancement using naïve bayes algorithm," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 79–82, 2019.
[206] A. Khusnul, H. Hidayati, and O. Nastiti, "Expert System for Stroke Classification Using Naive Bayes Classifier and Certainty Factor as Diagnosis Supporting Device," *J Phys Conf Ser*, vol. 1445, p. 12026, 2020, doi: 10.1088/1742-6596/1445/1/012026.
[207] N. Ç. B. Akkaya, "(11) (PDF) Comparison of Multi-class Classification Algorithms on Early Diagnosis of Heart Diseases," 2019. [Online]. Available: https://www.researchgate.net/publication/338950098_Comparison_of_Multi-class_Classification_Algorithms_on_Early_Diagnosis_of_Heart_Diseases
[208] G. Kumar, A. R. Chaudhary, and K. Kumar, "Internet banking security enhancement using naïve bayes algorithm," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 79–82, 2019.
[209] Pavan Vadapalli, "Naive Bayes Classifier: Pros & Cons, Applications & Types Explained," upGrad. [Online]. Available: https://www.upgrad.com/blog/naive-bayes-classifier/
[210] Sunil Ray, "Naive Bayes Classifier Explained: Applications and Practice Problems of Naive Bayes Classifier."
[211] S. Ruan, B. Chen, K. Song, and H. Li, "Weighted na\"{\i}ve Bayes text classification algorithm based on improved distance correlation coefficient," *Neural Comput. Appl.*, vol. 34, no. 4, pp. 2729–2738, Feb. 2022, doi: 10.1007/s00521-021-05989-6.
[212] Y. Wang, Y. Liu, and S. Chen, "Towards Adaptive Unknown Authentication for Universal Domain Adaptation by Classifier Paradox," 2022. [Online]. Available: https://arxiv.org/abs/2207.04494
[213] R. Zeng, L. Lin, and Y. Zhao, "A Novel Weight Adaptive Multi Factor Authorization Technology," 2023, pp. 446–457. doi: 10.1007/978-3-031-28867-8_33.
[214] Z. Wang, Q. Yan, Z. Wang, and X. Hei, "A Weighted Naive Bayes for Image Classification Based on Adaptive Genetic Algorithm," in *Advances in Natural Computation, Fuzzy*

Systems and Knowledge Discovery, N. Xiong, M. Li, K. Li, Z. Xiao, L. Liao, and L. Wang, Eds., Cham: Springer International Publishing, 2023, pp. 543–550.

[215] "US10671747B2 - Multi-user permission strategy to access sensitive information - Google Patents." Accessed: May 28, 2025. [Online]. Available: https://patents.google.com/patent/US10671747B2/en

[216] Y. Wang and H. Youn, "Feature Weighting Based on Inter-Category and Intra-Category Strength for Twitter Sentiment Analysis," *Applied Sciences 2019, Vol. 9, Page 92*, vol. 9, no. 1, p. 92, Dec. 2018, doi: 10.3390/APP9010092.

[217] "U.S. Patent for Adaptive user authentication Patent (Patent # 11,575,670 issued February 7, 2023) - Justia Patents Search." Accessed: May 28, 2025. [Online]. Available: https://patents.justia.com/patent/11575670

[218] L. Fei, B. Kang, V. Huynh, and Y. Deng, "Adaptively evidential weighted classifier combination," pp. 1–9.

[219] Z. Sari, D. R. Chandranegara, R. N. Khasanah, H. Wibowo, and W. Suharso, "Analysis of the Combination of Naïve Bayes and MHR (Mean of Horner's Rule) for Classification of Keystroke Dynamic Authentication," *Jurnal Online Informatika*, vol. 7, no. 1, p. 62, 2022, doi: 10.15575/join.v7i1.839.

[220] J. Blue, J. Condell, and T. Lunney, "It is probably me: A Bayesian approach to weighting digital identity sources," *2019 International Symposium on Networks, Computers and Communications, ISNCC 2019*, pp. 1–6, 2019, doi: 10.1109/ISNCC.2019.8909201.

[221] R. F. Rahman and Suharjito, "Crowd Face Detection with Naive Bayes in Attendance System Using Raspberry Pi," in *E3S Web of Conferences*, EDP Sciences, May 2023. doi: 10.1051/e3sconf/202338802010.

[222] H. Zhang, L. Jiang, and L. Yu, "Attribute and instance weighted naive Bayes," *Pattern Recognit*, vol. 111, Mar. 2021, doi: 10.1016/j.patcog.2020.107674.

[223] H. Zhang and L. Jiang, "Fine tuning attribute weighted naive Bayes," *Neurocomputing*, vol. 488, pp. 402–411, Jun. 2022, doi: 10.1016/j.neucom.2022.03.020.

[224] A. Jha, M. Dave, and S. Madan, "Comparison of Binary Class and Multi-Class Classifier Using Different Data Mining Classification Techniques," *SSRN Electronic Journal*, pp. 894–903, 2019, doi: 10.2139/ssrn.3464211.

[225] A. A. Salomatin, A. Y. Iskhakov, and R. V. Meshcheryakov, "Application of the User's Digital Footprint in the Adaptive Authentication Problem," *SIBCON 2021 - International Siberian Conference on Control and Communications*, May 2021, doi: 10.1109/SIBCON50419.2021.9438880.

[226] DataHub, "IPv4 geolocation," IPv4 geolocation.

[227] A. Acien, A. Morales, R. Vera-Rodriguez, and J. Fierrez, "Smartphone Sensors for Modeling Human-Computer Interaction : General Outlook and Research Datasets for User Authentication," in *IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 1273–1278. doi: 10.1109/COMPSAC48688.2020.00-81.

[228] Wolfgang, "Mobile Application User Statistics," 2018.

[229] M. B. Finan, "A Probability Course for the Actuaries," 2012.

[230] I. C. Obasi and C. Benson, "Evaluating the effectiveness of machine learning techniques in forecasting the severity of traffic accidents," *Heliyon*, vol. 9, no. 8, p. e18812, 2023, doi: 10.1016/j.heliyon.2023.e18812.

[231] Adam Hayes, "Positive Correlation: Definition, Measurement, Examples," Positive Correlation: Definition, Measurement, Examples. Accessed: May 30, 2025. [Online]. Available: https://www.investopedia.com/terms/p/positive-correlation.asp

[232] J. Muncaster and M. Turk, "Continuous Multimodal Authentication Using Dynamic Bayesian Networks," 2006.

[233] E. V. and İ. Ö. B. Merve Veziroğlu, "Performance Comparison between Naive Bayes and Machine Learning Algorithms for News Classification," in *Bayesian Inference - Recent Trends*, IntechOpen, 2024.

[234] R. Kumar, B. Goswami, S. Mhatre, and S. Agrawal, "Naive Bayes in Focus: A Thorough Examination of its Algorithmic Foundations and Use Cases," *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 2078–2081, 2024, doi: 10.38124/ijisrt/IJISRT24MAY1438.

[235] M. F. Azizah and A. T. Paramitha, "Predictive Modelling of Chronic Kidney Disease Using Gaussian Naive Bayes Algorithm," *International Journal of Artificial Intelligence in Medical Issues*, vol. 2, no. 2, pp. 125–135, 2024, doi: 10.56705/ijaimi.v2i2.160.

[236] M. Garba, M. A. Usman, and A. M. Gulumbe, "Improving Breast Cancer Detection with Naive Bayes: A Predictive Analytics Approach," pp. 185–196, 2024, doi: 10.5121/csit.2024.141116.

[237] A. Askari, A. d'Aspremont, and L. El Ghaoui, "Naive Feature Selection: A Nearly Tight Convex Relaxation for Sparse Naive Bayes," *Math. Oper. Res.*, vol. 49, no. 1, pp. 278–296, May 2023, doi: 10.1287/moor.2023.1356.

[238] H. Zhou, "Naive Bayes Classification," in *Learn Data Mining Through Excel: A Step-by-Step Approach for Understanding Machine Learning Methods*, Berkeley, CA: Apress, 2023, pp. 143–159. doi: 10.1007/978-1-4842-9771-1_9.

[239] F. Sun, W. Zang, R. Gravina, G. Fortino, and Y. Li, "Gait-based identification for elderly users in wearable healthcare systems," *Information Fusion*, vol. 53, no. June 2019, pp. 134–144, 2020, doi: 10.1016/j.inffus.2019.06.023.

[240] ncoa, "The Top 10 Most Common Chronic Conditions in Older Adults." Accessed: Feb. 08, 2024. [Online]. Available: https://www.ncoa.org/article/the-top-10-most-common-chronic-conditions-in-older-adults

[241] Statista, "Distribution of the Population of Sub-Saharan Africa from 2010 to 2022, by Age Group." Accessed: Aug. 19, 2023. [Online]. Available: https:%0A//www.statista.com/statistics/1225664/age-distribution-of-the-population-of-sub-saharan-africa/

[242] R. N. Ten Brink, R. I. Scollan, and M. A. Bedford, "Usability of Biometric Authentication Methods for Citizens with Disabilities," *9th Annual Internal Revenue Service-Tax Policy Center (IRS-TPC) Joint Research Conference on Tax Administration*, no. September, p. 40, 2019.

[243] M. Kante and P. Ndayizigamiye, "Internet of medical things, policies and geriatrics: An analysis of the national digital health strategy for South Africa 2019–2024 from the policy triangle framework perspective," *Sci Afr*, vol. 12, p. e00759, 2021, doi: 10.1016/j.sciaf.2021.e00759.

[244] K. Mtonga, S. Kumaran, C. Mikeka, and K. Jayavel, "Machine Learning-Based Patient Load Prediction and IoT Integrated Intelligent Patient Transfer Systems," *Future Internet*, vol. 11, no. 236, pp. 1–24, 2019, doi: 10.3390/fi11110236.

[245] P. Jyotheeswari and N. Jeyanthi, "An Adaptive Authentication Schemes based on the user Mobility in Medical-IoT," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. Volume-9 I, no. 2, pp. 2708–2713, 2019, doi: 10.35940/ijeat.B3051.129219.

[246] M. Al-zubaidie, Z. Zhang, and J. Zhang, "RAMHU : A New Robust Lightweight Scheme for Mutual Users Authentication in Healthcare Applications," *Security and Communication Networks*, vol. 2019, 2019, doi: https://doi.org/10.1155/2019/3263902.

[247] D. Nkomo and R. Brown, "Hybrid Cyber Security Framework for the Internet of Medical Things," in *Blockchain and Clinical Trial, Advanced Sciences and Technologies for Security Applications,* 2019, pp. 211–229.

[248] M. Zallio, J. McGrory, and D. Berry, "How to Democratize Internet of Things Devices: A Participatory Design Study to Improve Digital Literacy," *Advances in Intelligent Systems and Computing*, vol. 1202 AISC, no. Ahfe, pp. 139–150, 2020, doi: 10.1007/978-3-030-51194-4_19.

[249] J. M. Blythe and S. D. Johnson, "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," *IEEE Explore*, 2018.

[250] S. Meli, S. Nasabeh, and S. Luj, "MoSIoT : Modeling and Simulating IoT Healthcare-Monitoring Systems for People with Disabilities," *Int J Environ Res Public Health*, vol. 18, no. 2021, 2021, doi: https://doi.org/10.3390/ ijerph18126357.

[251] P. M. Mavhemwa, M. Zennaro, P. Nsengiyumva, and F. Nzanywayingoma, "User-Centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones," in *Artificial Intelligence Application in Networks and Systems*, R. Silhavy and P. Silhavy, Eds., Cham: Springer International Publishing, 2023, pp. 783–799.

[252] A. Y.- Powell, "Ensuring biometrics work for everyone - Raconteur," reconteur. Accessed: Apr. 23, 2021. [Online]. Available: https://www.raconteur.net/hr/diversity-inclusion/ensuring-biometrics-work-for-everyone/

[253] H. U. ; Khan, Y. ; Ali, F. Khan, H. Ullah Khan, Y. Ali, and F. Khan, "A Features-Based Privacy Preserving Assessment Model for Authentication of Internet of Medical Things (IoMT) Devices in Healthcare," *Mathematics 2023, Vol. 11, Page 1197*, vol. 11, no. 5, p. 1197, Feb. 2023, doi: 10.3390/MATH11051197.

[254] S. O'Dea, "• Mobile OS share in Africa 2018-2021 | Statista," Share of mobile operating systems in Africa 2018-2021, by month. Accessed: Jan. 16, 2022. [Online]. Available: https://www.statista.com/statistics/1045247/share-of-mobile-operating-systems-in-africa-by-month/

[255] H. L. S. R. P. De Silva, D. C. Wittebron, A. M. R. Lahiru, K. L. Madumadhavi, L. Rupasinghe, and K. Y. Abeywardena, "AuthDNA : An Adaptive Authentication Service for any Identity Server," in *International Conference on Advancements in Computing (ICAC) December 5-6, 2019. Malabe, Sri Lanka*, 2019.

[256] Mattias Tsegaye Gebrie, "UNIVERISITY OF POLYTECNICO DI TORINO MASTER ' S THESIS Risk based Adaptive Authentication for IoT in Smart Home eHealth Author : Mattias Tsegaye Gebrie," UNIVERISITY OF POLYTECNICO DI TORINO, 2017.

[257] N. Chakraborty, J. Li, S. Mondal, F. Chen, and Y. Pan, "On overcoming the identified limitations of a usable pin entry method," *IEEE Access*, vol. 7, pp. 124366–124378, 2019, doi: 10.1109/ACCESS.2019.2937948.

[258] H. Khan and K. Grindrod, "Evaluating Smartphone Authentication Schemes with Older Adults," in *In Proc. of SOUPS 2016*, 2016.

[259] J. Singh and Y. H. Kam, "Usable Authentication Methods for Seniors," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 3, pp. 94–100, 2019, doi: 10.35940/ijrte.C1018.1083S19.

[260] P. A. Grassi *et al.*, "Digital identity guidelines: authentication and lifecycle management," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63b.

[261] Y. Ashibani and Q. H. Mahmoud, "A User Authentication Model for IoT Networks Based on App Traffic Patterns," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, IEEE, 2018, pp. 632–638.

[262] A. Buriro, S. Gupta, A. Yautsiukhin, and B. Crispo, "Risk-Driven Behavioral Biometric-based One-Shot-cum-Continuous User Authentication Scheme," *J Signal Process Syst*, vol. 93, no. 9, pp. 989–1006, Sep. 2021, doi: 10.1007/S11265-021-01654-2;PAGE:STRING:ARTICLE/CHAPTER.

[263] D. Damopoulos and G. Kambourakis, "Hands-Free One-Time and Continuous Authentication Using Glass Wearable Devices," *Journal of Information Security and Applications*, vol. 46, pp. 138–150, Oct. 2018, doi: 10.1016/j.jisa.2019.02.002.

[264] S. Murali *et al.*, "Continuous Authentication Using Human-Induced Electric Potential," *ACM International Conference Proceeding Series*, pp. 409–423, 2023, doi: 10.1145/3627106.3627124.

[265] V. T. Hayashi and W. V. Ruggiero, "Hands-Free Authentication for Virtual Assistants with Trusted IoT Device and Machine Learning," *Sensors 2022, Vol. 22, Page 1325*, vol. 22, no. 4, p. 1325, Feb. 2022, doi: 10.3390/S22041325.

[266] D. Bhuva and S. Kumar, "A Novel Continuous Authentication Method using Biometrics for IOT Devices," *Internet of Things*, vol. 24, p. 100927, 2023, doi: 10.1016/j.iot.2023.100927.

[267] T. Zhao, Y. Wang, J. Liu, J. Cheng, Y. Chen, and J. Yu, "Robust Continuous Authentication Using Cardiac Biometrics From Wrist-Worn Wearables," *IEEE Internet Things J*, vol. 9, no. 12, pp. 9542–9556, Jun. 2022, doi: 10.1109/JIOT.2021.3128290.

[268] Z. Alattar, T. Abbes, and F. Zerai, "Privacy-preserving hands-free voice authentication leveraging edge technology," *SECURITY AND PRIVACY*, 2022, doi: 10.1002/spy2.290.

[269] Ucsc, "Choosing A Default Authentication Method," INFORMATION TECHNOLOGY SERVICES. Accessed: Jun. 03, 2021. [Online]. Available: https://its.ucsc.edu/mfa/default-auth.html

[270] C. Hew and M. Ramasamy, "Development of a IoT Based Low Cost Wearable Smart Health Monitoring System for Elderly," 2022, pp. 42–47. doi: 10.1109/ICSIMA55652.2022.9929133.

[271] A. M. Avi, Md. S. Rana, M. B. Bedar, and Md. A. Talukder, "An android application and speech recognition-based IoT-enabled deployment using NodeMCU for elderly individuals," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 5, pp. 2763–2776, 2023, doi: 10.11591/eei.v12i5.5062.

[272] E. and W. Department of Health, "The Belmont Report," THE BELMONT REPORT. Accessed: Jan. 28, 2023. [Online]. Available: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

[273] C.-K. Lo, H.-C. Chen, P.-Y. Lee, M.-C. Ku, L. Ogiela, and C.-H. Chuang, "Smart Dynamic Resource Allocation Model for Patient-Driven Mobile Medical Information System Using C4.5 Algorithm," 2019. [Online]. Available: http://www.journal.uestc.edu.cn.

[274] K. Chebib, "GSMA | IoT applications in the fight against COVID-19 | Mobile for Development," 2020. [Online]. Available:

https://www.gsma.com/mobilefordevelopment/blog/iot-applications-in-the-fight-against-covid-19/

[275] M. S. Rahman, N. C. Peeri, N. Shrestha, R. Zaki, U. Haque, and S. H. A. Hamid, "Defending against the Novel Coronavirus (COVID-19) outbreak: How can the Internet of Things (IoT)

help to save the world?," *Health Policy Technol*, vol. 9, no. 2, pp. 136–138, Jun. 2020, doi: 10.1016/j.hlpt.2020.04.005.

[276] L. Pryor, R. Dave, J. Seliya, and E. S. Boone, "Machine Learning Algorithms in User Authentication Schemes," *International Conference on Electrical, Computer, and Energy Technologies, ICECET 2021*, 2021, doi: 10.1109/ICECET52533.2021.9698440.

[277] D. Deb, A. Ross, A. K. Jain, K. Prakah-Asante, and K. V. Prasad, "Actions Speak Louder Than (Pass)words: Passive Authentication of Smartphone∗ Users via Deep Temporal Features," in *2019 International Conference on Biometrics, ICB 2019*, 2019. doi: 10.1109/ICB45273.2019.8987433.

[278] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, "Design and implementation of a contextual-based continuous authentication framework for smart homes," *Applied System Innovation*, vol. 2, no. 1, pp. 1–20, 2019, doi: 10.3390/asi2010004.

[279] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective," *IEEE Internet Things J*, vol. 7, no. 9, pp. 9128–9143, Sep. 2020, doi: 10.1109/JIOT.2020.3004077.

[280] S. Vhaduri and C. Poellabauer, "Wearable Device User Authentication Using Physiological and Behavioral Metrics," *IEEE*, pp. 1–6, 2017.

[281] S. Selvan and M. M. Singh, "Adaptive Contextual Risk-Based Model to Tackle Confidentiality-based Attacks Fog-iot Paradigm," *Computers*, vol. 11, no. 16, pp. 1–21, 2022.

[282] A. G. Martín, I. Martín de Diego, A. Fernández-Isabel, M. Beltrán, and R. R. Fernández, "Combining user behavioural information at the feature level to enhance continuous authentication systems," *Knowl Based Syst*, vol. 244, p. 108544, 2022, doi: 10.1016/j.knosys.2022.108544.

[283] J. M. J. V. M. S. S. M. S. S. H. H. M. P. M. Perez, "Machine learning as enabler of continuous and adaptive authentication in multimedia mobile devices," in *Handbook of Research on Multimedia Cyber SecurityPublisher: IGI Global*, 2020.

[284] S. Oranski, "Why Strong Healthcare IOT Security Requires Specialized Solutions," 2019.

[285] P. Musale, D. Baek, and B. J. Choi, "Lightweight Gait based Authentication Technique for IoT using Subconscious Level Activities," *IEEE*, pp. 564–567, 2018.

[286] A. Muratyan, W. Cheung, S. V. Dibbo, and S. Vhaduri, "Opportunistic Multi-Modal User Authentication for Health-Tracking IoT Wearables," *EAI/Springer Innovations in Communication and Computing*, pp. 1–18, Sep. 2021, doi: 10.1007/978-3-030-94285-4_1.

[287] Y. Cao, F. Li, Q. Zhang, S. Yang, and Y. Wang, "Towards Nonintrusive and Secure Mobile Two-Factor Authentication on Wearables," *IEEE Trans Mob Comput*, vol. 22, no. 5, pp. 3046–3061, May 2023, doi: 10.1109/TMC.2021.3133275.

[288] K. Al Ajlan, T. Alsboui, O. Alshaikh, I. Inuwa-Dute, S. Khan, and S. Parkinson, "The Emerging Challenges of Wearable Biometric Cryptosystems," *Cryptography 2024, Vol. 8, Page 27*, vol. 8, no. 3, p. 27, Jun. 2024, doi: 10.3390/CRYPTOGRAPHY8030027.

[289] A. Vassilakos and R. Martin, "Understanding the Challenge of Cybersecurity in Africa: A Holistic Analysis of Southern African Development Community (SADC) and Foundation for Future Research," *HOLISTICA – Journal of Business and Public Administration*, vol. 14, no. 1, pp. 162–172, 2023, doi: 10.2478/hjbpa-2023-0009.

[290] E. Nigussie, T. O. Olwal, A. Lemma, F. Mekuria, and B. Peterson, "IoT architecture for enhancing rural societal services in sub-Saharan Africa," *Procedia Comput Sci*, vol. 177, pp. 338–344, 2020, doi: 10.1016/j.procs.2020.10.045.

[291] A. Hassan, "Engineering Adaptive Authentication," 2021, pp. 13–18.
[292] W.-H. Lee and R. B. Lee, "Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning," Aug. 2017, [Online]. Available: http://arxiv.org/abs/1708.09754
[293] C. Smyth, G. Wang, R. Panicker, A. Nag, B. Cardiff, and D. John, "Continuous User Authentication using IoT Wearable Sensors," pp. 14–18, 2021.
[294] S. Deepthi, M. Balachandra, K. V. Prema, K. L. A. Yau, and A. K. Abhishek, "Using Behavioural Biometrics and Machine Learning in Smart Gadgets for Continuous User Authentication," *Journal of Machine and Computing*, vol. 4, no. 3, pp. 616–626, Jul. 2024, doi: 10.53759/7669/JMC202404059.
[295] W. Cheung and S. Vhaduri, "Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data," in *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 2020, pp. 587–592. doi: 10.1109/BioRob49111.2020.9224356.
[296] D. Ekiz, Y. Dardağan, and C. Ersoy, "Can A Smartband Be Used For Continuous Implicit Authentication in Real Life," *IEEE Access*, vol. PP, p. 1, 2020, doi: 10.1109/ACCESS.2020.2982852.
[297] T. S. Enamamu, N. Clarke, P. Haskell-Dowland, and F. Li, "Transparent authentication: utilising heart rate for user authentication," *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, pp. 283–289, May 2018, doi: 10.23919/ICITST.2017.8356401.
[298] M. Martinho, A. Fred, and H. Silva, "Towards Continuous User Recognition by Exploring Physiological Multimodality: An Electrocardiogram (ECG) and Blood Volume Pulse (BVP) Approach," in *2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI)*, 2018, pp. 1–6. doi: 10.1109/ISSI.2018.8538075.
[299] H. Nishat, T. S. Balaji, S. Shargunam, R. Sasikala, and K. Rani, "Development of Authentication Framework Using GAIT for IoT Communication Models," 2024, pp. 1–7. doi: 10.1109/ICOCWC60930.2024.10470660.
[300] J. Solano, L. Camacho, A. Correa, C. Deiro, J. Vargas, and M. Ochoa, "Risk-Based Static Authentication in Web Applications with Behavioral Biometrics and Session Context Analytics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11605 LNCS, pp. 3–23, 2019, doi: 10.1007/978-3-030-29729-9_1.
[301] M. T. Gebrie, "UNIVERISITY OF POLYTECNICO DI TORINO MASTER ' S THESIS Risk based Adaptive Authentication for IoT in Smart Home eHealth Author : Mattias Tsegaye Gebrie," pp. 1–77, 2017.
[302] A. Constantinides *et al.*, "Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations," *ACM Trans. Comput. Healthcare*, vol. 4, no. 1, Feb. 2023, doi: 10.1145/3564610.
[303] V. Krishnan, C. S. Sreeja, S. Binu, and M. Misbahuddin, "A JSON Web Signature Based Adaptive Authentication Modality for Healthcare Applications," in *2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)*, 2022, pp. 1–8. doi: 10.1109/PKIA56009.2022.9952258.
[304] A. Henaien and H. BelHadj, "An Ontology Based Authentication Framework for Healthcare Monitoring," in *Digital Health in Focus of Predictive, Preventive and*

Personalised Medicine, L. Chaari, Ed., Cham: Springer International Publishing, 2020, pp. 9–16. doi: 10.1007/978-3-030-49815-3_2.

[305] S. Vhaduri and C. Poellabauer, "Biometric-Based Wearable User Authentication During Sedentary and Non-sedentary Periods," *ArXiv:1811.07060v1*, pp. 1–4, 2018, [Online]. Available: http://arxiv.org/abs/1811.07060

[306] G. Deepak and H. K. N, "A Novel Approach for User Authentication for IoT Devices Using Human Pulse and IoT Cloud for OTP Generation," *Journal of Computer Science Engineering and Software Testing*, vol. 5, no. 3, pp. 15–20, 2019.

[307] T. Karanikiotis, M. D. Papamichail, K. C. Chatzidimitriou, N. C. I. Oikonomou, A. L. Symeonidis, and S. K. Saripalle, "Continuous Implicit Authentication through Touch Traces Modelling," *Proceedings - 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security, QRS 2020*, pp. 111–120, 2020, doi: 10.1109/QRS51102.2020.00026.

[308] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart User authentication through actuation of daily activities leveraging wifi-enabled IoT," *Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, vol. Part F1291, 2017, doi: 10.1145/3084041.3084061.

[309] A. Alzubaidi and J. Kalita, "Authentication of Smartphone Users Using," *JOURNAL OF IEEE COMMUNICATIONS SURVEYS AND TUTORIALS*, no. c, pp. 1–32, 2016, doi: 10.1109/COMST.2016.2537748.

[310] S. Liu, W. Shao, T. Li, W. Xu, and L. Song, "Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey," *Digital Signal Processing: A Review Journal*, vol. 125, p. 103120, 2022, doi: 10.1016/j.dsp.2021.103120.

[311] J. Maghsoudi, "A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones DPS Dissertation by Javid Maghsoudi Submitted in partial fulfillment of the requirements for the degree of Doctor of Professional Studies in Computing at School o," 2017.

[312] A. K. Das, S. Kalam, N. Sahar, and D. Sinha, "UCFL: User Categorization using Fuzzy Logic towards PUF based Two-Phase Authentication of Fog assisted IoT devices," *Comput Secur*, vol. 97, p. 101938, 2020, doi: 10.1016/j.cose.2020.101938.

[313] M. Migliardi, M. Guerar, S. Marzio, and C. Ferrari, "Continuous Authentication on a Smartwatch," in *Proceedings of the International Conference on Ubiquitous Computing {\&} Ambient Intelligence (UCAmI 2022)*, J. Bravo, S. Ochoa, and J. Favela, Eds., Cham: Springer International Publishing, 2023, pp. 1007–1018.

[314] M. Alawami, T. Abuhmed, M. AbuHamed, and H. Kim, "MotionID: Towards practical behavioral biometrics-based implicit user authentication on smartphones," *Pervasive Mob Comput*, vol. 101, p. 101922, 2024, doi: 10.1016/j.pmcj.2024.101922.

[315] Evidian, "Evaluating contextual factors to estimate and mitigate risks related to access requests," 2019.

[316] A. Arfaoui, S. Cherkaoui, A. Kribeche, and S. M. Senouci, "Context-Aware Adaptive Remote Access for IoT Applications," *IEEE Internet Things J*, vol. 7, no. 1, pp. 786–799, 2020, doi: 10.1109/JIOT.2019.2953144.

[317] K. Habib and L. Wolfgang, "Context-Aware Authentication for the Internet of Things Context-Aware Authentication for the Internet of Things," in *The Eleventh International Conference on Autonomic and Autonomous Systems*, 2015.

[318] M. Thomas, "Adaptive Authentication: How to Improve Security Without Annoying Users," 2023. [Online]. Available: https://www.openidentityplatform.org/blog/adaptive-authentication

[319] K. Phan, "Implementing Resiliency of Adaptive Multi-Factor Authentication Systems," St Claude State University, 2018. [Online]. Available:

https://repository.stcloudstate.edu/msia_etdshttps://repository.stcloudstate.edu/msia_etds/65
[320] M. Thomas, "How to Implement Adaptive Authentication Using Machine Learning." Accessed: Feb. 16, 2024. [Online]. Available: https://maxim-thomas.medium.com/how-to-implement-adaptive-authentication-using-machine-learning-52045219abf8
[321] J. M. Jorquera Valero *et al.*, "Improving the Security and QoE in Mobile Devices through an Intelligent and Adaptive Continuous Authentication System," *Sensors (Basel)*, vol. 18, no. 11, pp. 1–29, 2018, doi: 10.3390/s18113769.
[322] IBM, "Risk score calculation - IBM Documentation," Risk score calculation. Accessed: Jul. 25, 2022. [Online]. Available: https://www.ibm.com/docs/en/sva/10.0.1?topic=overview-risk-score-calculation
[323] P. M. Mavhemwa, M. Zennaro, P. Nsengiyumva, and F. Nzanywayingoma, "An Android-Based Internet of Medical Things Adaptive User Authentication and Authorization Model for the Elderly," *Journal of Cybersecurity and Privacy 2024, Vol. 4, Pages 993-1017*, vol. 4, no. 4, pp. 993–1017, Dec. 2024, doi: 10.3390/JCP4040046.
[324] K. Li, C. Cardoso, A. Moctezuma-Ramirez, A. Elgalad, and E. Perin, "Heart Rate Variability Measurement through a Smart Wearable Device: Another Breakthrough for Personal Health Monitoring?," *Int J Environ Res Public Health*, vol. 20, no. 24, 2023, doi: 10.3390/ijerph20247146.
[325] R. Ryu, S. Yeom, S. H. Kim, and D. Herbert, "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review," *IEEE Access*, vol. PP, p. 1, 2021, doi: 10.1109/ACCESS.2021.3061589.
[326] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY: Springer, 2006.
[327] E. Kamar and E. Horvitz, "Adaptive Access Control," in *AAAI Workshop on Artificial Intelligence and Security (AISec)*, 2014.
[328] S. Kim, J. Park, and J. Lee, "A comparative study of machine learning algorithms for on-device IoT applications," *IEEE Internet Things J*, vol. 6, no. 5, pp. 8436–8446, 2019.
[329] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, 2nd ed. New York, NY: Springer, 2009.
[330] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," *Nat Mach Intell*, vol. 1, no. 5, pp. 206–215, 2019.
[331] A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, 2nd ed. Sebastopol, CA: O'Reilly Media, 2019.