sustainability

Article

A Novel Cloud-Based IoT Framework for Secure Health Monitoring

Sahar Ebadinezhad [1,2,*] and Temitope Emmanuel Mobolade [1]

[1] Department of Computer Information Systems, Near East University, Nicosia 99138, Cyprus; 20184976@std.neu.edu.tr
[2] Computer Information Systems Research and Technology Center (CISRTC), Near East University, Nicosia 99138, Turkey
* Correspondence: sahar.ebadinezhad@neu.edu.tr

Abstract: The growing use of Internet of Things (IoT) technologies in a variety of sectors, including healthcare, has opened up new possibilities for gathering and analyzing patient data. In some cases, the elderly are exposed to significant risk and even mortality as a result of the global aging problem, which has become a burden in recent years. Numerous IoT devices are being created to monitor, track, and record the actions of the elderly to reduce these hazards. This study proposed a novel, dependable, cloud-based remote system patient monitoring framework for IoT health detection. The main distinguished part of this research is that we rarely can find a framework in the literature that is based on real-time systems by considering heartbeat (BPM), blood oxygen (SpO2), and body temperature at the same time. The implementation and testing of this real-time system is classified into six distinctly separated phases for developing both the hardware and software. To verify the performance of the suggested system, data were gathered from BOT-IoT datasets. The outcome enhances patient satisfaction, secure data transmission, and healthcare outcomes by showing that the proposed framework is more efficient than other compared protocols in terms of the decision time, which is 16.3 seconds for 46 features, with 100% accuracy.

Keywords: anomaly detection; cloud computing; health monitoring system; healthcare IoT architecture real-time monitoring; secure data transmission

check for updates

Citation: Ebadinezhad, S.; Mobolade, T.E. A Novel Cloud-Based IoT Framework for Secure Health Monitoring. *Sustainability* **2024**, *16*, 1349. https://doi.org/10.3390/su16031349

Academic Editor: Xiuwen Fu

Received: 8 October 2023
Revised: 4 January 2024
Accepted: 15 January 2024
Published: 5 February 2024

1. Introduction

The use of technology related to the Internet of Things (IoT) has significantly increased over the past several years in a variety of industries, and the healthcare industry is no exception. By enabling the collection and analysis of real-time patient data, the Internet of Things has the potential to completely transform the healthcare sector. This could lead to more precise diagnosis, individually tailored treatments, and remote health monitoring. One of the most significant applications of the Internet of Things in healthcare is the secure monitoring of patient health data, which requires cloud-based Internet of Things platforms [1].

Cloud-based Internet of Things for secure health monitoring combines the functionality of Internet of Things devices with the scalability and flexibility of cloud computing. For individuals involved in healthcare as well as those performing research on patients and their ailments, this convergence ushers in a new era. With the use of cloud infrastructure, data from a wide range of Internet of Things gadgets, such as wearable, sensors, and medical equipment, may be gathered, processed, and analyzed in real time. Utilizing cloud computing allows for this. This aids medical professionals in making decisions in a timely manner while also being well-informed, which ultimately results in improved patient care, earlier diagnosis of health problems, and preventative actions [2].

Adopting the IoT for reliable monitoring of health is no exception to the rule that data security is essential for healthcare applications. In 2022, there was a greater emphasis placed on the creation of stringent security measures to safeguard private health information that was transmitted and kept in the cloud. Advances in encryption methods, protocols related to secure data transmission, as well as access control mechanisms have been implemented to ensure that patient information is always accessible while maintaining its integrity and confidentiality. Furthermore, developments in machine learning and anomaly detection algorithms have made it possible to predict impending security breaches and take preventative measures [3].

The cloud-based IoT for safe health monitoring transforms healthcare through real-time data collection, assessment, and decision-making capabilities. As a result, costs decrease, and output improves. The significant progress achieved in 2022 and 2023 enabled the broad adoption of these technologies by easing concerns over interoperability, data security, and privacy. Enhancing patient care, identifying health problems early, and fostering more teamwork are all advantageous to patients, medical professionals, and researchers. Cloud-based IoT offers huge possibilities for the development of healthcare since it offers the key to transforming how we track and manage our own health.

The main motivation of our study, which could be beneficial for the readers and other researchers who would like to work in a similar field, is that our work establishes a new standard for healthcare monitoring by creating a microcontroller device and a strong framework for connecting Internet of Things devices to cloud infrastructure. Our secure protocol emphasizes the crucial need for enhanced privacy and security in health monitoring by ensuring real-time data collecting and analysis. We advocate for more research in this area by stressing the importance and benefits of this approach and addressing the security problems that currently exist in traditional health monitoring systems via a careful analysis of potential attacks and thorough assessments by employing machine learning algorithms. This driving force highlights how revolutionary our work may be in changing the face of safe health monitoring. Also, the contributions of this research are the following:

- Developing a microcontroller device for healthcare detection and monitoring;
- Proposing a secure framework and protocol in healthcare monitoring by emphasizing the integration of these IoT devices with cloud infrastructure for real-time data collecting and analysis in terms of hardware and software;
- Creating a compelling case for more research in this area by highlighting the significance and advantages of secure health monitoring utilizing cloud-based IoT;
- Exploring the security issues with conventional health monitoring systems by the use of four (4) machine learning algorithms and the impact of seven (7) attacks.

Moreover, this research contributes toward sustainable development and the application of sustainability. These sustainable integrated approaches aim to increase healthcare efficiency by utilizing a remote cloud-based system for a patient monitoring system that ensures successful interventions with little resource use. IoT devices are vital for risk reduction, especially when it comes to threats that older people have to face. This helps to meet sustainable goals for global health and well-being. By reducing unnecessary operations and associated costs, the application of an IoT-based data-driven solution promotes treatment accuracy and sustainability. Setting secure data transfer as a top priority demonstrates a dedication to long-term technological solutions that guarantee patient confidentiality and data protection. Deployment of cloud-based solutions also minimizes the need for physical infrastructure, which is in line with sustainability standards since it decreases energy and environmental impact. The consequent improvement in patient satisfaction supports preventative care and regimen adherence, which supports sustainable healthcare practices. In addition, adopting IoT technologies improves accessibility to healthcare, especially in underprivileged areas, aligning with sustainability objectives for fair and equal access to high-quality medical care.

Therefore, based on these research contributions, we can emphasize the main distinguished part of this study, which is based on real-time systems by considering heartbeat (BPM), blood oxygen (SpO2), and body temperature at the same time. This important matter rarely can be found in the literature. The implementation and testing of this real-time system are classified into six distinctly separated phases for developing both the hardware and software of our HCPMP framework.

The following is how the research is structured going forward: Section 2 delves into details about the relevant research. Section 3 provides an explanation of the several algorithms related to the Internet of Medical Things (IoMT). In Section 4, the technique is elaborated upon, with stages defined and a comprehensive proposed framework presented. The performance evaluation and research findings are covered in Section 5. Finally, a thorough discussion based on the findings and results is presented in Section 6.

2. The Literature Review

2.1. Secure Health Monitoring Using Cloud-Based IoT

Cloud-based IoT is becoming more and more valuable to the healthcare industry for secure health monitoring. By connecting devices with cloud infrastructure, it may improve real-time data collecting and analysis, ultimately leading to better patient care. Renowned for its scalability and versatility, this groundbreaking technology prioritizes patient data privacy and reliability, providing improved healthcare outcomes [1]. This study of the literature examines the advancements and difficulties in reliable health monitoring in cloud-based IoT, acknowledging the potential of IoT. With Singh and Chatterjee present an edge-centric model for safe health monitoring that emphasizes continuous surveillance, privacy, and reliable data transmission, edge computing is essential. Their study emphasizes how important it is to have strong security measures in place in order to reduce possible hazards [1].

Saif et al. (2022) examine reliable healthcare in the context of IoT and offer a thorough examination of standards along with a case study illustrating IoT's use in security health monitoring. In order to protect the integrity and confidentiality of healthcare data, their study emphasizes the need for strong security of information, confidentiality, and access control measures [2].

When considering issues in cloud-based IoT for health monitoring systems, it is imperative to address the significant factors of data security and privacy concerns. This study investigates the privacy and security concerns associated with healthcare systems based on the IoT [3]. The aforementioned issues highlighted are data breaches, unauthorized access, and platform-to-platform information exchange, which are deemed significant concerns. This study emphasizes the necessity of enhancing encryption techniques, implementing secure data transfer protocols, and employing access control systems to safeguard sensitive patient data.

The study conducted by Tiwari, Nahak, and Mishra (2023) examines the transformative capacity of the IoT in the realm of healthcare monitoring [4]. Their research highlights the significance of real-time data gathering and analysis facilitated by IoT and its potential to bring about a paradigm shift in the provision of healthcare services. Their study emphasizes the need for reliable and scalable IoT solutions in order to ensure secure health monitoring.

Moreover, interoperability is an additional concern in the realm of cloud-based IoT for health monitoring. Standardized communication protocols and data formats play a crucial role in facilitating smooth integration and efficient data transmission among IoT devices, healthcare systems, and cloud platforms [5]. This study suggests a real-time wearable health monitoring device that runs on the IoT and is cloud-based. It highlights how crucial interoperability is to enable thorough patient monitoring and effective care coordination.

2.2. Healthcare Systems

According to the increased operational effectiveness brought about by the adoption of IoT technology, healthcare organizations can now offer high-quality care at a lower cost. Consequently, healthcare professionals can provide patients with improved services and improved diagnostic capacities [6]. Biometric sensors gather indicators of a person's health for use in intelligent health systems. For the Internet of Things to function well, cloud computing infrastructure is necessary for efficient interactions between patients and caregivers or medical professionals [7].

Automated communication systems facilitate efficient information sharing on patients' current health status. This allows medical professionals to utilize established smart healthcare systems effectively [7]. Wearable technology's seamless communication with other devices enables comprehensive monitoring of physiological data, from blood pressure to oxygen saturation [8]. Online patient health portals facilitate easy communication of patient information among stakeholders. The IoT cloud platform, utilizing wearables, sensors, and mobile health initiatives, collects patient data. This information is then utilized by healthcare professionals, specialists, and insurers for effective care and preventative measures. Integrating cloud technology with IoT devices streamlines real-time data collection and accessibility for both patients and healthcare providers, offering numerous advantages [9].

2.3. Patient Health Monitoring System

The main goal of this section is to provide an explanation of health monitoring system for patients. The system is intended to efficiently and thoroughly track and monitor patients' health status. The main goal of the presented system by [10] is to efficiently track and document patients' health conditions in a medical context. It has been demonstrated that the healthcare sector greatly benefits from the use of IoT sensors, especially when it comes to remote patient health monitoring. The technologies that are used by the system are varied. This feature makes it easier for healthcare providers to monitor and evaluate their patients' health from a distance, which allows them to provide prompt advice and treatments that improve patient outcomes [10]. A three-tier architecture is frequently used for remote patient health monitoring. Wearable sensors are used as data sources at the network tier to measure things like blood pressure and body temperature.

The second IoT architecture level facilitates information exchange among sensors. The top tier involves nodes responsible for processing and analyzing collected data for research purposes [11]. Individuals with disabilities can access ambient assisted living services, providing companionship and health-related support. Integrated sensing, computation, and communication systems, including surgically implanted sensors like a heartbeat simulator, aid daily activities. Interconnected sensors in various items store data in a centralized cloud, facilitating analysis by caregivers. These devices, featuring biometric measurements like electrocardiograms, enable remote monitoring for improved healthcare [12].

2.4. Components of an Internet of Things (IoT)-Enabled Healthcare System

2.4.1. Data Acquisition

The process of obtaining data from a patient or healthcare unit involves the utilization of a sensor. Several sensors can be utilized for various purposes. For instance, the DS18B20 sensor is commonly employed for the acquisition of heartbeat readings. Additionally, the microcontroller Arduino Uno ATmega 328P is capable of capturing body temperature data [13].

2.4.2. Cloud Computing System

The recorded data from sensing devices are transmitted to a processor, such as the HLK-RM04 Serial, via a Wi-Fi module and subsequently saved on a MySQL server. The establishment of this connection is facilitated by the HTTP protocol [14].

2.4.3. The Real-Time Health Gateway

The Real-Time Health gateway allows users to access healthcare data through a Java-based gateway. This portal is accessible through various devices, such as mobile laptops, tablets, and personal computers, typically via Android applications. A possible example would be a smartphone application created to notify people on their phones every time a patient's condition is identified [15].

2.5. The Utilization of Cloud-Based IoT for the Purpose of Ensuring Secure and Intelligent Health Monitoring

Many academics are quite interested in using cloud-based IoT technology for health monitoring, especially when it comes to security and intelligence [16–19]. Thus, this section's goal is to provide a thorough analysis of previously released academic papers about cloud and Internet of Things technologies concerning health monitoring systems.

The goal of the proposed model was to enable early disease diagnosis by offering a reliable remote health surveillance system within a cloud-based IoT environment [16]. This paper presented a framework for health monitoring that ensures the integrity of medical and health data in the cloud by utilizing a remote health tracking approach and lightweight block cryptography methods. A patient's health state may now be evaluated and the advent of extremely critical situations can be predicted thanks to the use of methods for data mining in biological data analysis. This is now feasible because of the use of intelligent healthcare IoT gadgets, which use effective and safe block encryption techniques. A strong encryption technique was used to protect private patient information. In their study that combined IoT and cloud technologies, the researchers mainly depended on a sizable amount of data from IoT sensors as their primary resource.

An IoT-based mobile health platform for illness diagnosis was suggested by Verma and Sood in 2018 [20]. The primary goal of the project was to use medical IoT devices to collect health measures and then create student diagnostic results (SDR). To create health data from the perspective of students, the researchers methodically used medical sensors and a dataset they obtained from the Catholic University of California, Irvine (UCI). Finding students who had manifested severe disease was the primary goal. The researchers used contemporary algorithms for classification and diagnostic techniques to confirm the results. The calculation took into account the following metrics: sensitivity; specificity; f-measures; and accuracy. This study's conclusions state that patterns, frequencies, and scales must be used in diagnostic methods in order to diagnose people with certain disorders.

Ahmed M. R. et al. [21] introduced a novel four-tier architecture that leverages cloud computing to expedite the detection of cardiovascular illnesses. Their study employed five supervised machine learning techniques: decision trees (DT); random forests (RF); artificial neural networks (ANN); naïve Bayes (NB); and support vector machines (SVM). The primary objective of their investigation was to assess the efficacy of the chosen classification methods. Additionally, the researchers employed widely accepted evaluation criteria to evaluate the effectiveness of several machine learning algorithms. To further assess the five classifiers, the 10-fold cross-validation process was used.

Based on the conducted trials, the artificial neural network performed exceptionally well in the areas of accuracy, F-1 scores, precision, and sensitivity specificity. As such, the application of this particular program makes it possible to predict operational cardiovascular diseases, which, in turn, makes it easier to track health-related information for those who suffer from heart problems.

A study by Yang et al. (2016) looked into an IoT-based cloud-based electrocardiogram (ECG) monitoring system [22]. Creating a system that can be applied to intelligent healthcare environments was the aim of their study. The researchers proposed a novel method for using the Internet of Things to monitor ECG. ECG data are collected via a wearable surveillance node and then wirelessly transmitted to the Internet of Things cloud. The MQTT and HTTP protocols are used by the IoT cloud to provide users with real-time ECG data in a graphical format. The difficulty of cross-platform interoperability has been somewhat lessened by the simplicity with which web browser-equipped smart terminals might retrieve ECG data. Experiments are undertaken on individuals who are in good health in order to assess the reliability of the system. The empirical evidence illustrates that the suggested system exhibits a high level of dependability in the acquisition and presentation of ECG data in real time. This capability holds the potential to assist in the initial identification of specific cardiac ailments.

Begum et al. devised a framework known as the Smart Healthcare Monitoring System within the IoT [23]. The principal aim of this framework is to enable individuals with cardiac conditions to accurately assess their body temperature, heart rate (measured in beats per minute), and body position in a sanitary setting. The evaluation of the framework is conducted on a participant who willingly participates in this study. During the evaluation, various physiological parameters, such as body temperature and heart rate, are measured. Additionally, the participant's body movement is observed, and the ECG graph is analyzed using serial plotting software hosted on a local server. The e-health system created by Monteiro et al. is founded on the integration of the IoT, fog computing, and cloud computing [24]. The authors propose an advanced e-health architecture that utilizes IoT for data collection, fog computing for preliminary data processing and temporary storage, and cloud computing for data analysis, processing, and long-term storage. Furthermore, there are significant challenges related to the implementation of an e-health application that ensures optimal availability, performance, and accessibility while minimizing the expenses associated with deployment and maintenance.

In the context of this discourse, several noteworthy gaps in research have been identified, each pertaining to a specific aspect that warrants scrutiny and exploration. The identification and resolution of these gaps will result in the development of healthcare solutions that possess dependability, effectiveness, and ethical integrity while also harnessing the potential of cloud-based Internet of Things technologies.

While this study of the literature aims to examine the developments and obstacles in cloud-based IoT for intelligent, secure health monitoring, some of the existing gaps in the literature are addressed as follows. A significant area of unmet research need is developing strong security protocols to protect private health information. Complex data intelligence techniques and algorithms also need to be created to process the vast amounts of IoT data in the healthcare industry and provide predictive analytics, real-time surveillance, decision support, and anomaly detection. Communication frameworks and defined protocols are necessary to guarantee seamless integration and interoperability. Ensuring high levels of resilience and dependability is crucial for cloud-based IoT in the healthcare industry. It is imperative to tackle ethical and legal concerns, including patient permission, data ownership, and compliance with regulations such as GDPR and HIPAA.

3. Internet of Medical Things (IoMT) Algorithms

The algorithms that are employed in the context of the IoMT are a group of computational methods that were created expressly to analyze and understand the data generated by IoT devices in the healthcare industry. Numerous fields, including data analysis, natural language processing, control systems, predictive modeling, and decision assistance, could benefit from the application of these technologies. IoMT algorithms aim to improve patient outcomes, reduce healthcare costs, and enhance the overall healthcare system by providing healthcare professionals with valuable insights and knowledge.

3.1. Algorithms for Data Analysis in IoMT

When IoMT data analysis algorithms are used, computational methods are applied to analyze data from IoT devices in the healthcare industry to extract useful information. Making use of these techniques is essential for spotting trends, patterns, and anomalies that may be used to improve patient outcomes and reduce healthcare costs. The algorithms indicated above are utilized to identify patterns or trends in the data that could indicate the existence of a health issue, such as diabetes or a cardiac condition. The IoMT's data analysis algorithms can identify patterns, create prediction models, extract useful information, and examine signals coming from medical devices. Numerous data analysis methods can be used in the IoMT domain, including the following:

3.1.1. Statistical Analysis Algorithms

The purpose of analysis methods is to look over large datasets and find interesting patterns or trends in the data. These instruments can be used to create correlations between different data, such as blood pressure and heart rate;

3.1.2. Machine Learning Algorithms

Include a range of methods that are used to analyze data and find underlying patterns, such as supervised and unsupervised learning. It is possible to use predictive models to make predictions about future health problems;

3.1.3. Data Mining Algorithms

Large databases can have valuable information retrieved from them utilizing data mining techniques. These instruments can identify trends or patterns in the data that may point to a potential health issue. Signal processing algorithms are used in the examination and interpretation of data via IoT healthcare devices, particularly heart rate monitoring devices' ECG values. These technologies can identify trends or patterns in information that may indicate the existence of a potential health issue;

3.2. Statistical Analysis Algorithms for the IoMT

Statistical analysis techniques in the context of IoMT can be used to extract meaningful information from large-scale datasets generated by IoT-enabled medical devices. An algorithm can determine the average and variance in a patient's heart rate by using descriptive statistics. This allows for the discovery of abnormal heart rate patterns and may even aid in the diagnosis of a cardiac condition. Data can be succinctly summarized and descriptively illustrated through the use of statistical evaluation algorithms in the wider context of the IoMT. Its further uses include finding correlations between variables, drawing logical conclusions, and examining patterns and trends in data across time. Numerous statistical analytic techniques are suitable for IoMT, including the following:

This section's primary focus will be on the study of descriptive statistics. To summarize and characterize the data, the aforementioned approaches are used, among other things, to compute the mean, median, and standard deviation of a particular set of data. These technologies are capable of analyzing and spotting patterns or trends in the dataset. Additionally, temporal data analysis is utilized. These methods are used to evaluate information that has been systematically and purposefully collected over a predetermined time frame. These gadgets can recognize and evaluate patterns or trends in the data, including changes in heart rate over time;

3.3. Using Cryptographic Algorithms in the IoMT Environment

Cryptography plays a crucial role in ensuring the privacy and confidentiality of medical data within the framework of the Internet of Medical Things [25]. Cryptography is the purposeful use of mathematical methods to safeguard and preserve the authenticity, integrity, and confidentiality of data and communications. Cryptography is essential to ensuring the confidentiality, integrity, and validity of medical IoMT data. To ensure safe data processing by a variety of devices, safe data retention in databases, as well as secure data transit over networks, cryptographic techniques are used;

It is important to recognize that IoT devices are limited in energy, storage, and computing capabilities. Thus, in order to prevent overtaxing these devices and possibly jeopardizing their security, great care must be taken while selecting the encryption techniques that are utilized in them. In addition, medical institutions must comply with legal requirements like the Health Insurance Portability and Accountability Act (HIPAA), which requires the adoption of strong security protocols, one of which is the use of cryptography, to protect patient information. The choice of cryptographic algorithm for Internet of Medical Things (IoMT) systems depends on the particular needs and constraints of the system in question.

On the other hand, several cryptographic techniques often used in IoMT applications have been found [26].

3.3.1. The Advanced Encryption Standard (AES)

One popular symmetric encryption technique used for encrypting information in IoMT systems is AES. The system is quick, has strong security features, and does not have much processing power.

3.3.2. Rivest–Shamir–Adleman (RSA)

A popular type of asymmetrical encryption that is often used for the safe transfer of cryptographic keys between devices in IoMT systems is the RSA method. Additionally, it is often used for the objective of digital certificate verification.

3.3.3. Elliptic Curve Cryptography (ECC)

Because of its strong security features and small key size, ECC is becoming a more popular asymmetric encryption technique in IoMT systems. Hashing functions are important in the field of computer science. Hash functions are commonly used in IoMT systems to protect data integrity. Moreover, these technologies have real-world uses in the field of digital signature methods.

3.3.4. Light-Weight Cryptography (LWC)

LWC is an innovative cryptography technique designed specifically to meet the needs of low-power devices, which are commonly found in the IoT space. The encryption technique that is being examined stands out due to its energy efficiency, affordability, and lightweight construction.

It is crucial to recognize that an algorithm's effectiveness depends on both its underlying architecture and how it is put into practice. Implementation performed correctly is essential to maintaining system security. Moreover, in order to successfully neutralize new threats and vulnerabilities, the system's security must be continuously monitored and updated [27,28].

3.4. Application of Elliptic Curve Cryptography (ECC) in the IoMT

The ECC's relatively small key size, strong security features, and ability to support digital signatures and exchange of keys make it a very good choice for deployment in IoMT systems. Furthermore, the encryption algorithm's smaller key size helps devices require less processing and storage power. Because of this feature, it is especially well-suited for usage in IoMT systems that operate with constrained resources, like IoT devices. Attacks using quantum computing are less likely to succeed with ECC, a problem that could occur with other encryption methods. The following steps are often included in the integration of ECC into IoMT systems; key creation within the IoMT security architecture is generating distinct key pairs utilizing NIST-compliant ECC techniques. The ECC method and public key are used to encrypt medical data, guaranteeing safe transfer or storage. The private key and the ECC method are necessary for decryption. Safeguarding keys, creating new ones, and removing compromised keys are all essential components of key management. Hashing functions detect unauthorized modifications, preserving data integrity. Authentication limits access to authorized entities by using digital signatures or certificates. ECC ensures confidentiality and communication integrity by facilitating secure key exchange. Maintaining system performance and mitigating emerging hazards require frequent updates and monitoring.

- It is imperative to recognize that the incorporation of ECC inside IoMT systems may display unpredictability, depending on the unique requirements and constraints of the system. Furthermore, to effectively handle new threats and vulnerabilities in the system, continuous monitoring and security system maintenance are essential. The ECC technique is a type of cryptography using public keys that provides a higher degree of security with smaller key sizes than other public-key cryptography techniques such as RSA. This feature makes it extremely beneficial in situations where resources, including processing power and storage space, are scarce. Three integers in a row make up the provided data [29–31];

- Efficiency: When compared to other public-key encryption methods, the ECC algorithm exhibits better computational efficiency and requires less memory and computing resources. This feature makes it especially beneficial to use in situations when resources are limited, including mobile devices and Internet of Things devices [32–34];
- Scalability: Due to its versatility and scalability, ECC is appropriate for a wide range of applications with different security requirements. The degree of protection of ECC may be adjusted by increasing the key size, making it suitable for a range of applications that require various degrees of security [32,35];
- Resistance against attacks by quantum computers: Despite the anticipated increase in strength in the future, ECC is impervious to attacks by quantum computing devices. This is because ECC's underlying mathematics differs from other public-key encryption techniques that are susceptible to quantum computer attacks [29–31].

4. Methodology

To ensure safe data transmission against injection, password, scanning, denial-of-service, man-in-the-middle, and distributed denial-of-service attacks, we developed an Internet of Things patient monitoring tool and healthcare surveillance device in this study. Six machine learning models, including XGBoost, GradBoost, Decision Trees (DT), Random Forest (RF), Logistic Regression (LR), and Support Vector Machines (SVM), were assessed.

The choice of employing XGBoost, GradBoost, Decision Trees (DT), Random Forest (RF), Logistic Regression (LR), Support Vector Machines (SVM), and Random Forest (RF) in our study was due to our need for thoroughly assessing our IoT patient monitoring system within the proposed secure data transmission scheme. Each machine learning model contributes unique features and strengths to the research, guaranteeing a thorough evaluation of the system's functionality. We leverage a variety of algorithms to capture different aspects of the behavior of the model and determine the best strategy for improving security against a range of potential attacks, such as injection, password, man-in-the-middle, denial of service, distributed denial of service, and scanning attacks. Using various models may increase the accuracy and consistency of our results, which leads to a more complex comprehension of the system's effectiveness and resilience.

The following subsections will illustrate all the phases of development, testing, and comparison. For this research, we divided our experiment into six (6) consecutive and distinguished phases:

Phase 1: The proposal of the unique framework (HCPMP), which consists of three main stages: Control stage; Detection stage; and Data capturing stage;

Phase 2: Providing a Mobile application;

Phase 3: Providing real-time results for 37 individual patients from Cyprus;

Phase 4: Providing results for 630 individual patients by utilizing the **HealthAdvisor** dataset to ensure the accuracy of the obtained result from phase 2;

Phase 5: Providing outcome from the obtained result under various attacks such as man-in-the-middle, denial of service, distributed denial of service, injection, password, and scanning on each ML algorithm separately to obtain each ML's model accuracy, precision, recall, and F1-score after the attack;

Phase 6: Comparing the security aspects of HCPMP with algorithms that utilized the **BoT-IoT** dataset.

Each of these phases can be explained briefly in the following manner to illustrate assurance of data confidentiality, integrity, and availability in cloud-based IoT systems:

Phase 1: The Unique Framework (HCPMP) proposal:

Control Stage: To prevent unwanted access to the framework, access restrictions and user authentication procedures are put into place;

Detection Stage: Using anomaly detection methods to spot odd behaviors or patterns that might point to security risks;

Data Capturing Stage: Ensuring secure and encrypted data collection to prevent manipulation or interception during transmission;

Phase 2: Developing a Mobile App:

Secure Communication: Implementing secure connection protocols, such as HTTPS, can help prevent eavesdropping by encrypting data sent between the smartphone application and the server in the cloud;

Phase 3: Presenting 37 Different Patients' Real-Time Results:

End-to-end Encryption: Utilizing end-to-end encryption to ensure confidentiality while protecting sensitive health data as they are transferred from patients as individuals to the cloud;

Frequent Security Audits: To find and fix weaknesses in the system for delivering results instantly, conduct regular security audits;

Phase 4: Presenting 630 Individual Patients Their Results:

Data validation: By ensuring the integrity and quality of conclusions produced from a larger dataset (HealthAdvisor), data validation techniques boost data reliability (HealthAdvisor);

Data Anonymization: Employing strategies to uphold privacy norms and protect personal identities;

Phase 5: Presenting the Results of the Attacks Under Different Conditions:

Intrusion Detection Systems (IDS): Integrating IDS allows you to swiftly detect and stop attacks, maintaining system availability and integrity. Encryption techniques are used to secure data both during transmission and at rest. These techniques are particularly crucial in the scenario of a man-in-the-middle attack. Distributed denial of service (DDoS) mitigation is the use of DDoS mitigation strategies to preserve availability during denial-of-service attacks;

Phase 6: Comparing Security Aspects with Security Metrics from the BoT-IoT:

Dataset Comparison: By addressing integrity, availability, and confidentiality issues at each step of the HCPMP execution throughout cloud-based IoT platforms, these techniques integrate to establish a strong security posture. Consistent monitoring, assessment, and adaptation to new security threats are all part of this all-encompassing security plan. The BoT-IoT dataset is used to evaluate safety measures like precision, recall, and F1-score to contrast the safety features of HCPMP with methods. Confidentiality strategies will help to ensure that no individual's confidentiality within the BoT-IoT dataset is compromised during the comparison.

4.1. Data Collection Tool

This research design was modeled based on the pattern of the ESP32 version 1.0.6 methodological framework. The ESP32, a component of the ESP family, is a flexible microcontroller well-known for IoT applications. This study's approach, which was inspired by ESP32 IoT health initiatives, emphasizes the use of its capabilities for health monitoring. Moreover, tests were conducted and collected from people whose vitals were intact, as well as from certain patients, e.g., heart patients, etc. The development of our system includes critical aspects that include both hardware and software components, which are specified with specifications in Table 1.

Moreover, the component details about the IoT device (Hardware Components)), which is proposed for patient monitoring, are provided in the list below.

Max 30100 pulse oximeter and heart rate sensor—This is a highly reliable integrated pulse oximeter and heart rate sensor IC. It detects pulse oximetry (SpO2) and heart rate (HR) signals with the aid of two LEDs, a photodetector, enhanced optics, and low-noise analog signal processing. The Max 30100 is a pulse oximeter and heart rate sensor designed to accurately measure and track heart rate and blood oxygen levels; The manufacturer and location for this device are Analog Devices, Inc., Wilmington, and Massachusetts, USA accordingly.

Table 1. Hardware and software components in our framework.

System Components	Specifications
Hardware	Max30100 pulse oximeter and heart rate sensor DHT 11 Node MCU (esp8266) Arduino Pro mini micro-controllers Extras (serial cables and a laptop)
Software	Flutter (open-source UI software development kit (SDK)) MySQL Server and IoT analysis platform (Thinger.IO) Visual Studio
Programing language	JavaScript, Python C++ on Arduino studio

DHT 11—This basic digital temperature and humidity sensor is incredibly inexpensive. Using a capacitive humidity sensor and a thermistor, it measures the ambient air and outputs a digital signal on the data pin (no analog input pins are needed). The DHT11 is a digital temperature and humidity sensor; The manufacturer and location for this device are AM2302, and Shenzhen, China accordingly.

Node MCU (esp 8266)—This is an open-source, Lua-based firmware and development board for Internet of Things applications. It consists of the ESP-12E module, which includes an ESP8266 chip with a Tensilica Xtensa 32-bit LX106 RISC microprocessor. This microprocessor has a configurable clock speed ranging from 80 MHz to 160 MHz and RTOS support. The NodeMCU has 128 KB of RAM and 4 MB of flash memory for storing data and applications; The manufacturer and location for this device are Espressif System, and Shanghai, China accordingly.

Arduino Pro mini microcontrollers—The Arduino Pro Mini is a small and low-cost microcontroller board that is based on the ATMEGA328P microcontroller. It is designed to be a compact, low-power alternative to the larger and more powerful Arduino boards, making it suitable for use in portable devices, battery-powered projects, and other applications where space and power consumption are important considerations; The manufacturer and location for this device are Arduino, and Torino, Italy accordingly.

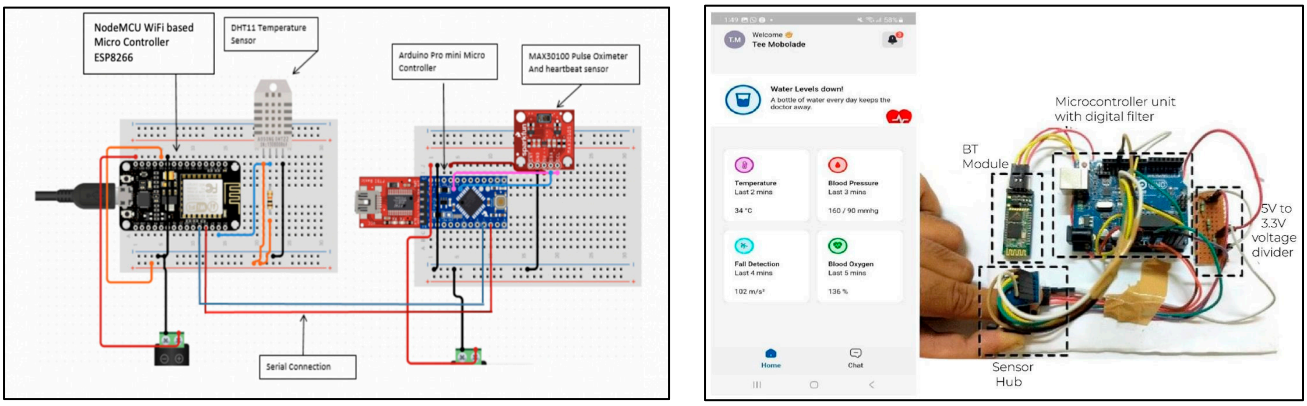
Extras—serial cables are utilized to facilitate communication between the Arduino board and other gadgets or a computer. A serial port, commonly referred to as a UART or USART, is included on every Arduino board, and some even have multiple of them. Pins 0 and 1 are used on older boards (Uno, Nano, Mini, and Mega) to communicate with the computer.

4.2. Data Collection Procedures

Our system incorporates two prominent microcontrollers. The utilization of the Node MCU, alternatively referred to as ESP8266, is essential for establishing an internet connection and facilitating the transmission of data to an internet server. Conversely, the Arduino Pro Mini assumes the role of the principal unit responsible for processing the acquired data. Moreover, it is equipped with two separate sensors that are utilized to evaluate the individual's well-being. The DHT11 sensor is commonly used for measuring temperature, whereas the Max30100 sensor is typically employed for monitoring heart rate and blood oxygen levels. The sensors are positioned in direct contact with the patient's finger, specifically the heartbeat sensor. Subsequently, the Arduino Pro-mini device is responsible for converting the unprocessed data acquired from the pulses detected by the said sensor into relevant information regarding the patient's heartbeat and blood oxygen levels. The identical procedure occurs when utilizing the DHT11 temperature sensor. The connection between the Arduino Pro-Mini and the ESP8266 is established through the hardware interface. This connection is required because the ESP8266 needs to receive the processed data from the Arduino Pro-Mini. In turn, the ESP8266 is in charge of enabling data analysis on the IoT platform and transferring information about patients to MySQL servers or databases. The construction of a serial communications link between the two controllers enables the accomplishment of this goal. One popular serial communication technique is the Ubiquitous Asynchronous Receiver–Transmitter (UART). The Rx and Tx ports on both microcontrollers can be used to transfer data from the wireless transmitter to the receiver. The ESP8266 is configured to use Wi-Fi to connect to the internet. After that, a patient's data are sent to the IoT analyzer. The patient's information is then sent via APIs (application programming interfaces) and HTTP (Hypertext Transfer Protocol) commands to the MySQL server and the IoT analysis platform. The IoT platform is responsible for the real-time monitoring and analysis of the patient's health status. The aforementioned data are also saved within the database to facilitate enhanced comprehension and utilization for several other objectives. The database will receive and store the patient's identification number, heartbeat measurement, blood oxygen saturation level, body temperature, as well as the timestamp indicating the date and time when the data were uploaded to the server or database.

4.3. Phase 1: Proposed Framework of Health Condition Prediction and Monitoring Protocol (HCPMP)

The suggested architecture (HCPMP), known as the Hybrid Cloud Performance Management Process, comprises three primary steps. The control stage involves the introduction of the patient or individual to the Max30100 sensors and the hardware health detection component depicted in Figure 1. The detection stage entails the placement of the individual's finger on the Max30100 sensor, and once it is detected by the IoT Patient Monitoring System, the person's information is identified, as illustrated in Figure 2. The data capturing stage involves the population of the patient's data into an SQL database after it has been detected by the IoT Patient Monitoring System.



(**a**) (**b**)

Figure 1. Health detection component of the developed device. (**a**) Hardware of health detection component. (**b**) Software and wearable devices.

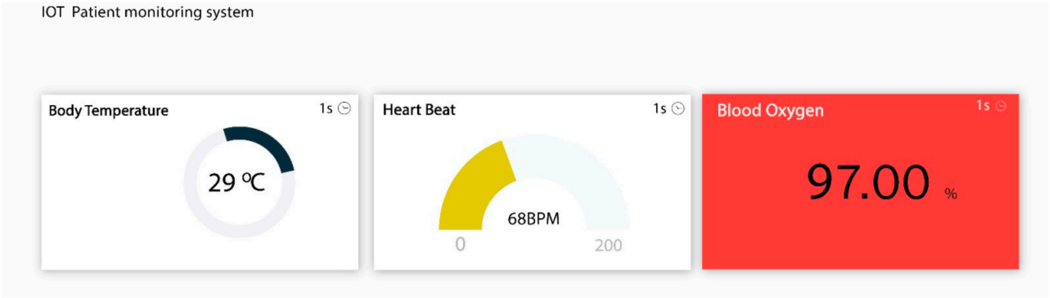


Figure 2. Detection stage.

In Algorithm 1, we give the primary framework presented, where the variable "BPM" denotes the expected heart rate in beats per minute; "SpO2" denotes the predicted oxygen saturation in percentage, and "Temp" denotes the predicted body temperature. The system utilizes a set of health features with specific threshold ranges for adults. These threshold ranges are as follows: the threshold range for beats per minute (BPM) is between 60 and 100 beats; the threshold range for oxygen saturation (SpO2) is between 96 and 98 percent; and the threshold range for body temperature is between 36.5 and 37.5 degrees Celsius. Table 2 presents the threshold range for each age group and type.

Table 2. Hardware and software components in our framework.

Feature	Threshold Range
Oxygen Saturation (Spo2)	
	Babies (0 to 12 months): 100 to 160 bpm for infants
95% to 100%	Kids (1–17 years old): 70–100 bpm
	Adults (above 18): 60 to 100 bpm
	Oral (Mouth): from 36.4 °C to 37.6 °C (from 97.6 °F to 99.6 °F)
Body Temperature (Temp)	Rectal (Rectum): from 37.0 °C to 38.1 °C (from 98.6 °F to 100.6 °F)
	Armpit (Axillary): from 35.9 °C to 37.0 °C (from 96.6 °F to 98.6 °F)

This study involved the administration of 37 sample tests to a cohort of 37 participants, with the results of only 5 individuals being shown in Table 3. The data were uniquely recorded for each individual, utilizing their login ID, heartbeat (BPM), blood oxygen (SpO2), body temperature, time stamps, and pertinent attributes such as "Age", "Gender", "BMI", "Activity Level", "Glucose", "Temp", "Health_status", and "Medication" are encompassed within the input features. The data were gathered from persons residing in Cyprus. In order to guarantee the precision of the acquired outcome, we incorporated the HealthAdvisor dataset into our protocol and conducted a comparative analysis of the security features between HCPMP and algorithms that employed the BoT-IoT dataset [36].

Table 3. Result for 5 individual patients.

Patient ID	Metric Data	Threshold	Data RTIoMT	Data with External Device
AA1231	**BPM**	60–100	70.994619	69.8
	SpO2	95–100	97	97
	Body Temp	36.5–37.5	29.685	30
AA1232	**BPM**	60–100	75.00	75.3
	SpO2	95–100	94	94
	Body Temp	36.5–37.5	20.00	20.1
AA1233	**BPM**	60–100	79.450255	79
	SpO2	95–100	95	95
	Body Temp	36.5–37.5	30.00	30.21
AA1234	**BPM**	60–100	57.60589	58
	SpO2	95–100	97	97
	Body Temp	36.5–37.5	27.53	27.31
AA1235	**BPM**	60–100	60.00	60.1
	SpO2	95–100	91	91
	Body Temp	36.5–37.5	38.00	38.02

Algorithm 1. Main framework of HCPMP

```
    Input:
        data = pd.read_csv('health.csv');
        patient's information;
        # Load the dataset (Training set $T_F$ consists of $N$ Features $F = \{f_1,....f_N\}$);
        # Split the data into features (X) and target variable (y);
        # Split the data into training and testing sets;
        # Scale the features using StandardScaler;
        # Logistic Regression;
        # Decision Tree;
        # Random Forest;
        # Support Vector Machines;
        # XGBoost;
        # GradBoost.
    Output:
        ○ Secure data transmission to the cloud server and hospital database;
        ○ Set of $N$ features providing the highest accuracy $F^* = \{f^*_1,....f^*_N\}$ (Generating the
      performance metric of collected data for each algorithm (Accuracy, Precision, Recall,
      F1-score));
        ○ Transformed Training set $T_{F*:}$
1.  Device initialization;
2.  DB connection and data processing;
3.  For each time interval tÎ T do {;
4.  Calculate BPM by using pseudocode 1;
5.  Calculate SpO2 by using pseudocode 2;
6.  Calculate BodyTemprature by using pseudocode 3;
7.  For i in {n,....N} do
    1: Train ML model on $T_F$;
    2: Evaluate model performance;
    3: Calculate feature importance or ranking;
8.  While the collected data from the Thresholdrange {,
    Return to patient real-time evaluation;
    Otherwise,
9.  IF BPM! = Thresholdrange Then {
         a. Send voice alert "BPM is abnormal";
         b. Send BPM value to the cloud server securely by integrating ECC based encryption
            algorithm;
         c. Send an emergency call to the ambulance and notify the doctor};
10. IF SpO2! = Thresholdrange Then {
         a. Send voice alert "SpO2is abnormal";
         b. Send SpO2value to the cloud server by integrating ECC based encryption algorithm;
         c. Send an emergency call to the ambulance and notify the doctor};
11. IF BodyTemprature! = Thresholdrange Then {
         a. Send voice alert "BodyTemprature is abnormal";
         b. Send BodyTemprature value to the cloud server by integrating ECC-based
            encryption algorithm;
         c. Send an emergency call to the ambulance and notify the doctor};
    End while}
  End For}
End for
12. Return $T_{F*}$, $F^*$ (Generate the performance metric of collected data (Accuracy, Precision,
    Recall, F1-score))
13. Stop.
```

Pseudocode 1. Calculating BPM

```
# Step 1: Define Standard Thresholds
          bpm_threshold_min = 60
          bpm_threshold_max = 100
# Step 2: Data Preprocessing
          data = pd.read_csv('your_dataset.csv')
# Step 3: BPM Measurement
          abnormal_bpm = data[(data['BPM'] < bpm_threshold_min) | (data['BPM'] >
          bpm_threshold_max)]
# Step 4: Generate Measurement Results
          if not abnormal_bpm.empty:
          print("Abnormal BPM Measurements:")
          print(abnormal_bpm)
# Step 5: Return measurement's status
          BPM_status = (BPM >= BPM_threshold)? 'Normal': 'Abnormal'
```

Pseudocode 2. Calculating SpO2

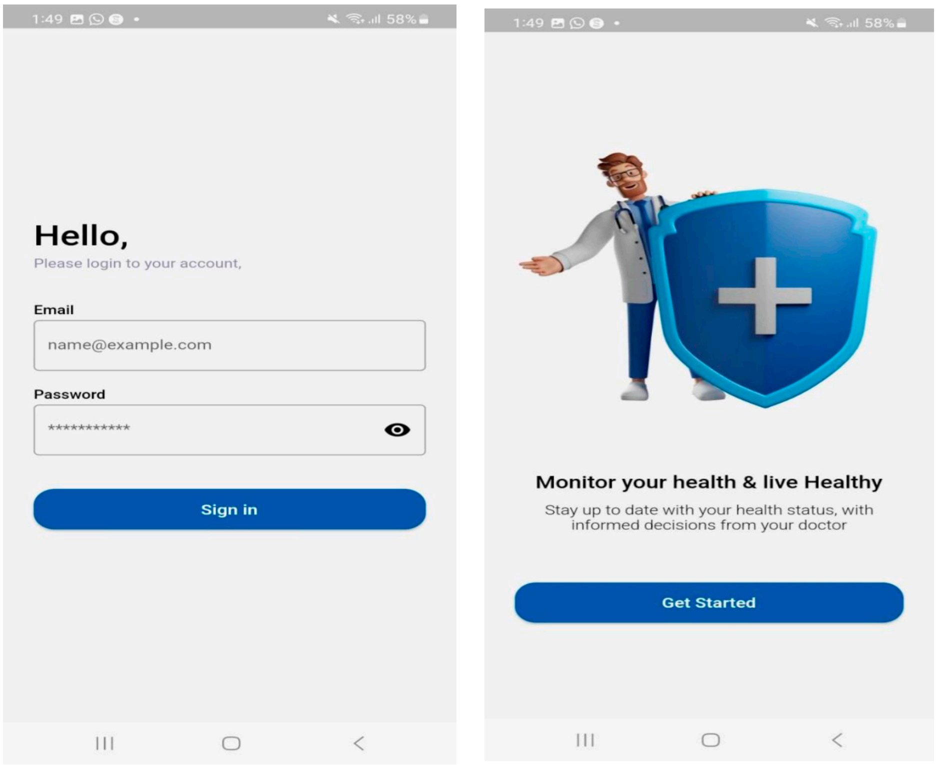
```
# Step 1: Define Standard Thresholds
          spo2_threshold_min = 95
# Step 2: Data Preprocessing
          data = pd.read_csv('your_dataset.csv')
# Step 3: SpO2 Measurement
          abnormal_spo2 = data[data['SpO2'] < spo2_threshold_min]
# Step 4: Generate Measurement Results
          if not abnormal_spo2.empty:
          print("Abnormal SpO2 Measurements:")
          print(abnormal_spo2)
# Step 5: Return measurement's status
          SpO2_status = (SpO2 >= SpO2_threshold)? 'Normal': 'Abnormal'
```

Pseudocode 3. Calculating BodyTemprature

```
# Step 1: Define Standard Thresholds
          temperature_threshold_min = 36.5
          temperature_threshold_max = 37.5
# Step 2: Data Preprocessing
          data = pd.read_csv('your_dataset.csv')
# Step 3: Temperature Measurement
          abnormal_temperature=data[(data['Temperature']<temperature_threshol
          d_min)|(data['Temperature']
          >temperature_threshold_max)]
# Step 4: Generate Measurement Results
          if not abnormal_temperature.empty:
          print ("Abnormal Temperature Measurements:")
          print(abnormal_temperature)
# Step 5: Return measurement's status
          BodyTemp_status = (BodyTemp >= BodyTemp_threshold)? 'Normal': 'Abnormal'
```

4.4. Phase 2: Proposed Mobile Application (System Interfaces)

To make using our device easier, we created a phone application that allows each user to log into their account and see their heart rate in real- time. This also allows a doctor to preview the heart rates of his patients from anywhere in the world and in real time. Figure 3 shows the first interface, which is the login interface. Here, the user is allowed to either create a new account or log into an existing one simply by entering his personal information.



Hello,

Please login to your account,

Email: name@example.com

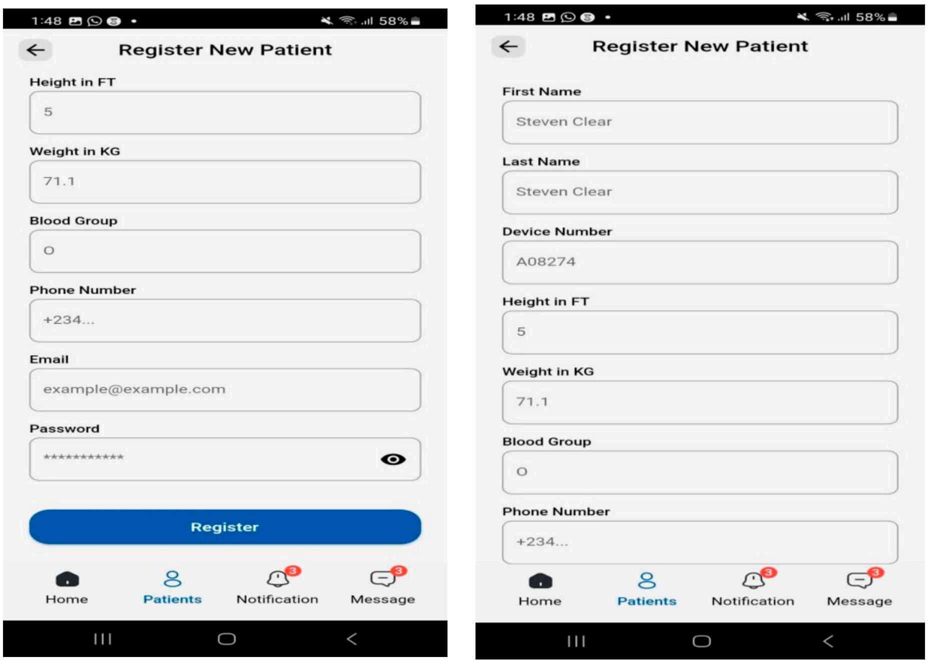
Password: ***********

Monitor your health & live Healthy

Stay up to date with your health status, with informed decisions from your doctor

Figure 3. The login interface and welcome interface to our system.

Figure 4 shows an interface that permits the user to register by inserting the totality of his personal information into the application. This information can later be accessed and modified as needed.



Register New Patient

Height in FT: 5

Weight in KG: 71.1

Blood Group: O

Phone Number: +234...

Email: example@example.com

Password: ***********

Register New Patient

First Name: Steven Clear

Last Name: Steven Clear

Device Number: A08274

Height in FT: 5

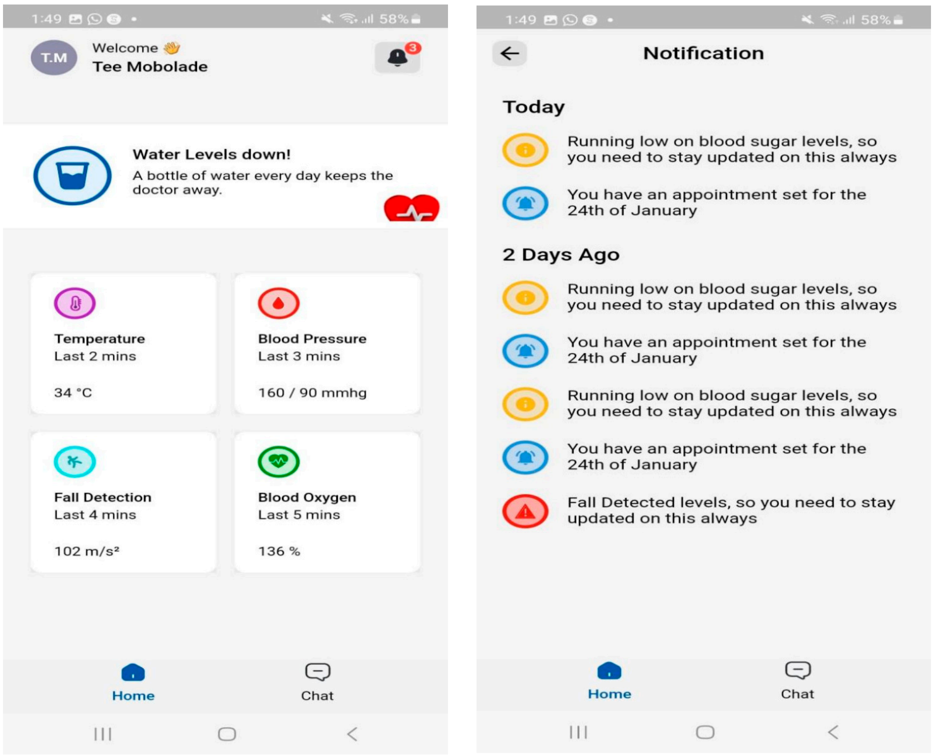
Weight in KG: 71.1

Blood Group: O

Phone Number: +234...

Figure 4. Sign-up interface.

Figure 5 shows the monitoring of the user's rates daily, and a reminder is then sent to the user in the form of notifications. The rates monitored include temperature, blood pressure, water levels, and blood oxygen.



1:49 58%

T.M

Welcome 👋

Tee Mobolade

3

Water Levels down!

A bottle of water every day keeps the doctor away.

Temperature
Last 2 mins
34 °C

Blood Pressure
Last 3 mins
160 / 90 mmhg

Fall Detection
Last 4 mins
102 m/s²

Blood Oxygen
Last 5 mins
136 %

1:49 58%

Notification

Today

Running low on blood sugar levels, so you need to stay updated on this always

You have an appointment set for the 24th of January

2 Days Ago

Running low on blood sugar levels, so you need to stay updated on this always

You have an appointment set for the 24th of January

Running low on blood sugar levels, so you need to stay updated on this always

You have an appointment set for the 24th of January

Fall Detected levels, so you need to stay updated on this always

Figure 5. Monitoring interface.

5. Result and Performance Evaluation

5.1. Phase 3: Obtaining Real-Time Results for 37 Individual Patients

The results obtained from the testing of our device have been compared with machines in real time on the basis of certain metrics to determine its functionality. These data are collected every 3 s, and the collected data are presented in Table 3 for only five patients. We applied the Gradient Boosting Classifier (GBC) algorithm to our protocol. Gradient Boosting is a machine learning ensemble method that combines a number of weak predictive models (usually decision trees) to produce a strong predictive model. This approach for supervised learning is generally employed for categorization jobs, which follow the steps of initializing the ensemble, training the base learners, building an ensemble, iteratively refining the ensemble, and making predictions. This table also provides two types of collected data to check the accuracy of the obtained data from our proposed hardware, which is indicated with “Data RTIoMT”, which shows real-time data collection, transmission, or processing of medical data using our IoT device. On the other hand, “Data with External Devices” are data collected from real devices already used in hospitals, and these medical devices are readily available in the pharmacy. Therefore, we can see that our proposed device collects accurate data. The average performance of the HCPMP protocol for these 37 volunteered patients is illustrated in Table 4.

Table 4. Average Results of HCPMP—37 Volunteered Patients.

Algorithms/Parameters	Accuracy	Precision	Recall	F1-Score
Random Forest (RF)	99.2%	99%	99%	99%
Support Vector Machines (SVM)	96.82%	100%	100%	100%
Decision Trees (DT)	100%	100%	100%	100%
Logistic Regression (LR)	97%	97%	97%	97%

5.2. Using the HealthAdvisor Dataset in the Proposed Framework

(A) Phase 4: Using the HealthAdvisor dataset [37] without attack

This set is publicly available and comprises real-time data of 630 individual patients with the values of age, gender, BMI, activity level measurement, medication, SpO2, BPM, and temperature. A total of 56% of the patients were male, and 44% were female. The age of the samples is 45–100 years old. The outcome of the experiment is shown in Table 5.

Table 5. Results of HCPMP—HealthAdvisor data-setdata set.

Algorithms/Parameters	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Random Forest (RF)	98.41%	98.52%	98.41%	98.395
Support Vector Machines (SVM)	96.82%	97%	96.82%	96.76%
Decision Trees (DT)	99.2%	99.31%	99.2%	99.21%
Logistic Regression (LR)	96.85%	97.1%	96.83%	96.77%

(B) Phase 5: Security results from various attacks

In this phase, we illustrate the results obtained under various attacks. Hence, we apply each individual attack, such as man-in-the-middle, denial of service, distributed denial of service, injection, password, and scanning, on each ML algorithm separately to obtain each ML's model accuracy, precision, recall, and F1-score after the attack. We include all the related tables, which are the outcomes of this phase, in the Supplementary Materials. Table 6 shows the comparison of the weighted average of all the attacks of our ML models.

Table 6. Comparison of a weighted average of the attacks.

ML Algorithms/Parameters	**Precision**	**Recall**	**F1-Score**
Random Forest (RF)	90.77%	91.66%	91.80%
Support Vector Machines (SVM)	89.44%	91%	90.9%
Decision Trees (DT)	89.33%	90.77%	90.7%
Logistic Regression (LR)	87.55%	91%	90%

5.3. Phase 6: Comparison of the Security Level of the Protocol with Others

In this phase of this study, we concentrated on comparing our protocol with others in the literature. The BoT-IoT data set [36] is implemented in our protocol. This data set includes DoS, DDoS, Reconnaissance, and Theft Attacks, and we compared the outcomes to some existing algorithms. The BoT-IoT dataset was developed by creating a realistic network environment at UNSW Canberra's Cyber Range Laboratory. The traffic on the network was a mix of regular and BoT-IoT types of traffic. The environment includes both regular traffic and assaults like DoS and DDoS, as well as Reconnaissance and theft attacks. There are 46 attributes in the data collection that are related to traffic characteristics. This set is recent and representative of present IoT traffic. Table 7 shows the outcome from this dataset and comparative analysis.

Table 7. Comparison with previous research—BOT-IoT.

Research/ Parameters	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Decision Time**	**No. of Features**
[38]	100%	100%	100%	100%	17.2 s	20
[39]	99.80%	-	98%	-	-	10
[40]	100%	-	-	-	11.39 s	20
[41]	96.3%	-	-	-	-	26
[42]	99.99%	-	-	-	-	19
[43]	100%	100%	100%	100%	15 s	16
HCPMP (Proposed)	**100%**	**100%**	**100%**	**100%**	**16.3 s**	**46**

Moreover, the application of formal verification and validation (FV&V) approaches can potentially address the issues of reliability and safety in IoT systems [44].

6. Discussion, Analysis, and Limitations

This section provides a concise evaluation of the performance of the four models based on the outcomes of the categorization. Table 7 presents the accuracy, precision, recall, and F1-score for each target class for all models. Also, it provides a comparison between the proposed method and existing approaches.

6.1. Discussion and Analysis

In comparison to Table 5, ref. [38] we considered an event detection-based approach by utilizing Extra Tree, Random Forest, and Deep Neural Network and achieved an accuracy of 100%. It had a precision and recall of 100%. Halim et al. [39] used GA-based Feature Selection (GbFS) in their study, which is an enhanced Genetic Algorithm (GA)-based feature selection method for Securing a network from cyber attacks, and achieved an accuracy of 99.80% and recall of 98%. The model used 10 features for classification. Rezaei A. [40] proposed new ensemble learning by adopting ANN and DT models for detecting bots and botnets in the IoT network and achieved an accuracy of 100%. Zeeshan et al. [41] proposed a new Protocol-Based Deep Intrusion Detection architecture with an accuracy of 96.3% by applying the LSTM algorithm. Nimbalkar et al. [42] proposed a system based on feature selection by adopting Information Gain (IG) and Gain Ratio (GR) methods for detecting DoS attacks by using 19 features and achieving 99.99% accuracy. Ismail M. et al. [43] present a method for feature selection in small training sample classification called enhanced recursive feature elimination (EnRFE). In terms of classification accuracy, it is 100%. Their experimental results suggest that the proposed technique outperforms the original RFE.

From another perspective of our findings and experimental methods, by using several ML techniques, the Random Forest (RF) model demonstrates outstanding performance across all categories, exhibiting high levels of precision, recall, and F1-score for the majority of classes. This model achieved a perfect accuracy rate of 100%, indicating that each forecast made was correct. Both the weighted average and macro average measures provide a 100% value, indicating a uniform level of performance across all classes. Furthermore, the performance of "INJECTION," "MITM," "PASSWORD," and "SCANNING" is noticeably worse, although their metrics remain satisfactory. Moreover, HCMP is more efficient than other protocols in terms of the decision time, which is 16.30 s for 46 features.

The support vector machine (SVM) model exhibits strong performance, demonstrating favorable precision, recall, and F1-score across the majority of classes. Similar to the Random Forest model, it achieved a 100% accuracy rate, signifying that all of its predictions were correct. Both the weighted average and macro average measures exhibit a consistent and harmonious performance, with both measures achieving a perfect score of 100%.

Though it still performs admirably, the model using DT is marginally less effective than both the RF and SVM methods. Most of the courses had good recall, accuracy, and F1-scores. Even with a few errors here and there, the accuracy rate is still remarkably good at 99% overall. The achievement of a 99% score within the weighted average and macro average metrics indicates that the student has demonstrated a complete performance in numerous classes.

For most classes, the logistical regression (LR) model performs well with good accuracy, recollection, and F1-score metrics. With an accuracy of one hundred percent rate, the model showed that it was highly reliable because all of the predictions it made came true. Given that they both produce a 100% result, the weighted average metrics show consistent performance.

Overall, the four models—Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), and Logistic Regression (LR)—perform admirably, displaying high F1-scores and accuracy levels. While support vector machine (SVM) and the random forest (RF) models offer ideal accuracy rates of 100%, the decision tree (DT) and logistic regression

(LR) models show an accuracy rate of 99%. Most classes show strong prediction accuracy concerning precision, recall, and F1-scores. It is crucial to remember that other aspects like computing performance, interoperability, and dataset size may also have an impact on the selection of the best model. However, based on the presented classification data, the SVM and RF models perform better due to their perfect accuracy and uniform metrics within all classes.

We used the same parameters as the candidate's research in Table 7, which involved the use of 20 features for classification via the method we employed to ensure a fair comparison. Based on the obtained findings, it can be inferred that our suggested model, the Hybrid Classification and Prediction Model (HCPMP), showed superior performance compared to the other strategies. Specifically, the HCPMP achieved flawless accuracy, precision, recall, and F1-score. In contrast to the preceding iterations, this particular version incorporated a greater number of features, as outlined in Table 6. When evaluating the effectiveness of these models, it is essential to consider several factors, such as the characteristics of the dataset and its real-world application.

Maintaining an ongoing process of upgrading and retraining machine learning algorithms is essential for efficiently adapting to evolving cybersecurity threats. However, it is crucial to recognize that in some medical settings, access to necessary resources and information might not always be easy. Thus, one of the most important areas of research in IoMT cybersecurity is the creation of long-term and economical strategies for preserving current machine learning algorithms.

Ultimately, developing standardized frameworks for communication, protocols, and data formats is crucial to building a trustworthy, safe, and compatible health monitoring system. The HCPMP architecture can maintain security and efficiency criteria while effectively and ethically addressing the complexities of healthcare data.

6.2. HCPMP Framework Limitations

By exploring the potential limitations during the implementation and testing of the system, we can mention security testing scenarios in Phase 5, which involve evaluating security features under different types of assaults on individual machine learning algorithms. Nevertheless, real-world situations may entail many or more sophisticated attacks, and this study's emphasis on single attacks might not accurately represent the whole security environment. Although thorough, the Phase 5 attacks (man-in-the-middle, denial of service, etc.) might not cover all possible security risks in practical situations, leaving certain vulnerabilities undiscovered. This study's focus on specific attacks may not account for emerging or evolving security threats in the rapidly changing landscape of healthcare cybersecurity.

However, it is important to recognize that selecting the best model involves more than only accuracy measurements. The size of the dataset, interoperability, and processing power are important considerations for choosing the best model. Nonetheless, when considering the provided classification outcomes, the RF and SVM models prove to be superior choices, displaying flawless accuracy and consistent metrics across all classes. These findings demonstrate the transformative potential of machine learning and data analytics in the analysis of health-related information in cloud-based environments, offering not only accurate predictions but also recommendations for practical implementation in healthcare settings.

7. Conclusions

Three key stages that comprise the framework (HCPMP) that we presented in this research are as follows: the control stage; the detection stage; and the data-capturing step. This real-time mechanism is implemented and tested in six (6) consecutive and distinguished phases for both hardware and software aspects. Extensive data were collected from multiple persons and datasets to validate the proposed system's performance. Moreover, the security comparison of HCPMP with six different methods in the literature in the same context is evaluated by applying the BoT-IoT dataset. This suggested model, which is HCPM, showed superior performance compared to the other strategies. The outcome improves healthcare results, resource allocation, secure data transmission, and patient satisfaction. As medical IoT devices grow more common, it is critical to keep researching and improving ML-based techniques in order to enhance their effectiveness in detecting and mitigating cybersecurity threats in future directions. Also, to achieve high accuracy and security of IoMT application, the heterogeneous ensemble learning method can be applied to our method in the future and be compared with a few studies that implemented this type of method.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/su16031349/s1.

Author Contributions: Validation, supervision, writing—original draft preparation, writing—review and editing, S.E.; conceptualization, methodology, software, and investigation, T.E.M.; formal analysis, S.E. and T.E.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board.

Informed Consent Statement: Informed consent was obtained from all subjects involved in this study. All involved persons gave informed consent (verbal as appropriate) before study inclusion.

Data Availability Statement: The data presented in this study are available in Supplementary Material. Also, this research utilized the HealthAdvisor dataset (https://www.kaggle.com/datasets/dhruvi2002/health-advisor?resource=download, accessed on 7 October 2023) and BOT_IoT dataset [36], which are publicly available and openly accessible. While the dataset is publicly accessible, it is important to note that the code used in our research is proprietary and cannot be shared due to confidentiality and intellectual property considerations. The code contains sensitive algorithms and proprietary methodologies that are integral to our research and cannot be disclosed at this time.

Acknowledgments: I would like to thank my supervisor, Sahar Ebadinezhad, for providing insight and expertise that greatly assisted this research.

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

References

1. Singh, A.; Chatterjee, K. Edge computing-based secure health monitoring framework for electronic healthcare system. *Clust. Comput.* **2023**, *26*, 1205–1220. [CrossRef]
2. Saif, S.; Bhattacharjee, P.; Karmakar, K.; Saha, R.; Biswas, S. IoT-Based Secure Health Care: Challenges, Requirements and Case Study. In *Internet of Things Based Smart Healthcare: Intelligent and Secure Solutions Applying Machine Learning Techniques*; Springer Nature Singapore: Singapore, 2022; pp. 327–350.
3. Awotunde, J.B.; Jimoh, R.G.; Folorunso, S.O.; Adeniyi, E.A.; Abiodun, K.M.; Banjo, O.O. Privacy and security concerns in IoT-based healthcare systems. In *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*; Springer International Publishing: Cham, Switzerland, 2021; pp. 105–134.
4. Tiwari, S.; Nahak, K.; Mishra, A. Revolutionizing Healthcare: The Power of Iot in Health Monitoring. *J. Data Acquis. Process.* **2023**, *38*, 2416.
5. Paulraj, G.J.L.; Jebadurai, I.J.; Jebadurai, J.; Samuel, N.E. Cloud-based real-time wearable health monitoring device using IoT. In *Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020*; Springer: Singapore, 2021; pp. 1081–1087.
6. Abdulmalek, S.; Nasir, A.; Jabbar, W.A.; Almuhaya MA, M.; Bairagi, A.K.; Khan, M.A.; Kee, S.H. IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. *Healthcare* **2022**, *10*, 1993. [CrossRef] [PubMed]
7. Bardach, S.H.; Real, K.; Bardach, D.R. Perspectives of healthcare practitioners: An exploration of interprofessional communication using electronic medical records. *J. Interprof. Care* **2017**, *31*, 300–306. [CrossRef] [PubMed]
8. TechJini. How IoT and Wearables can Solve Today's Healthcare Challenges. 2017. Available online: https://www.techjini.com/blog/IoT-wearables-can-solvetodays-healthcare-challenges/ (accessed on 7 October 2023).
9. Neelam, B.S.; Shimray, B.A. Applicability of RINA in IoT communication for acceptable latency and resiliency against device authentication attacks. In Proceedings of the 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2–4 April 2021; pp. 1–7. [CrossRef]

10. Yew, H.T.; Ng, M.F.; Ping, S.Z.; Chung, S.K.; Chekima, A.; Dargham, J.A. IoT Based Real-Time Remote Patient Monitoring System. In Proceedings of the 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 28–29 February 2020; pp. 176–179. [CrossRef]
11. Barnaghi, P.; Tönjes, R.; Höller, J.; Hauswirth, M.; Sheth, A.; Anantharam, P. CityPulse: Real-Time IoT Stream Processing and Large-Scale Data Analytics for Smart City Applications. 2014. Available online: http://www.ict-citypulse.eu (accessed on 7 October 2023).
12. Fujitsu. Real-Time IoT Tracking and Visualization. *IoTone.* 2016. Available online: https://www.iotone.com/case-study/real-time-iot-tracking-and-visualization-improve-manufacturing/c1040 (accessed on 7 October 2023).
13. Saha, R.; Biswas, S.; Sarmah, S.; Karmakar, S.; Das, P. A working prototype using DS18B20 temperature sensor and arduino for health monitoring. *SN Comput. Sci.* **2021**, *2*, 1–21.
14. Goel, V.; Srivastava, S.; Pandit, D.; Tripathi, D.; Goel, P. Heart Rate Monitoring System Using Finger Tip through IOT. *Int. Res. J. Eng. Technol.* **2018**, *5*, 1114–1117.
15. Abbasi, M.A.; Memon, Z.A.; Memon, J.; Syed, T.Q.; Alshboul, R. Addressing the Future Data Management Challenges in IoT: A Proposed Framework. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 197–207.
16. Akhbarifar, S.; Javadi HH, S.; Rahmani, A.M.; Hosseinzadeh, M. A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment. *Pers. Ubiquitous Comput.* **2020**, *27*, 697–713. [CrossRef] [PubMed]
17. Hassanalieragh, M.; Page, A.; Soyata, T.; Sharma, G.; Aktas, M.; Mateos, G.; Kantarci, B.; Andreescu, S. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. In Proceedings of the 2015 IEEE International Conference on Services Computing, SCC 2015, New York, NY, USA, 27 June–2 July 2015. [CrossRef]
18. Hossain, M.S.; Muhammad, G. Cloud-assisted Industrial Internet of Things (IIoT)—Enabled framework for health monitoring. *Comput. Netw.* **2016**, *101*, 192–202. [CrossRef]
19. Hu, J.X.; Chen, C.L.; Fan, C.L.; Wang, K.H. An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing. *J. Sens.* **2017**, *2017*, 3734764. [CrossRef]
20. Verma, P.; Sood, S.K. Cloud-centric IoT based disease diagnosis healthcare framework. *J. Parallel Distrib. Comput.* **2018**, *116*, 27–38. [CrossRef]
21. Ahmed, M.R.; Hasan Mahmud, S.M.; Hossin, M.A.; Jahan, H.; Haider Noori, S.R. A cloud based four-tier architecture for early detection of heart disease with machine learning algorithms. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications, ICCC 2018, Chengdu, China, 7–10 December 2018. [CrossRef]
22. Yang, Z.; Zhou, Q.; Lei, L.; Zheng, K.; Xiang, W. An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare. *J. Med. Syst.* **2016**, *40*, 286. [CrossRef] [PubMed]
23. Begum, V.; Vajubunnisa Begum, R.; Dharmarajan, D.K. Smart Healthcare Monitoring System in IoT. *Eur. J. Mol. Clin. Med.* **2020**, *7*, 2647–2661.
24. Monteiro, K.; Rocha, E.; Silva, E.; Santos, G.L.; Santos, W.; Endo, P.T. Developing an e-health system based on IoT, Fog and cloud computing. In Proceedings of the 11th IEEE/ACM International Conference on Utility and Cloud Computing Companion, UCC Companion 2018, Zurich, Switzerland, 17–20 December 2019. [CrossRef]
25. Hsu, Y.H.; Wang, J. Internet of Medical Things (IoMT) system design for data security enhancement. *Future Gener. Comput. Syst.* **2020**, *107*, 644–654. [CrossRef]
26. Raza, S.; Wallgren, L.; Voigt, T. A survey of attacks and security mechanisms in the Internet of Things. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1637–1652.
27. McQueen, R.J.; Kudva, M.S. A survey of security in Internet of Things. *J. Netw. Comput. Appl.* **2018**, *103*, 131–145. [CrossRef]
28. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the Internet of Things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012; ACM: New York, NY, USA, 2012; pp. 13–16. [CrossRef]
29. Al-Dahoud, A.; Hamida, E.B.; Alkhzaimi, H. A survey of elliptic curve cryptography. *J. King Saud Univ. Comput. Inf. Sci.* **2021**, *33*, 62–74.
30. Satoh, A.; Yamada, K.; Hoshi, T.; Yasuda, K. An implementation and performance evaluation of fast elliptic curve cryptography on Intel SGX. In Proceedings of the 14th ACM Asia Conference on Computer and Communications Security, Auckland New Zealand, 9–12 July 2019; pp. 217–228.
31. Xiao, Y.; Zhang, S.; Zhang, C.; Zhang, X. An efficient implementation of elliptic curve cryptography on FPGA. *J. Signal Process. Syst.* **2018**, *90*, 881–889.
32. Kumari, A.; Yahya Abbasi, M.; Kumar, V.; Khan, A.A. A secure user authentication protocol using elliptic 839 curve cryptography. *J. Discret. Math. Sci. Cryptogr.* **2019**, *22*, 521–530. [CrossRef]
33. Ren, Y.; Gao, W.; Wu, J.; Liu, M.; Li, J. Efficient implementation of elliptic curve cryptography on RISC-V processor. In Proceedings of the 2019 18th International Symposium on Parallel and Distributed Computing (ISPDC), Amsterdam, The Netherlands, 3–7 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 62–69.
34. Singh, G.; Kumar, A.; Kumar, N. Performance evaluation of elliptic curve cryptography on ARM Cortex-A8 processor. In Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 21–23 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 93–97.

35. Kumar, A.; Pandey, P.; Chawla, K. A scalable elliptic curve cryptography based key agreement scheme for IoT. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 3737–3752.
36. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet data-set in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796, (BOT-IOT). [CrossRef]
37. Kaggle, Data Science Company. Find Open Datasets and Machine Learning Projects. *DHRUVI2002 Updated 2 Years Ago*. Available online: https://www.kaggle.com (accessed on 7 October 2023).
38. De Souza, C.A.; Westphall, C.B.; Machado, R.B. Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments. *Comput. Electr. Eng.* **2022**, *98*, 107694. [CrossRef]
39. Halim, Z.; Yousaf, M.N.; Waqas, M.; Sulaiman, M.; Abbas, G.; Hussain, M.; Ahmad, I.; Hanif, M. An effective genetic algorithm-based feature selection method for intrusion detection systems. *Comput. Secur.* **2021**, *110*, 102448. [CrossRef]
40. Rezaei, A. Using Ensemble Learning Technique for Detecting Botnet on IoT. *SN Comput. Sci.* **2021**, *2*, 148. [CrossRef]
41. Zeeshan, M.; Riaz, Q.; Bilal, M.A.; Shahzad, M.K.; Jabeen, H.; Haider, S.A.; Rahim, A. Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets. *IEEE Access* **2022**, *10*, 2269–2283. [CrossRef]
42. Nimbalkar, P.; Kshirsagar, D. Feature selection for intrusion detection system in internet-of-things (iot). *ICT Express* **2021**, *7*, 177–181. [CrossRef]
43. Ismail, M.G.; Abd El Ghany, M.; Salem, M.A.M. Enhanced Recursive Feature Elimination for IoT Intrusion Detection Systems. In Proceedings of the 2022 International Conference on Microelectronics (ICM), Casablanca, Morocco, 4–7 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 193–196.
44. Krichen, M. A Survey on Formal Verification and Validation Techniques for Internet of Things. *Appl. Sci.* **2022**, *13*, 8122. [CrossRef]

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.