





Article

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

Prudence M. Mavhemwa <sup>1,\*</sup> , Marco Zennaro <sup>2</sup> , Philibert Nsengiyumva <sup>3</sup>  and Frederic Nzanywayingoma <sup>4</sup> 

<sup>1</sup> African Centre of Excellence in Internet of Things, University of Rwanda, Kigali P.O. Box 3900, Rwanda

<sup>2</sup> Science, Technology, and Innovation Unit, Abdus Salam International Centre for Theoretical Physics, 34151 Trieste, Italy; mzennaro@ictp.it

<sup>3</sup> Department of Electrical and Electronic Engineering, University of Rwanda, Kigali P.O. Box 3900, Rwanda; p.nsengiyumva@ur.ac.rw

<sup>4</sup> Department of Information Systems, University of Rwanda, Kigali P.O. Box 3900, Rwanda; f.nzanywayingoma@ur.ac.rw

\* Correspondence: pmavhemwa@gmail.com; Tel.: +263-773845525

**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<sub>HMT</sub> 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 generalizing 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.

**Keywords:** elderly patients; SSA; chronic ailments; risk calculation; adaptive authentication; smartphone; usable security



**Citation:** Mavhemwa, P.M.; Zennaro, M.; Nsengiyumva, P.; Nzanywayingoma, F. An Android-Based Internet of Medical Things Adaptive User Authentication and Authorization Model for the Elderly. *J. Cybersecur. Priv.* **2024**, *4*, 993–1017. <https://doi.org/10.3390/jcp4040046>

Academic Editor: Georgios Kambourakis

Received: 19 August 2024

Revised: 31 October 2024

Accepted: 1 November 2024

Published: 2 December 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Around 77% of the global elderly population, aged 65 and above, suffer from chronic diseases like stroke, hypertension, asthma, diabetes, and cognitive impairment [1]. In the United States, 95% of individuals over 60 years old suffer from at least one chronic illness, while 80% grapple with multiple conditions [2]. Even the elderly population in Sub-Saharan Africa (SSA), comprising 3.06% of the overall population [3,4], 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 [5,6], and inadequately staffed healthcare facilities pose challenges in accommodating all patients [7].

The recent COVID-19 pandemic has accelerated the adoption of home-based care [8,9], prompting the integration of the Internet of Medical Things (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 [10] 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 [9,11,12]. Generally, Internet of Things (IoT) systems cater to both technical and non-technical users [13], but most end users, including elderly individuals, lack technological proficiency and are unlikely to implement security measures, making them susceptible to potential attacks [14]. At the same time, the development of security protocols often fails to account for the health issues prevalent in older populations [15,16], but when it comes to authentication, elderly users have their authenticator preferences [17].

Although smartphones are commonly utilized for authentication purposes, there is little empirical support regarding their effectiveness across various age demographics, including the elderly [5]. Despite ongoing research on suitable authentication techniques [1], there is a lack of extensive research on the practicality of authentication technologies for senior citizens and individuals with disabilities [18]. Most previous research has either focused on device authentication [19], security without usability and vice versa [20–22], physiological authentication [23], 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% [24]. 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 [25–31], they come with additional hardware and require more movements among the elderly, thereby increasing cost and inconvenience.

The rest of the paper is organized as follows: Section 2 analyzes the various authenticators available and their strengths and weaknesses. Related work is discussed in Section 3. The details of our proposed framework are discussed in Section 4. The results and findings are presented in Section 5. A discussion of results is presented in Section 6. Finally, Section 7 concludes and provides future work.

## 2. 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 [32]. Elderly individuals with chronic conditions

like arthritis, Parkinson's, and osteoporosis face challenges in utilizing some authentication systems [32], making them more susceptible to security breaches [33]. Authentication is a critical component in maintaining network security [34], 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 [35]. Figure 1 shows examples of factors used in MFA.

What you know?	What you have?	What you are?	The context you are in
password  lock pattern 	smart phone  smart card 	user biometrics  device unique ID 	location  activity 

**Figure 1.** Examples of factors used in MFA. Reproduced with permission from Hazratifard et al. [9].

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

## 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 [36]. It is liked by the elderly [17], 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 [37]. However, elderly individuals often struggle with password input due to arthritis, early-stage dementia [5], deteriorating vision [38], frustration [36], and lack of prior technology exposure [39].

### 2.1.3. Graphical Password

Images, instead of alphanumeric characters, are utilized for memory stimulation and are easier to remember than text [36], 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 [36] 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 [39], but may not be suitable for elderly individuals with typing difficulties.

## 2.2. Biometric Authenticators

Biometrics identify living individuals by utilizing physiological attributes as well as behavioral traits for accurate individual authentication [40]. Biometric traits are widely used as authenticators in mobile devices combining the “what you have” and “what you are” dimensions [9]. Of late, most IoT devices are improving their sensorial abilities, enabling user data collection for authentication [9], with success significantly influenced by user experience [41].

### 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 [42].

#### Fingerprint/Palm

Although older users prefer fingerprint authentication [32], they are less likely to successfully authenticate using it. Off-the-shelf smart devices now offer scanner capture technology [43], but factors like aging, moisture, gender, medical, and occupation can hinder its effectiveness [41].

#### 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 [43], age, and environmental light intensity [41].

#### 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 [43], 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 [32]. Factors like glasses, facial expressions, age, poses, and lighting influence results [41].

### 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 [43] 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 [44], but older adults face more challenges due to walking challenges [1].

#### Heart Rate Biometric Identification

Heart rate signals are unique and consistent over time [45], 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 [46], 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 [34] reducing the monotonous selection of the same authentication factors and identifying risks more effectively than the one-size-fits-all approach [47].

### 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 [48]. There has been a lot of research on adaptive authentication, but not much of it has produced real-world, workable solutions [49].

## 2.5. Authentication and Authorization Attacks in the IoMT

Because health data are sensitive and IoT device environments are resource-constrained, authentication and authorization attacks in the Internet of Medical Things (IoMT) present serious security risks, particularly in smart-home applications [50–52]. 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 jeopardize patient data and device functionality [53]. Physically Unclonable Functions (PUFs) are one type of authentication mechanism that can be cloned by ML-based modeling attacks, granting unauthorized access [54], but by incorporating ML techniques into authentication and authorization procedures, the unique challenges presented by IoMT networks can be addressed and attack resistance can be increased [55]. Biometric Authenticated Key Exchange (BAKE), one of the lightweight cryptographic protocols, improves security by offering mutual authentication and protecting against phishing attacks [56]. 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 centralized 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) [57]. Research is still ongoing to improve these standards, which are incorporated at the hardware level in our proposed work.

## 3. Related Work

### 3.1. IoMT Authentication

The authors of [19] 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 [58]. 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 [21] 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 [22], which used decentralized identifiers (DIDs) and verifiable credentials (VCs) together with OAuth-based authorization 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. A study [59] 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 [23]. 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 looks 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.

Authors [20] 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 [60]. The scheme could resist various well-known attacks showing that biometric keys were crucial for identification and authentication, but the work generalized 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 [61]. 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 [62]. 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 1.** Our proposed work against previous work.

Item	Previous Work	Our Proposed Work
Usable security	Previous works focused on security without usability and vice versa [20–22]	Our proposed Android app aims to balance usability and security.
Device authentication	Most previous research focused on device authentication [19,21].	Our work aims to authenticate both the user and device on medical platforms for security and usability.



Table 1. Cont.

Item	Previous Work	Our Proposed Work
Continuous authentication	A model based on app traffic patterns continuously authenticates users by analyzing network traffic, achieving an impressive average F-measure of 95.5% was developed [25], one that utilized touch-timing differences and hand-movement gestures [26], hands-free one-time and continuous authentication using glass wearable devices [27], 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 [27], continuous authentication scheme using human-induced electric potential measured by wearables [28], combining trusted IoT devices and continuous authentication based on smart-home behavior [63], hands-free continuous authentication using ECG and EMG biometrics that required no human interaction [29], continuous authentication (CA) using cardiac biometrics from wrist-worn wearables [30], a single-factor authentication scheme that required only two short voice inputs [31].	Previous techniques either required additional hardware or movement of the elderly people thereby inconveniencing them. We aim to use static authentication for improved usability amongst elderly users.
Adaptive authentication	Current authentication techniques impose what users must use [64].	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 [65,66].	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 [67–69].	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 [70], 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. The authors of [71] 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 [72] 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 [73].

## 4. Research Method

The proposed adaptive authentication model analyzes 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 [74–77]. 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 categorized 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<sub>HMT</sub> 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:

$$P(Y | X) = \frac{P(X | Y) \cdot P(Y)}{P(X)}, \quad (1)$$

where  $X = (x_1, x_2, \dots, x_n)$  represent the user's context. Expanding using the chain rule gives

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

which simplifies to

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

Let  $P(y | x_1, \dots, x_n)$  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 categorization decision rule:

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

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

$$P(III | MobChnge, \dots, TimeChnge) = \frac{P(MobChnge | III) \cdot P(GPSChnge | III) \dots P(TimeChnge | III)}{P(MobChnge)P(GPSChnge) \dots P(TimeChnge)}, \quad (5)$$

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

##### 4.1.1. Proposed System Overview

We utilized 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 authorization.

---

**Algorithm1.** Adaptive authentication and authorization for elderly users

---

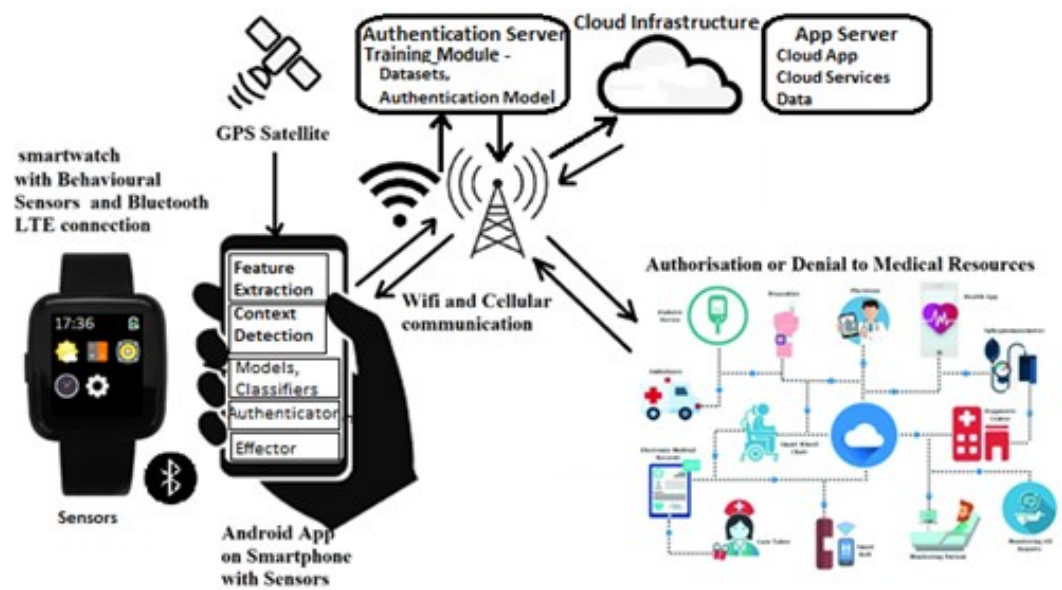
- Input:** *Mobile\_Browser, Mobile\_OS, IPAddress, Network\_Type, GPS\_Coordinates, Access\_Time, Knowledge\_based data, Biometric\_data, Age.*
- Output:** *Risk score, trust score, and authentication result.*
- Assumption:** The usability of authenticators is significantly influenced by age and medical 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
    - 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. *Authorize:*
    - Grant access to requested resources.
- 

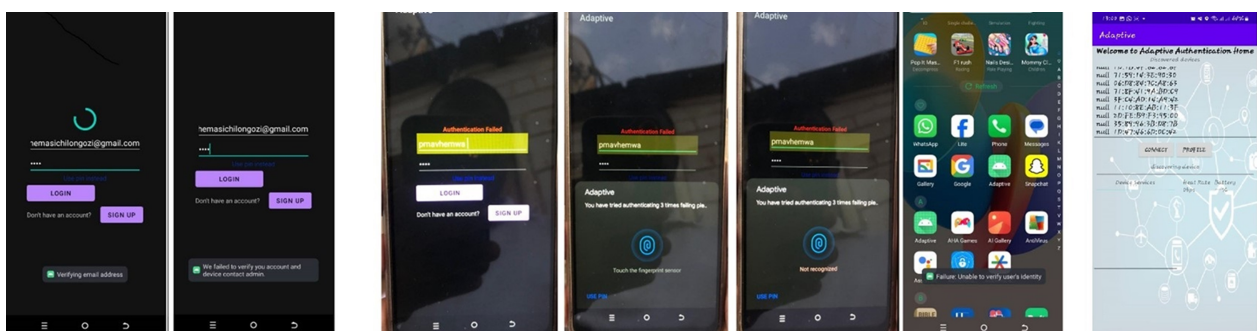
The following is a summary of the algorithm: With the help of enumerators, users downloaded, installed, and registered on the adaptive app on their smartphones. Through the use of device sensors, the application gathered information in the background about the user, the device, the network, the location, the access time, and other details required

to create a preliminary user profile. To ascertain the risk involved with that login attempt, the application then computed the risk score. One could log in with the same or different contextual data on the same or different days. Depending on how the user deviated from the known profile, the users went through a series of phases of authentication at varying degrees until they received an acceptable trust score, at which point they would be authorized. 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.

To connect with the server for risk assessment, authenticator selection, and ultimately authorization, 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 for our work, we used Figure 3c's panel to represent the authorization stage. It offered the option to search for Bluetooth devices for behavioral authentication following initial authorization. Figure 4 shows the signup and login screens.



a) Unregistered user trying to login

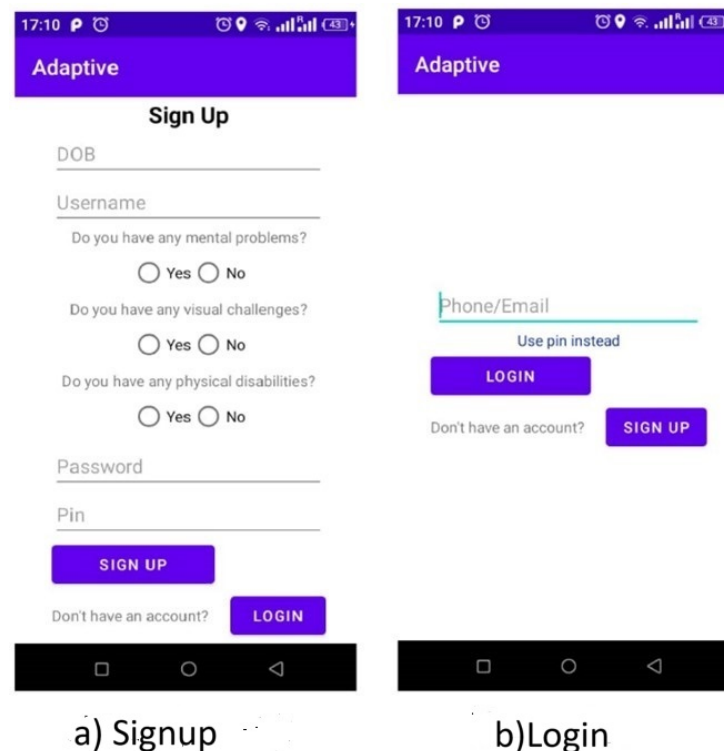
b) Authentication stepped up on registered user

c) Authenticated

**Figure 3.** Login process until authorization.

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.** Signup and login screens.

#### Pre-Study Survey

To help with prototype development, a previous study [17] 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. 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 utilized 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 [78]. 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. 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 analyze 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 Authorization

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

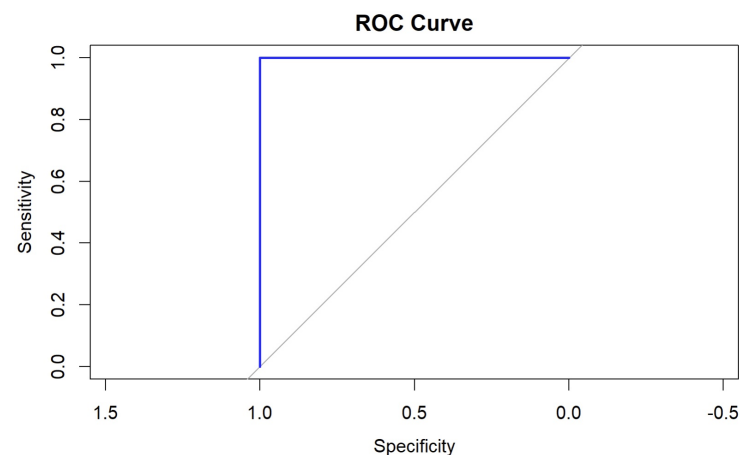
As can be seen, the model accurately classified every instance in the dataset, with a 95% confidence interval indicating a 100% accuracy. The model's low  $p$ -value suggested superior performance compared to the baseline, with a true accuracy of at least 98.44%. The No Information Rate indicated that 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 generalizes well and does not overfit the training set.

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

**Figure 5.** Overall confusion matrix and statistics.

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 authorization with the Area Under the Curve (AUC) of one with control = 0 and cases = 1.



**Figure 6.** ROC curve for authentication and authorization.

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

**Table 2.** Combination of AUC with other performance metrics.

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 recognized 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. Normalization 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 3.** Combination of AUC with other performance metrics.

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.

a)	b)	c)
94 21 26 94	Accuracy: 0.8 95% CI: (0.7431, 0.8492) No Information Rate: 0.5106 P-Value [Acc > NIR]: <2e-16  Kappa: 0.6002	McNemar's Test P-Value: 0.5596  Sensitivity: 0.7833 Specificity: 0.8174 Pos Pred Value: 0.8174 Neg Pred Value: 0.7833 Prevalence: 0.5106 Detection Rate: 0.4000 Detection Prevalence: 0.4894 Balanced Accuracy: 0.8004  'Positive' class: 0

**Figure 7.** Confusion matrix and statistics for health impact on authentication.

A 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, utilizing 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 normalization where (a) is the confusion matrix, (b) is the Kappa test, and (c) is McNemar’s test.

a)	b)	c)
28 0	Accuracy: 1	McNemar’s Test P-Value: NA
0 43	95% CI: (0.9494, 1)	Sensitivity: 1.0000
	No Information Rate: 0.6056	Specificity: 1.0000
	P-Value [Acc > NIR]: 3.443e-16	Pos Pred Value: 1.0000
	Kappa: 1	Neg Pred Value: 1.0000
		Prevalence: 0.3944
		Detection Rate: 0.3944
		Detection Prevalence: 0.3944
		Balanced Accuracy: 1.0000
		‘Positive’ Class: 0
a) General Confusion Matrix and Statistics		
27 0	Accuracy: 0.9859	McNemar’s Test P-Value: 1
1 43	95% CI: (0.924, 0.9996)	Sensitivity: 0.9643
	No Information Rate: 0.6056	Specificity: 1.0000
	P-Value [Acc > NIR]: 1.626e-14	Pos Pred Value: 1.0000
	Kappa: 0.9703	Neg Pred Value: 0.9773
		Prevalence: 0.3944
		Detection Rate: 0.3803
		Detection Prevalence: 0.3803
		Balanced Accuracy: 0.9821
		‘Positive’ Class: 0
b) L1/L2 and Elastic Net Confusion Matrix and Statistics		

**Figure 8.** Confusion matrix and statistics for the train–test split and L1, L2 normalization.

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 generalized 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 normalization. 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 utilized 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 generalizability, 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 generalization 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      0.00000000      0.0000000
3        265      1.0000000      1.0000000      0.00000000      0.0000000

Access confusion matrix and other metrics
      120  0      Accuracy: 1      McNemar's Test P-Value: NA
      0 115      95% CI: (0.9844, 1)
      P-value [Acc > NIR]: <      Sensitivity: 1.0000
      2.2e-16      No Information Rate:      Specificity: 1.0000
      Kappa: 1      Pos Pred Value: 1.0000
      Detection Rate: 0.5106      Neg Pred Value: 1.0000
      Detection Prevalence: 0.5106      Prevalence: 0.5106
      Balanced Accuracy: 1.0000
      'Positive' Class: 0

```

**Figure 9.** Confusion matrix and statistics for the cross-validation option.

### 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 traveled 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

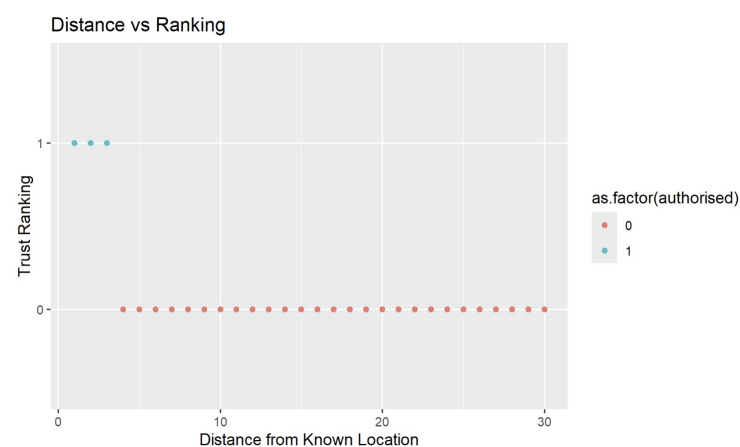
Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)    0.912344   0.028185   32.37  <2e-16 ***
dist_from_epicenter -0.044475   0.002147  -20.71  <2e-16 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

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

The linear regression analysis revealed a significant negative correlation between *Dist from epicenter* and *authorized*. The likelihood of obtaining authorization decreased as the distance from the epicenter increased. The relationship was statistically significant due to the significant variability in the authorized 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.

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.

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 analyzed 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 4.** Overall success and completion ratios.

Metric	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 utilized.

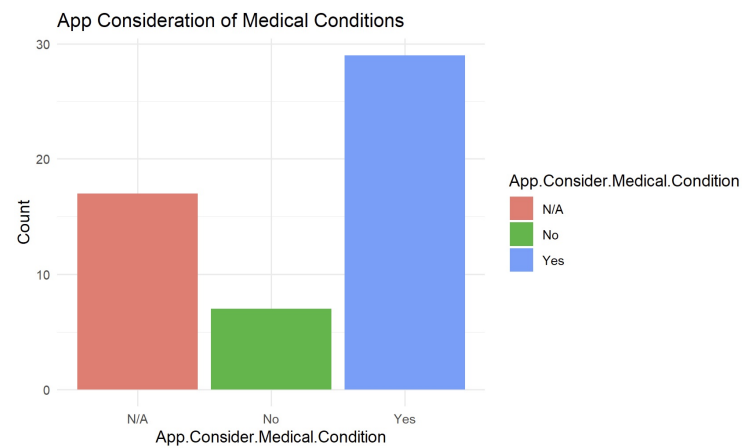
## 5.7. Usability Considerations

We used 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.

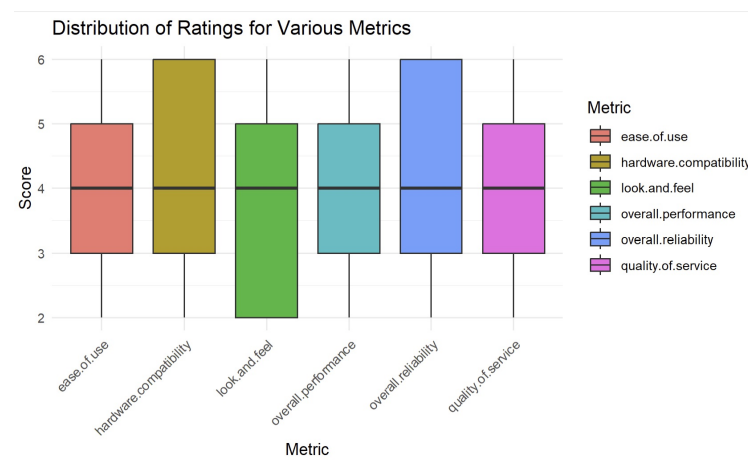
Most respondents concurred that the app took into account their medical issues. Regarding further usability measures, the responses were compiled as depicted in Figure 14.

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 below.

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



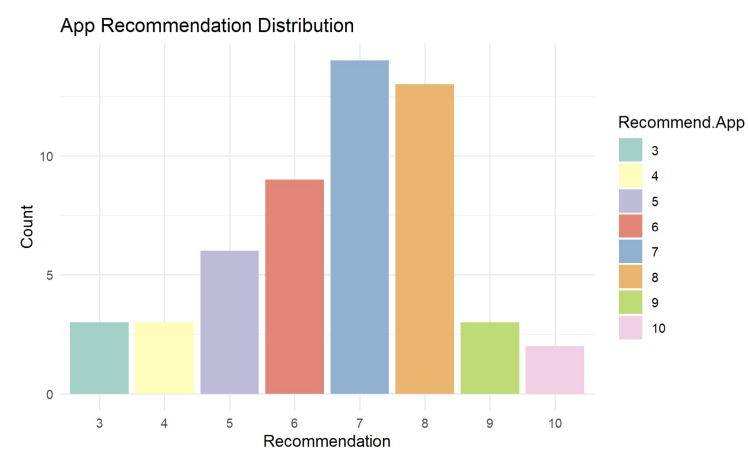
**Figure 13.** App consideration of user medical conditions.



**Figure 14.** Usability metrics.

**Table 5.** Frequency of errors.

Issue Occurrence	Number of Users
Never	14
Rarely	21
Sometimes	14
Often	4



**Figure 15.** App recommendation to others.

## 6. 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 utilizing 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 authorized and unauthorized 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 recognized 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 normalization 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 generalizability.

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.

A 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 generalization 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 a greater distance diminishes confidence, authorization 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 a 100% accuracy in training; nevertheless, the final authorization 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 [32], 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. Conclusions and Future Work

The model exhibited exceptional performance in calculating risk, trust, and authorization 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 generalizability 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 analyzed over time. Contextual elements such as ambient light and the context of device usage could also be utilized to assess the risk of a login attempt. 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 normalization 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 Sub-Saharan Africa (SSA), whose socioeconomic circumstances may differ from those of other continents, some degree of geographic and demographic generalization 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 other authors have noted [74,75], 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.

**Author Contributions:** Conceptualization, P.M.M.; methodology, P.M.M. and M.Z.; software, P.M.M.; validation, P.M.M. and P.N.; formal analysis, F.N.; investigation, resources, data curation, P.M.M.; writing—original draft preparation, P.M.M.; writing—review and editing, M.Z.; visualization, P.M.M.; supervision, M.Z., P.N. and F.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** The APC was funded by PASET-RSIF.

**Institutional Review Board Statement:** The study was conducted following the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of the University of Rwanda's College of Medicine and Health Sciences' Institutional Review Board (IRB) Reference Number 102/CMHS IRB/2023/ of 31 January 2023.

**Informed Consent Statement:** Informed consent was obtained from all subjects involved in the study. The data collected did not directly identify participants, so obtaining written consent was not necessary.

**Data Availability Statement:** The data presented in this study are available on request from the corresponding author due to ethical reasons.

**Acknowledgments:** This work was jointly supported by the African Centre of Excellence in Internet of Things (ACEIoT) from the College of Science and Technology, University of Rwanda, and the Regional Innovation Scholarship Fund (RSIF).

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

SSA	Sub-Saharan Africa
IoMT	Internet of Medical Things
IoHT	Internet of Health Things
IoT	Internet of Things
MFA	Multi-factor authentication
LAS	Lightweight Authentication Scheme
PSSUQ	Post-Study System Usability Questionnaire
DID	Decentralized identifier
VC	Verifiable credentials
CASA	Context-Aware Scalable Authentication
CYOA	Choose Your Own Authenticator
AUC	Area Under the Curve
PPv	Positive predictive value
NPV	Negative predictive value
FPR	False Positive Rat

FNR	False Negative Rate
FRR	False Rejection Rate
FAR	False Acceptance Rate

## References

1. Sun, F.; Zang, W.; Gravina, R.; Fortino, G.; Li, Y. Gait-based identification for elderly users in wearable healthcare systems. *Inf. Fusion* **2020**, *53*, 134–144. [\[CrossRef\]](#)
2. The National Council on Aging (NCOA). The Top 10 Most Common Chronic Conditions in Older Adults. 2023. Available online: <https://www.ncoa.org/article/the-top-10-most-common-chronic-conditions-in-older-adults/> (accessed on 8 January 2024).
3. Statista. Distribution of the Population of Sub-Saharan Africa from 2010 to 2022, by Age Group. Available online: <https://www.statista.com/statistics/1225664/age-distribution-of-the-population-of-sub-saharan-africa/> (accessed on 11 October 2024).
4. The World Bank. Population Ages 65 and Above (% of Total Population)—Sub-Saharan Africa | Data. 2021. Available online: <https://data.worldbank.org/indicator/SP.POP.65UP.TO?locations=ZF> (accessed on 22 December 2021).
5. Ten Brink, R.N.; Scollan, R.I.; Bedford, M.A. *Usability of Biometric Authentication Methods for Citizens with Disabilities*; IRS-TPC; The MITRE Corporation: Bedford, MA, USA, 2019; 40p.
6. Kante, M.; Ndayizigamiye, P. 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.* **2021**, *12*, e00759. [\[CrossRef\]](#)
7. Mtonga, K.; Kumaran, S.; Mikeka, C.; Jayavel, K. Machine Learning-Based Patient Load Prediction and IoT Integrated Intelligent Patient Transfer Systems. *Future Internet* **2019**, *11*, 236. [\[CrossRef\]](#)
8. Jyotheeswari, P.; Jeyanthi, N. An Adaptive Authentication Scheme based on the User Mobility in Medical-IoT. *Int. J. Eng. Adv. Technol.* **2019**, *91*, 2708–2713. [\[CrossRef\]](#)
9. Hazratifard, M.; Gebali, F.; Mamun, M. Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial. *Sensors* **2022**, *22*, 7655. [\[CrossRef\]](#) [\[PubMed\]](#)
10. Santana-Mancilla, P.C.; Anido-Rifon, L.E.; Contreras-Castillo, J.; Buenrostro-Mariscal, R. Heuristic evaluation of an IoMT system for remote health monitoring in senior care. *Int. J. Environ. Res. Public Health* **2020**, *17*, 1586. [\[CrossRef\]](#)
11. Al-zubaidie, M.; Zhang, Z.; Zhang, J. RAMHU: A New Robust Lightweight Scheme for Mutual Users Authentication in Healthcare Applications. *Secur. Commun. Netw.* **2019**, *2019*, 3263902. [\[CrossRef\]](#)
12. Nkomo, D.; Brown, R. Hybrid Cyber Security Framework for the Internet of Medical Things. In *Blockchain and Clinical Trial, Advanced Sciences and Technologies for Security Applications*; IEEE: Piscataway, NJ, USA, 2019; pp. 211–229.
13. Zallio, M.; McGrory, J.; Berry, D. How to Democratize Internet of Things Devices: A Participatory Design Study to Improve Digital Literacy. In *Advances in Industrial Design*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 139–150. [\[CrossRef\]](#)
14. Blythe, J.M.; Johnson, S.D. 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. In *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018*, London, UK, 28–29 March 2018; IEEE: Piscataway, NJ, USA, 2018.
15. Das, S.; Kim, A.; Jelen, B.; Huber, L.L.; Camp, L.J. Non-Inclusive Online Security: Older Adults’ Experience with Two-Factor Authentication. In *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS 2021)*, Kauai, HI, USA, 5–8 January 2021.
16. Meli, S.; Nasabeh, S.; Luj, S. MoSIoT: Modeling and Simulating IoT Healthcare-Monitoring Systems for People with Disabilities. *Int. J. Environ. Res. Public Health* **2021**, *18*, 6357. [\[CrossRef\]](#)
17. Mavhemwa, P.M.; Zennaro, M.; Nsengiyumva, P.; Nzanywayingoma, F. User-Centred Design of Machine Learning Based Internet of Medical Things (IoMT) Adaptive User Authentication Using Wearables and Smartphones. In *Proceedings of the Artificial Intelligence Application in Networks and Systems*; Silhavy, R., Silhavy, P., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 783–799.
18. Powell, A.Y. Ensuring Biometrics Work for Everyone—Raconteur. 2021. Available online: <https://www.raconteur.net/hr/diversity-inclusion/ensuring-biometrics-work-for-everyone/> (accessed on 23 April 2021).
19. Panchami, V.; Lincy G., R.M.; Mathews, M.M.; Justine, S. A Provably Secure, Privacy-Preserving Lightweight Authentication Scheme for Peer-to-Peer Communication in Healthcare Systems based on Internet of Medical Things. *Comput. Commun.* **2023**, *212*, 284–297. [\[CrossRef\]](#)
20. Khan, H.; Ali, Y.; Khan, F. A Features-Based Privacy Preserving Assessment Model for Authentication of Internet of Medical Things (IoMT) Devices in Healthcare. *Mathematics* **2023**, *11*, 1197. [\[CrossRef\]](#)
21. Kim, K.; Ryu, J.; Lee, Y.; Won, D. An Improved Lightweight User Authentication Scheme for the Internet of Medical Things. *Sensors* **2023**, *23*, 1122. [\[CrossRef\]](#) [\[PubMed\]](#)
22. Farhan, M.; Salih, A.; Butt, U. 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*, Edinburgh, UK, 11–13 August 2023; Association for Computing Machinery: New York, NY, USA, 2023; ICISS ’23, pp. 254–261. [\[CrossRef\]](#)
23. Enamamu, T.S., Intelligent Authentication Framework for Internet of Medical Things (IoMT). In *Illumination of Artificial Intelligence in Cybersecurity and Forensics*; Springer International Publishing: Cham, Switzerland, 2022; pp. 97–121. [\[CrossRef\]](#)

24. O'Dea, S. Mobile OS Share in Africa 2018–2021 | Statista. 2021. Available online: <https://www.statista.com/statistics/1045247/share-of-mobile-operating-systems-in-africa-by-month/> (accessed on 16 January 2022).
25. Ashibani, Y.; Mahmoud, Q.H. A User Authentication Model for IoT Networks Based on App Traffic Patterns. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 632–638. [\[CrossRef\]](#)
26. Buriro, A.; Gupta, S.; Yautsiukhin, A.; Crispo, B. Risk-Driven Behavioral Biometric-based One-Shot-cum-Continuous User Authentication Scheme. *J. Signal Process. Syst.* **2021**, *93*, 989–1006. [\[CrossRef\]](#)
27. Damopoulos, D.; Portokalidis, G. Hands-Free One-Time and Continuous Authentication Using Glass Wearable Devices. *arXiv* **2018**, arXiv:1810.02496. [\[CrossRef\]](#)
28. Murali, S.; Jin, W.; Sivaraman, V.; Zhu, H.; Ji, T.; Li, P.; Li, M. Continuous Authentication Using Human-Induced Electric Potential. In Proceedings of the 39th Annual Computer Security Applications Conference, Austin, TX, USA, 4–8 December 2023; Association for Computing Machinery: New York, NY, USA, 2023; ACSAC '23; pp. 409–423. [\[CrossRef\]](#)
29. Bhuvu, D.R.; Kumar, S. A Novel Continuous Authentication Method using Biometrics for IOT Devices. *Internet Things* **2023**, *24*, 100927. [\[CrossRef\]](#)
30. Zhao, T.; Wang, Y.; Liu, J.; Cheng, J.; Chen, Y.; Yu, J. Robust Continuous Authentication Using Cardiac Biometrics From wrist-Worn Wearables. *IEEE Internet Things J.* **2022**, *9*, 9542–9556. [\[CrossRef\]](#)
31. Alattar, Z.S.; Abbes, T.; Zerai, F. Privacy-preserving hands-free voice authentication leveraging edge technology. *Secur. Priv.* **2022**, *6*, e290. [\[CrossRef\]](#)
32. Grindrod, K.; Khan, H.; Hengartner, U.; Ong, S.; Logan, A.G.; Vogel, D.; Gebotys, R.; Yang, J. Evaluating authentication options for mobile health applications in younger and older adults. *PLoS ONE* **2018**, *13*, e0189048. [\[CrossRef\]](#)
33. Silva, H.L.S.R.P.D.; Wittebron, D.C.; Lahiru, A.M.R.; Madumadhavi, K.L.; Rupasinghe, L.; Abeywardena, K.Y. AuthDNA: An Adaptive Authentication Service for any Identity Server. In Proceedings of the International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka, 5–6 December 2019.
34. Gebrie, M.T.; Abie, H. Risk-Based Adaptive Authentication for Internet of Things in Smart Home eHealth. In Proceedings of the Proceedings of ECSA'17, Canterbury, UK, 11–15 September 2017; 7p. [\[CrossRef\]](#)
35. Azmi, K.; Bakar, A.; Daud, N.I. Adaptive Authentication: A Case Study for Unified Authentication Platform. In Proceedings of the CS and IT-CSCP 2015, Chennai, India, 25–26 July 2015; pp. 61–72.
36. Ehatisham-ul Haq, M.; Azam, M.A.; Loo, J.; Shuang, K.; Islam, S.; Naeem, U.; Amin, Y. Authentication of smartphone users based on activity recognition and mobile sensing. *Sensors* **2017**, *17*, 2043. [\[CrossRef\]](#)
37. Chakraborty, N.; Li, J.; Mondal, S.; Chen, F.; Pan, Y. On overcoming the identified limitations of a usable pin entry method. *IEEE Access* **2019**, *7*, 124366–124378. [\[CrossRef\]](#)
38. Khan, H.; Grindrod, K. Evaluating Smartphone Authentication Schemes with Older Adults. In Proceedings of the SOUPS 2016, Denver, CO, USA, 22–24 June 2016.
39. Singh, J.; Kam, Y.H.s. Usable Authentication Methods for Seniors. *Int. J. Recent Technol. Eng.* **2019**, *8*, 94–100. [\[CrossRef\]](#)
40. Gurnani, B.; Kaur, K.; Sharma, T.; Sharma, V. Commentary: Unfolding the role of biometric identification procedures in the current digital era. *Indian J. Ophthalmol.* **2023**, *71*, 61–62. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perlner, R.A.; Regenscheid, A.R.; Burr, W.E.; Richer, J.P.; Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; et al. *Digital Identity Guidelines: Authentication and Lifecycle Management*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. [\[CrossRef\]](#)
42. Zheng, Z.; Pan, T.; Song, Y. Development of Human Action Feature Recognition Using Sensors. *Inf. Technol. J.* **2022**, *21*, 8–13. [\[CrossRef\]](#)
43. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Internet of Things for Smart Cities: Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. *IEEE Netw.* **2019**, *33*, 82–88. [\[CrossRef\]](#)
44. Shi, C.; Liu, J.; Liu, H.; Chen, Y. Smart User authentication through actuation of daily activities leveraging WiFi-enabled IoT. In Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Chennai, India, 10–14 July 2017; Volume Part F1291. [\[CrossRef\]](#)
45. Batool, S.; Saqib, N.A.; Khattack, M.K.; Hassan, A. *Identification of Remote IoT Users Using Sensor Data Analytics*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 69, pp. 328–337. [\[CrossRef\]](#)
46. Gonzalez-manzano, L.; Fuentes, J.M.D.E.; Ribagorda, A. Leveraging User-related Internet of Things for Continuous Authentication: A Survey. *ACM Comput. Surv.* **2019**, *52*, 1–38. [\[CrossRef\]](#)
47. Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. *Comput. Secur.* **2016**, *63*, 85–116. [\[CrossRef\]](#)
48. Hintze, D.; Koch, E.; Scholz, S.; Mayrhofer, R. Location-based risk assessment for mobile authentication. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany, 12–16 September 2016; Association for Computing Machinery: New York, NY, USA, 2016; UbiComp'16, pp. 85–88. [\[CrossRef\]](#)
49. Arias-cabarcos, P. A Survey on Adaptive Authentication. *ACM Comput. Surv.* **2019**, *52*, 80. [\[CrossRef\]](#)

50. Gamundani, A.M.; Phillips, A.; Muyingi, H.N. An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 50–57. [\[CrossRef\]](#)
51. Albalawi, A.; Almrshed, A.; Badhib, A.; Alshehri, S. A Survey on Authentication Techniques for the Internet of Things. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–5. [\[CrossRef\]](#)
52. Sahu, A.K.; Sharma, S.; Tripathi, S.S.; Singh, K.N. A Study of Authentication Protocols in Internet of Things. In Proceedings of the 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 19–21 December 2019; pp. 217–221. [\[CrossRef\]](#)
53. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare. *IEEE Internet Things J.* **2022**, *9*, 2649–2656. [\[CrossRef\]](#)
54. Gope, P.; Millwood, O.; Sikdar, B. A Scalable Protocol Level Approach to Prevent Machine Learning Attacks on Physically Unclonable Function Based Authentication Mechanisms for Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1971–1980. [\[CrossRef\]](#)
55. Ahmed, K.I.; Tahir, M.; Habaebi, M.H.; Lau, S.L.; Ahad, A. Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction. *Sensors* **2021**, *21*, 5122. [\[CrossRef\]](#)
56. Griffin, P.H. Secure authentication on the Internet of Things. In Proceedings of the SoutheastCon 2017, Concord, NC, USA, 30 March–2 April 2017; pp. 1–5. [\[CrossRef\]](#)
57. Brown, B. 802.11: The security differences between b and i. *IEEE Potentials* **2003**, *22*, 23–27. [\[CrossRef\]](#)
58. Khan, M.A.; Din, I.U.; Almogren, A. Securing Access to Internet of Medical Things Using a Graphical-Password-Based User Authentication Scheme. *Sustainability* **2023**, *15*, 5207. [\[CrossRef\]](#)
59. Bali, M.; Yenikar, A. IOT-based secure wireless medical sensor networks using multifactor authentication. In *Futuristic Trends in IOT Volume 3 Book 2*; IIP Edited Book Series; Selftype Developers Pvt. Ltd.: Chikmagalur, India, 2024; pp. 146–162. [\[CrossRef\]](#)
60. Kumar, T.; Braeken, A.; Liyanage, M.; Ylianttila, M. Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017. [\[CrossRef\]](#)
61. Sharma, G.; Singh, G. Robust User Authentication Scheme for IoT-Based Healthcare applications. In *Recent Advancements in Smart Remote Patient Monitoring, Wearable Devices, and Diagnostics Systems*; IGI Global: Hershey, PA, USA, 2023; pp. 170–182. [\[CrossRef\]](#)
62. Khan, M.; Ud Din, I.; Majali, T.; Kim, B.S. A Survey of Authentication in Internet of Things-Enabled Healthcare Systems. *Sensors* **2022**, *22*, 9089. [\[CrossRef\]](#) [\[PubMed\]](#)
63. Hayashi, V.T.; Ruggiero, W.V. Hands-Free Authentication for Virtual Assistants with Trusted IoT Device and Machine Learning. *Sensors* **2022**, *22*, 1325. [\[CrossRef\]](#)
64. Uscs. Choosing A Default Authentication Method. *Inf. Technol. Serv.* **2019**.
65. Hew, C.W.; Ramasamy, M.R.S. Development of a IoT Based Low Cost Wearable Smart Health Monitoring System for Elderly. In Proceedings of the 2022 IEEE 8th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Melaka, Malaysia, 26–28 September 2022. [\[CrossRef\]](#)
66. Avi, A.M.; Rana, M.S. An android application and speech recognition-based IoT-enabled deployment using NodeMCU for elderly individuals. *Bull. Electr. Eng. Inform.* **2023**, *12*, 2763–2776. [\[CrossRef\]](#)
67. Adekanmbi, O. Assessment Of User Authentication Risks In A Healthcare Knowledge Management System. *Res. Int. Bus. Financ.* **2015**, *14*, 95–106. [\[CrossRef\]](#)
68. Hyun-Kyung, P.; Seo, B.J.; Hyun-Min, O.; Lee, J.H. Risk Analysis Apparatus and Method for Risk Based Authentication. U.S. Patent 11,003,749, 2018.
69. Lester, M.W.; Casillas, D.R.; Davey, R.A.; Morris, M.F.; Mortensen, M.K.; Row, J.D.; Buckingham, T.B.; Sanclemente, T. Scalable Risk-Based Authentication Methods and Systems. U.S. Patent 10,432,605, 1 October 2019.
70. Hayashi, E.; Hong, J.; Das, S.; Amini, S.; Oakley, I. CASA: Context - Aware Scalable Authentication. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS) 2013, Newcastle, UK, 24–26 July 2013; pp. 1–10.
71. Forget, A.; Chiasson, S.; Biddle, R. Choose Your Own Authentication. In Proceedings of the NSPW, Twente, The Netherlands, 8–11 September 2015.
72. Wójtowicz, A.; Chmielewski, J. Model for adaptable context-based biometric authentication for mobile devices. *Pers Ubiquit Comput.* **2016**, *20*, 195–207. [\[CrossRef\]](#)
73. Arias-Cabarcos, P.; Krupitzer, C. On the design of distributed adaptive authentication systems. In Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, USA, 12–14 July 2017.
74. Veziroğlu, M.; Veziroğlu, E.; İhsan Ömür Bucak. *Performance Comparison Between Naive Bayes and Machine Learning Algorithms for News Classification*; IntechOpen: Rijeka, Croatia, 2024; Chapter 5. [\[CrossRef\]](#)
75. Kumar, R.; Goswami, B.; Mhatre, S.M.; Agrawal, S. Naive Bayes in Focus: A Thorough Examination of its Algorithmic Foundations and Use Cases. *Int. J. Innov. Sci. Res. Technol.* **2024**, *9*, 2078–2081. [\[CrossRef\]](#)
76. Azizah, M.F.; Paramitha, A.T. Predictive Modelling of Chronic Kidney Disease Using Gaussian Naive Bayes Algorithm. *Int. J. Artif. Intell. Med Issues* **2024**, *2*, 125–135. [\[CrossRef\]](#)

77. Garba, M.; Usman, M.; Gulumbe, A.M. Improving Breast Cancer Detection with Naive Bayes: A Predictive Analytics Approach. *Comput. Sci. Inf. Technol.* **2024**, *14*, 185–196. [[CrossRef](#)]
78. Department of Health, Education, and Welfare. The Belmont Report. 1979. A Foundational Document in the Field of Bioethics. Available online: <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html> (accessed on 28 January 2023).

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.