electronics

MDPI

Article

Machine-Learning-Based IoT–Edge Computing Healthcare Solutions

Abdulrahman K. Alnaim [1,*] and Ahmed M. Alwakeel [2,3]

[1] Department of Management Information Systems, School of Business, King Faisal University, Al Ahsa 31982, Saudi Arabia
[2] Faculty of Computers & Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[3] Sensor Network and Cellular Systems Research Center, University of Tabuk, Tabuk 71491, Saudi Arabia
* Correspondence: aalnaim@kfu.edu.sa

Abstract: The data that medical sensors collect can be overwhelming, making it challenging to glean the most relevant insights. An algorithm for a body sensor network is needed for the purpose of spotting outliers in the collected data. Methods of machine learning and statistical sampling can be used in the research process. Real-time response optimization is a growing field, as more and more computationally intensive tasks are offloaded to the backend. Optimizing data transfers is a topic of study. Computing power is dispersed across many domains. Computation will become a network bottleneck as more and more devices gain Internet-of-Things capabilities. It is crucial to employ both task-level parallelism and distributed computing. To avoid running down the battery, the typical solution is to send the processing to a server in the background. The widespread deployment of Internet-of-Things (IoT) devices has raised serious privacy and security concerns among people everywhere. The rapid expansion of cyber threats has rendered our current privacy and security measures inadequate. Machine learning (ML) methods are gaining popularity because of the reliability of the results that they produce, which can be used to anticipate and detect vulnerabilities in Internet-of-Things-based systems. Network response times are improved by edge computing, which also increases decentralization and security. Edge nodes, which frequently communicate with the cloud, can now handle a sizable portion of mission-critical computation. Real-time, highly efficient solutions are possible with the help of this technology. To this end, we use a distributed-edge-computing-based Internet-of-Things (IoT) framework to investigate how cloud and edge computing can be combined with ML. IoT devices with sensor frameworks can collect massive amounts of data for subsequent analysis. The front-end component can benefit from some forethought in determining what information is most crucial. To accomplish this, an IoT server in the background can offer advice and direction. The idea is to use machine learning in the backend servers to find data signatures of interest. We intend to use the following ideas in the medical field as a case study. Using a distributed-edge-computing-based Internet-of-Things (IoT) framework, we are investigating how to combine the strengths of both cloud and edge computing with those of machine learning.

Keywords: ML; edge computing; IoT; cloud computing

Citation: Alnaim, A.K.; Alwakeel, A.M. Machine-Learning-Based IoT–Edge Computing Healthcare Solutions. *Electronics* **2023**, *12*, 1027. https://doi.org/10.3390/electronics12041027

Academic Editors: Samaneh Madanian, Julie Dugdale and Mahyar T. Moghaddam

Received: 17 December 2022
Revised: 11 February 2023
Accepted: 15 February 2023
Published: 18 February 2023

1. Introduction

The term “Internet of Things” (IoT) refers to a network infrastructure in which disparate computing devices can communicate with one another, facilitating the collection and exchange of data without requiring human intervention. IoT is a relatively new field of study that promises to usher in a plethora of technological advances. Many fields have benefited greatly from the innovations made possible by this technology. The Internet of Medical Things (IoMT) is a growing subset of IoT that has found widespread use in the healthcare industry [1–5].

Implanted medical devices (IMDs) and wearable devices are two examples of the kinds of IoT applications that can be used in a healthcare system based on the Internet of Things to help doctors and patients receive the best possible care. There are clear advantages to remote patient monitoring, as shown by studies. Through the use of this technology, non-critical patients can be monitored remotely, relieving stress on medical personnel and hospital resources [6–9].

Such a system enables the medical team to keep tabs on the health of their patients no matter where they happen to be located and allows elderly patients the freedom to remain in the comfort of their own homes while still receiving the care they need. Medication plans, such as those for rehabilitation, diabetes management, and ambient assisted living (AAL), have benefited from the incorporation of IoMT technology in numerous works [2]. In cases involving patients with physical injuries, a system has been developed to determine the most effective medication regimen. By comparing the patient's case to those already in the system's database, the system is able to determine the most effective rehabilitation strategy and necessary medications. In 87.9% of cases where doctors accepted the generated plan, the system was highly effective. The treatment of Parkinson's disease is another medical area where IoMT technology has been put to use. Incorporating vision-based technology into medical wearable devices would allow for continuous monitoring of the patient's physical state, as well as for the identification of security attacks, such as DDoS attacks [9–14].

The obesity-related disease diabetes has been analyzed elsewhere. Two blood glucose measurements are needed in this system: one is a fluctuating blood sugar level, and the other is an inaccurate reading. The system takes these two measurements as inputs and decides whether to notify the patient directly, the medical staff, or the patient's loved ones. Preemptive heart attack detection is another area where the IoMT has found usefulness. An electrocardiography (ECG) sensor is used to monitor the heart's electrical activity. This information is then sent to the patient's mobile device via a microcontroller for further analysis. Many people's lives could be spared with the help of this system by allowing doctors to intervene before a heart attack even occurs [15–19].

For at-home care of the elderly, a system called SPHERE has been proposed. By utilizing this system, the elderly are able to remain in the comfort of their own homes, rather than making frequent trips to the hospital, or even having to stay there. However, protecting patients' personal information has emerged as a major concern. With patients' medical records being transmitted over wireless channels and stored in a database, there is a greater potential for security breaches. A patient's privacy and safety could be at risk if they were to use a piece of technology incorrectly. One of the primary goals of modern healthcare IT, therefore, is to guarantee the safety of remote patient monitoring and emergency response.

The main contributions of this study are as follows:

- The design of edge-based computing to collect patients' data.
- To secure the communication between edge nodes and secure the patient data.
- The application of a new hybrid model to predict and mitigate cyberattacks in a medical healthcare system consisting of IoT and edge nodes.
- Development of new machine learning algorithms specifically tailored for use on edge devices with limited resources.
- Investigation of privacy and security concerns surrounding the collection and transmission of personal health data.
- Studies on the effectiveness of IoT–edge-computing-based solutions for improving patient outcomes and reducing healthcare costs.
- The possibility of new IoT devices and sensors for use in healthcare applications.
- Integration of IoT–edge computing with other technologies, such as 5G networks, to improve data transmission and processing capabilities.
- Comparison of different edge computing architectures (fog computing, cloudlets, etc.) and their suitability for healthcare applications.
- Investigating the scalability and reliability of IoT–edge-computing-based solutions for healthcare applications
- Development of models for data fusion and data analytics for healthcare applications.

2. Related Work

The field of IoT–edge-computing-based healthcare solutions is relatively new, but it has been growing rapidly in recent years. The key drivers behind this growth include the increasing availability of low-cost IoT devices, advancements in machine learning and edge computing technologies, and the need for more cost-effective and efficient healthcare delivery [20–24].

One of the earliest research topics in this area focused on the use of wireless sensor networks (WSNs) for remote monitoring of patients with chronic conditions, such as diabetes and heart disease. These studies demonstrated the feasibility of using WSNs to collect and transmit patient data, but they also highlighted the need for more advanced data processing and analysis capabilities at the edge [25–28].

More recent research has focused on the development of new machine learning algorithms specifically tailored for use on edge devices, as well as the integration of edge computing with other technologies, such as 5G networks. There have also been a number of studies investigating the privacy and security concerns associated with the collection and transmission of personal health data.

Research has also been carried out on the effectiveness of IoT–edge-computing-based solutions for improving patient outcomes and reducing healthcare costs. These studies have shown that these solutions can lead to improved patient outcomes and reduced healthcare costs.

In addition, there has been a growing interest in developing new IoT devices and sensors for use in healthcare applications, as well as the exploration of different edge computing architectures (fog computing, cloudlets, etc.) and their suitability for healthcare applications.

Overall, the research background on IoT–edge-computing-based healthcare solutions is still developing, and there are a lot of areas to be explored.

Edge computing is a rapidly expanding trend in the computing industry. In numerous traditional applications, distributed cloud computing is used at the edge to complete tasks. The system is more complicated than cloud computing because of constraints on resources, transmission efficiency, functionality, and other edge-network-based considerations. When edge devices work together, an inherently unstable state emerges. In this research area, Raj et al. [29] presented a novel framework for optimizing cooperative networks at the network's periphery. In addition, the collaboration of edge nodes can be optimized to boost performance on specific activities. In order to demonstrate the efficacy of the proposed architecture, real datasets collected from the elderly and their wearable sensors are employed. Extensive experimentation is also helpful in verifying the effectiveness of the given optimization algorithm.

Using deep learning to sift through massive amounts of raw sensor data from IoT devices in real-world settings holds great promise. Deep learning is well suited for application at the edge of the network because of its modular design. Conventional models of edge computing are inflexible. IoT–edge computing benefits from a more adaptable architectural design. The proposed approach integrates many agents and a versatile edge computing architecture for deep learning at the edge. Due to the low processing power of current edge nodes, researchers [30] have also developed a unique offloading approach to boost the efficiency of deep learning applications deployed on the edge. Flexible and advanced, the FEC architecture is a concept for Internet-of-Things systems that can adapt to different settings and focus on the needs of individual users. The performance of deep learning tasks executed in the FEC architecture for edge computing environments was evaluated. Analyses of the data demonstrate that, compared to other optimization strategies for deep learning for IoT, our strategy is the most effective.

Emerging ICT technologies such as wearables, the Internet of Things, and edge computing are rapidly transforming healthcare into digital health. Consumer gadgets such as smart, wearable fitness watches are also becoming increasingly popular as a means of tracking one's health and fitness. Despite these developments, the healthcare system has not yet made full use of these devices' potential to capture longitudinal behavioral patterns. User-generated data from such devices could form part of a more comprehensive and preventative healthcare solution if they could be collected without compromising an individual's privacy. A previous paper [31] proposed an edge-assisted data analytics framework that makes use of federated learning to retrain local machine learning models with user-generated data. This approach has the potential to utilize pretrained models to derive user-specific insights without compromising confidentiality or cloud infrastructure. We also highlight research issues that might be investigated further within the proposed framework, and indicate some possible application scenarios.

For effective and equitable resource allocation, such as electricity and battery life, in IoT-based industrial applications, edge computing has surpassed cloud computing. This is due to several factors, including the former's processing complexity and the latter's additional latency. Meanwhile, the use of AI for efficient and precise resource management has gained widespread attention, particularly in industrial settings. Coordination of AI at the edge will significantly increase the range and processing speed of IoT-based devices in industrial settings. However, inappropriate and inefficient conventional trends of fair resource allotment pose a significant challenge in the context of these power-hungry, short-battery-life, delay-intolerant portable gadgets. In addition, large-scale industrial datasets suggest that conventional methods of extending the battery's life and reducing power consumption—such as predictive transmission power control (PTPC) and Baseline—are insufficient for supporting a dynamic wireless channel. To address this issue, [32] presented a forward central dynamic and availability approach (FCDAA) by adjusting the cycle time of sensing and transmission operations in mobile devices based on the Internet of Things. IoT energy dissipation was evaluated using a system-level battery model and data reliability model for edge AI-based IoT devices in a hybrid TPC/duty-cycle network. To provide effective monitoring of industrial platforms, two major scenarios were introduced: static (i.e., product processing) and dynamic (i.e., vibration and defect diagnostics). By experimentally tweaking the duty cycle and TPC, the suggested FCDAA improves energy efficiency and battery longevity, with acceptable reliability (0.95).

Cognitive computing, artificial intelligence, pattern recognition, chatbots, wearables, and edge-distributed ledgers can all help collect and interpret medical data for decision-making in the present epidemic. Cognitive computing is especially useful in the medical field because it can quickly analyze large datasets and provide highly personalized, insightful recommendations to aid in the diagnosis of disease. However, the world is currently experiencing a pandemic of COVID-19, and early identification is crucial to lowering the fatality rate. Radiologists can benefit from deep learning (DL) models while looking over huge datasets of chest X-rays. However, they need a massive quantity of training data, which must be stored in a single location. So, for DL-based COVID-19 detection, the FL approach may be utilized to construct a shared model without relying on local data. In their study, Lydia et al. [33] demonstrated a federated-deep-learning-based COVID-19 (FDL-COVID) detection model running on an IoT-enabled edge computing platform. First, data from the patient are collected by the IoT devices, and then a DL model is developed with the help of the SqueezeNet model. Using the SqueezeNet model, the cloud server receives the encrypted variables from the IoT devices and conducts FL on the important variables to generate a global cloud model. Moreover, the hyperparameters of the SqueezeNet architecture are properly tuned using the glowworm swarm optimization technique. Results from a variety of studies performed on the benchmark CXR dataset were evaluated on a number of different metrics. The experimental results demonstrated that the FDL-COVID method outperformed the others.

Patients today want a healthcare system that is as fast-paced and individualized as their lives require. Real-time gathering and analysis of health data requires a low-latency, low-energy environment that may be achieved with the help of 5G speeds and cutting-edge computing methods. Prior healthcare research has mostly concentrated on novel fog architecture and sensor types, ignoring the need for optimal computing techniques such as encryption, authentication, and classification employed on the devices deployed in an edge computing architecture. The primary objective of [2] was to provide a comprehensive overview of the state-of-the-art and cutting-edge edge computing architectures and methodologies for healthcare applications, as well as to outline the specific needs and difficulties associated with devices for diverse use cases. Most edge computing use cases revolve around health data categorization, such as heart rate and motion sensor monitoring, or fall detection. Disease-specific symptom monitoring is performed by other low-latency applications, such as for gait problems in Parkinson's disease patients. The authors also provide a comprehensive analysis of data operations in edge computing, including topics such as data transfer, encryption, authentication, categorization, reduction, and prediction. Despite these benefits, edge computing has its own unique set of difficulties, such as the need for advanced privacy and data reduction techniques to achieve the same level of performance as cloud-based alternatives while reducing the computational complexity. Researchers have found potential new areas of study in edge computing for healthcare that might improve patients' lives.

Data synchronization prior to cutover and migration is a significant barrier for modern cloud-based architecture. The requirement for a centralized IoT-based system has been hindered by the cloud's limited scalability with regard to security issues. The fundamental reason for this is that health-related systems such as health monitoring, etc., demand computational operations on high-volume data, along with the sensitivity of device delay that has evolved during these systems' operation. Fog computing is a novel approach to enhancing cloud computing's efficiency, since it allows for the utilization of both remote and onsite resources to best serve customers [34]. There are still several shortcomings in the current fog computing models that need to be addressed. For example, it is possible to manage result accuracy and overestimate reaction time separately, but doing so simultaneously reduces system compatibility. In order to improve real-world healthcare systems, such as those dealing with heart disease and other conditions, a new framework called FETCH has been created. This framework collaborates with edge computing devices to work on deep learning technology and automated monitoring. The suggested fog-enabled cloud computing system makes use of FogBus, which exhibits its value in terms of power consumption, network bandwidth, jitter, latency, process execution time, and the correctness of its results.

Though they are not necessarily connected, cloud computing and the IoT both play important roles in our daily lives. The combination of these two technologies has the potential to improve several areas, including medicine, security, assisted living, farming, and asset monitoring. However, due to network latency issues, cloud computing is not a good fit for applications that need instantaneous replies. As a result, a new method called "edge computing" was developed to move processing to the "edge of the network", where it may experience lower latency. Real-time answers, battery power, bandwidth costs, and data security and privacy are only some of the issues that may be addressed by edge computing. This paper focuses on how edge computing and IoT may be used in the medical industry. Kumar et al. [35] focused on the potential for incorporating cloud/edge computing and machine learning paradigms into a distributed-computing-based IoT framework. The goal is to be able to sift through the massive amounts of data produced by the front-end sensor frameworks in IoT devices and find the specific pieces of information that are relevant. Front-end modules can be made smarter so that they can prioritize data on their own. A backend IoT server can offer advice on how to do this. The proposal is for the backend server to include machine-learning-based implementations so that it can automatically learn data signatures of interest from the data it has already received.

Smart healthcare services that are timely, inexpensive, and effective are in high demand because of the rise in both technology and population. Intelligent approaches to overcoming the challenges in this area are required to keep up with the rising demands placed on this vital infrastructure. This is because, unlike conventional cloud- and IoT-based healthcare systems, edge computing technology may move processes closer to the data sources, thereby reducing latency and energy usage. In addition, AI's ability to automate insights in smart healthcare systems raises the prospect of earlier detection and prediction of high-risk diseases, together with reduced patient healthcare expenditures and improved treatment efficacy. The authors of [36] aimed to discuss the advantages of using AI and other forms of edge intelligence in smart healthcare systems. On top of that, the authors proposed a new smart healthcare paradigm to increase the use of AI and edge technology in healthcare IT. The report also addresses problems and potential future research avenues brought up by the combination of these technologies. Table 1 shows the comparative analysis of previous state-of-the-art studies:

Table 1. Comparative analysis.

References	Datasets	Techniques	Outcome
[29]	Real datasets obtained from elderly people and their wearable sensors	Edge cooperative network is optimized with a novel framework	Optimization framework is developed for ECN
[30]		Combines deep learning into edge computing and flexible edge computing	Outperforms other optimization solutions on deep learning for IoT
[32]	Large-scale industrial datasets	Forward central dynamic and available approach, data reliability model for edge artificial intelligence	FCDAA enhances energy efficiency and battery lifetime at acceptable reliability (~0.95) by appropriately tuning the duty cycle
[33]	Federated-deep-learning-based COVID-19 dataset	Federated-deep-learning-based COVID-19 (FDL-COVID) detection model	Enhanced performance of the FDL-COVID technique
[2]	Edge nodes dataset	Current and emerging edge computing architectures and techniques	Comparable performance to cloud-based counterparts
[34]	Edge nodes dataset	FETCH is a proposed framework	Complex deep learning model to set edge computing standards
[35]	Edge nodes dataset	Edge computing	The endpoint IoT device; such a solution can also pull data from the cloud and handle any offloading that needs to be performed
[36]	Edge nodes dataset	Edge technology along with AI techniques	Smart healthcare systems benefit from edge technology since it lessens the system's reliance on the network and its energy usage

3. Materials and Methods

Safe AI-based edge-distributed ledger assistance in the healthcare system is depicted in Figure 1 below. In addition to the user, wireless network, edge-distributed ledger, trusted agent, and healthcare server, an expert system is also part of the system. It is possible that users have been cured of a disease or are infected with a different one. In order to monitor the patient's health, they use a number of implanted and external sensors. Smartphones and other personal digital assistant (PDA) devices can also be used to collect and store medical data from sensors. An individual can use a personal digital assistant (PDA) to record their medical history, which can then be encrypted and uploaded on a regular basis as a block to the edge-distributed ledger. The data, timestamp, and other details from the preceding block are included in each link here.

Permitted agents come in two varieties: those that validate, and those that record. A subset of nodes, known as validating agents, ensures that each and every transaction is legitimate (VA). For a transaction to be included in the edge-distributed ledger, it must have been verified by the network's validators. After verification, recording agents save the data in blocks that can only be accessed by authorized users.

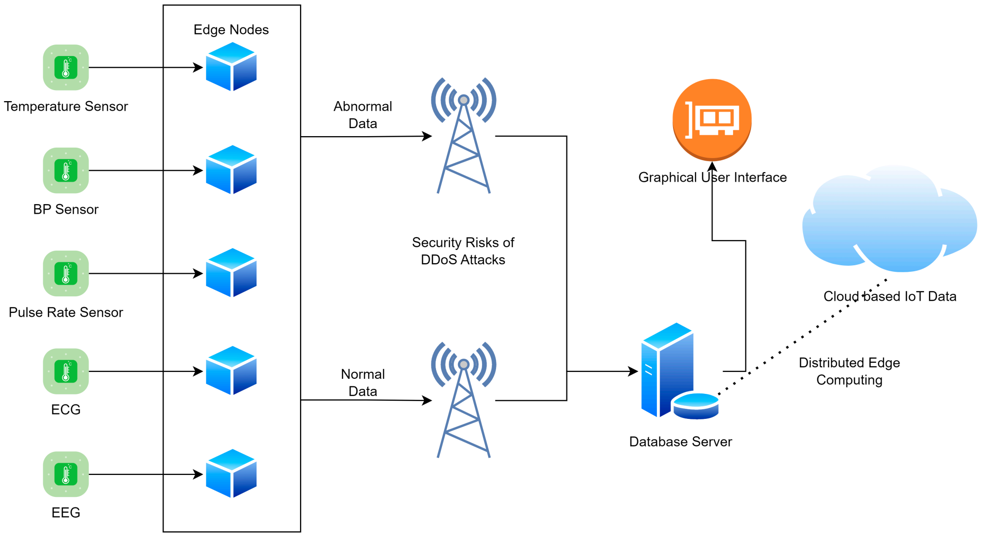

Figure 1. Proposed architecture.

The network includes separate ledgers kept by the medical staff, the hospital, and the diagnostic expert system. A diagnostic expert system can be relied upon to make accurate and informed decisions, just like a human specialist. Prior to the advent of the encrypted edge-distributed ledger, data analysis was used to detect various diseases. With the help of sensors implanted in the patient's body, life-saving medications can be administered remotely. A schematic depicting the essence of our proposed model is presented in Figure 1.

3.1. Medical Healthcare System

There is a dearth of hospitals, medical supplies, and qualified medical professionals. Lack of universal access to accurate medical diagnosis has resulted in the premature deaths of many citizens. The proposed paradigm allows for the monitoring and diagnosis of large numbers of people at once, which may prove useful in addressing such a widespread crisis. Healthcare facilities and patients can share data using this system. Patients' medical records are managed on the edge-distributed ledger via a distributed database. Data authenticity, confidentiality, and integrity are all protected by the public-key cryptosystem. Based on the patient's past medical records, AI recommends a specialist, disease category, and medication. Figure 2 shows the edge-based medical healthcare system.

3.2. Security and Privacy Preservation

The proposed approach uses an identity-based cryptosystem based on the elliptic-curve cryptosystem in order to protect patient information. The IBC does not need to verify the recipient's public key. By comparison, ECC arithmetic is approximately 20 times more efficient than modular exponentiation. According to RSA's bit-length comparison, a 1024-bit RSA key is just as secure as a 128-bit ECC key. The unique characteristics of IBC and ECC can be used to benefit IoT applications in a variety of different ways.

3.3. Proposed Edge-Node-Based Healthcare IoT System

Edge node communication can be classified into two types—in vivo and in vitro—depending on the location of the radio signal. Individuals in the body domain network can be identified using a new in vivo communication approach called body-coupled communication. Because most edge node devices are worn on the person, we are referring to low-power, short-range communication. This might be an example of "external communication". Figure 3 shows the proposed edge node sensors–IoT-based system.

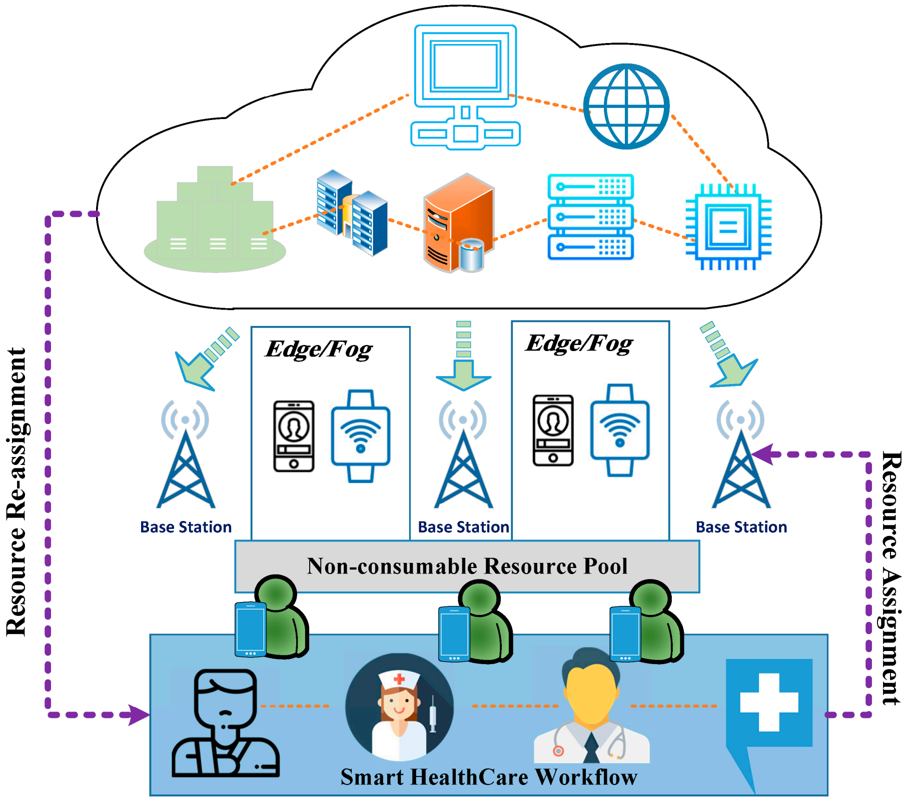

Figure 2. Edge-based medical healthcare system.

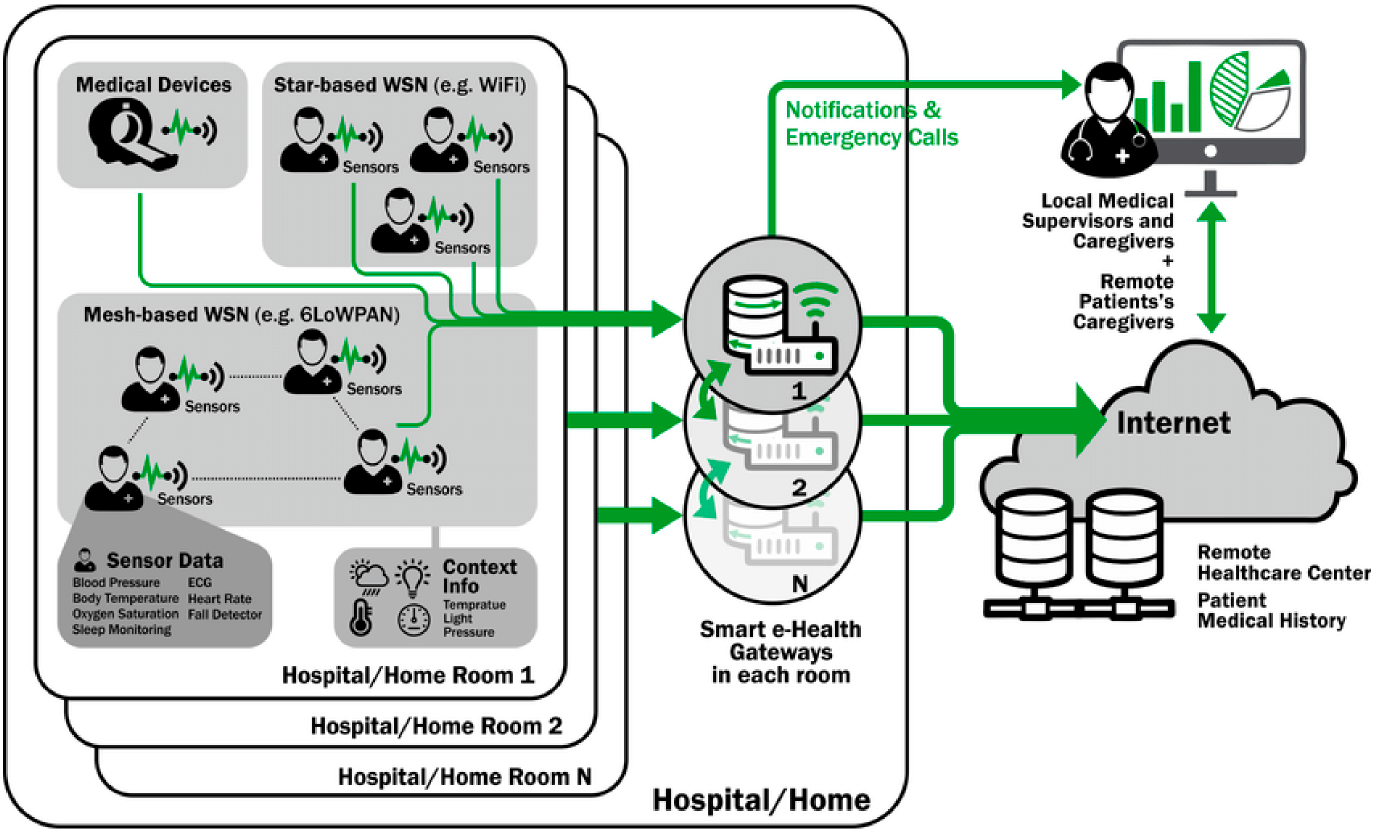

Figure 3. Proposed edge node sensors–IoT-based system.

3.4. Proposed Edge-Distributed Ledger Model

P2P networks are responsible for ensuring that communication between nodes on an edge-distributed ledger is unlimited. This is necessary given that nodes can be located anywhere in the world and still have equal access to the application. P2P networks are also responsible for ensuring that communication between nodes on an edge-distributed ledger is unlimited. The peer-to-peer network does not use a centralized server; thus, every node is both a user and a creator of content at the same time. Establishing and maintaining connections with other nodes is a necessary step in the routing process, as is propagating and validating transactions and syncing data blocks. There are numerous nodes in a network (both transactions and blocks are data structures of the edge-distributed ledger, as described below). This demonstrates the lack of a central authority and the flat topology that characterizes P2P networks. APIs (application programming interfaces) are available in a lot of edge-distributed ledger apps. These application programming interfaces (APIs) make it possible for customers to communicate directly with the service without respect to the underlying technology.

3.5. Public Edge-Distributed Ledger Technology

We have made use of the technology that allows anyone to join a public edge-distributed ledger network at any time, and we have found that it is extremely useful. As a general rule, participation is available to anybody and everybody. As a consequence of this, everyone will be able to view the ledger and take part in the process of developing the consensus. One example of a public edge-distributed ledger network that springs to mind is Ethereum. Since the public edge-distributed ledger is available to anybody and everybody, there is no one organization that can claim to have complete control over its development. The ability for new users to join a distributed ledger at any moment is what determines whether or not the ledger is considered to be public. It is possible for users of a public edge-distributed ledger to have equal access to and involvement in the data of the ledger, as well as the ability to create new blocks of data. For the most part, public edge-distributed ledgers have been utilized for the trading of cryptocurrencies, as well as for the mining of those currencies. The public edge-distributed ledger strategy can serve to alleviate some of the challenges associated with data tempering that are present in cloud-based data storage. This can be accomplished by centralizing data storage within an edge-distributed ledger. Figure 4 shows the proposed P2P communications.

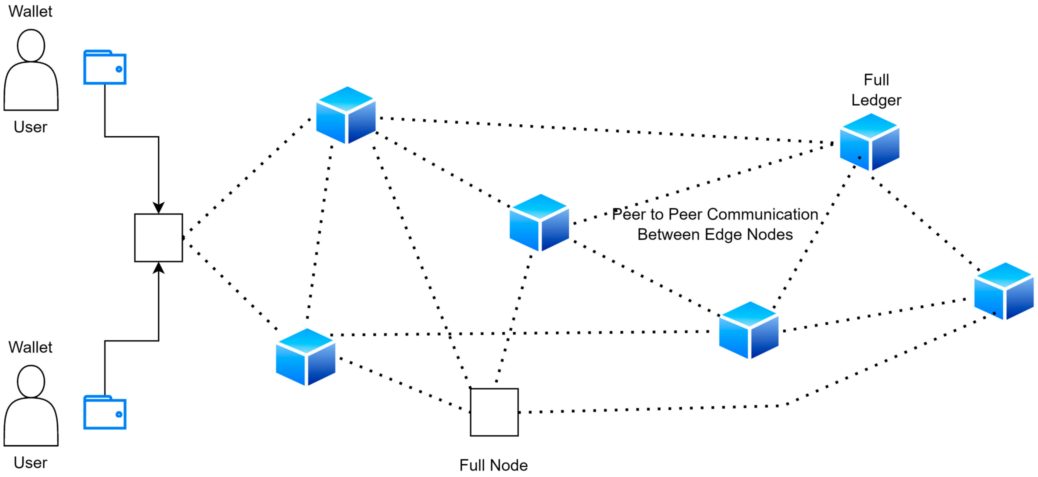

Figure 4. Proposed P2P communications.

3.6. Cloud-Based Edge-Distributed Ledger

The protection of their data is mostly the responsibility of many businesses' central databases. On the other hand, hackers are receiving a growing amount of attention. One of the most common strategies utilized by cybercriminals to gain access to large amounts of data is to launch a script assault on a central database. However, distributed ledger technologies and edge-distributed ledgers offer an additional layer of complexity. A significant number of edge-distributed ledger research projects have the objective of enhancing the safety of data storage. It is possible that this will be a game-changer for the end user. It is feasible that edge-distributed ledgers will lead to data storage solutions that are more secure, but that also give people unrestricted access to their own data. Applications on the cutting edge of the distributed ledger space frequently make use of the first cryptocurrency. Users are able to make money from the data of third parties, which can help them avoid identity theft and other problems caused by recent large-scale data breaches. Digital signatures offer two benefits to the transactions that take place on edge-distributed ledgers: message integrity, and non-repudiation. A system for storing data in the cloud that uses a distributed ledger at the edge is best suited for use with lesser amounts of data. After that, an additional layer of security is dispatched throughout the network. This is made feasible by the use of a hash algorithm, encryption using public and private keys, and transaction logs. The storage of distributed ledgers at the edge has the potential to be an alternative to cloud storage that is less expensive, more secure, and more dependable. In order to guarantee the safety of the data, suppliers of centralized cloud storage create multiple copies of the information and store them in a wide variety of data centers. In previous research, the use of cloud storage presented a significant challenge due to the ease with which data might be altered. In contrast, we made use of centralized cloud storage for this analysis. Cloud storage firms ensure the safety of customers' information by making numerous backup copies of it and storing them in a wide variety of data centers.

3.7. Privacy Preservation Strategy

RSA, Blowfish, and the Advanced Encryption Standard are the three primary algorithms that are used in cryptography. In this study, we present a hybrid method for protecting privacy that is composed of all three of these algorithms. In order to protect sensitive information, edge node networks (EDGE NODEs) make use of a number of different encryption algorithms. However, the development of more advanced and cutting-edge technologies is rendering these previously utilized methods outdated. The amount of time needed to gain access to a cryptographic system has been drastically cut down thanks to advancements in hardware. The present systems have been weakened as a result of a variety of attacks.

These systems are now significantly more susceptible to being cracked by cryptographers as a result of cryptanalysis and other specialized mathematical attacks. Another risk that modern systems are exposed to is one related to key security. Existing solutions suffer from significant shortcomings in terms of both the storage and transfer of sensitive keys. Another essential part of protecting sensitive data is making certain that their functioning is not hindered in any way. Encryption algorithms typically use longer key lengths in order to provide higher degrees of security; however, this might negatively impact the performance of the system.

A standalone cryptosystem with a single layer of encryption can occasionally have trade-offs that could result in data leakage and also reduce the level of key protection. A system that operates in isolation is susceptible to a variety of weaknesses, which can frequently compromise the data's safety. Sometimes, the performance and speed of independent systems are compromised because of the many problems that can arise from using them. As a result, there is an ever-increasing demand for a system that can circumvent the performance-versus-security trade-offs that are inherent to the usage of cryptographic algorithms individually.

There are several examples of real-world applications of IoT–edge-computing-based healthcare solutions:

Remote monitoring of patients with chronic conditions: Wearable devices such as smartwatches and fitness trackers can be used to collect data on a patient's vital signs, such as heart rate, blood pressure, and activity level. These data are sent to an edge computing device for real-time analysis, which can be used to identify patterns or anomalies that could indicate a change in the patient's condition.

Real-time drug dosing: Edge computing devices with machine learning capabilities can be used to adjust the dosage of drugs in real time based on the patient's vital signs. This can help to prevent drug overdose and improve patient outcomes.

In-home care: IoT-enabled devices such as cameras and sensors can be used to monitor patients in their homes, allowing healthcare providers to check in on them remotely.

Operating rooms: IoT-enabled devices can monitor patients' vital signs during surgery, and edge computing devices can analyze the data in real time to alert the surgical team to any changes in the patient's condition.

Assisted-living facilities: IoT sensors can monitor the movement of elderly patients in assisted-living facilities and alert staff if there is a fall or other emergency.

In general, IoT–edge-computing-based healthcare solutions have the potential to improve patient outcomes and reduce healthcare costs by enabling real-time monitoring and analysis of vital signs, providing more accurate and timely interventions, and allowing patients to be monitored remotely.

4. Results

We were particularly concerned about the amount of power that would be needed for the calculation of messages and their transmission across edge node networks as a result of the utilization of distributed ledgers at the edge to safeguard patient data. In order to guarantee the system's safety, we relied on models based on machine learning to fulfil the requirement of early detection.

4.1. Communication vs. Security Level in Edge Nodes

Signcryption adds a large amount of communication overhead. The transmission overhead is primarily determined by the signed message's size. In a traditional EDGE NODE, each user simply needs two bytes. Figure 5 depicts the cost of communication and the level of security. As the level of security increases, so does the amount of communication required.

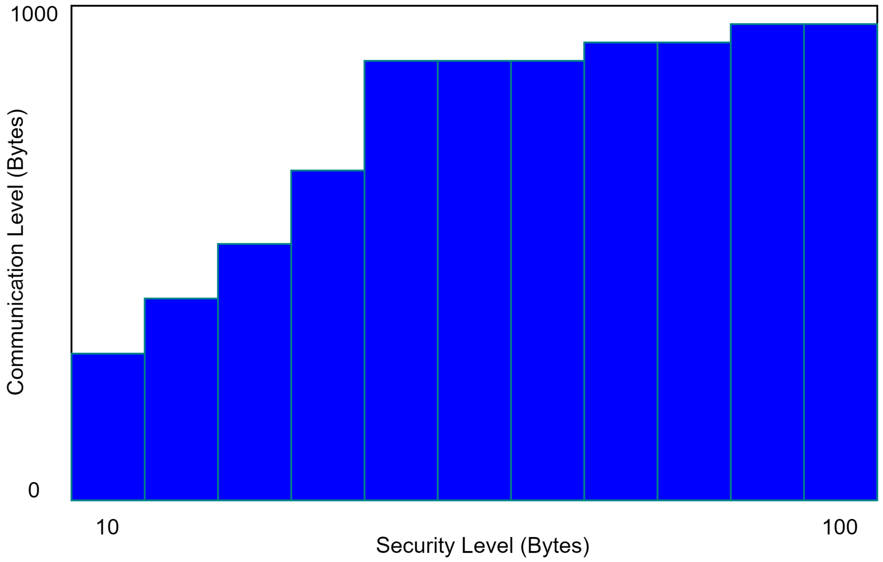

Figure 5. Performance of the proposed system in communication.

4.2. Edge-Distributed Ledger Performance

In this subsection, we tested the planned EDGE NODE platform with its distributed ledger activated to ensure its performance. One ordered node and four peer nodes were used to test the edge-distributed ledger network's efficiency. It was determined how many data could be sent per second (TPS) using the proposed EDGE NODE technology after experimenting with different send rates. There are many ways in which throughput can be broken down. A consensus was reached on the definition of transaction throughput as the sum of all edge-distributed ledger transactions processed in the time allotted. The amount of reading performed by nodes on the periphery of the distributed ledger networks was counted using readthrough during the specified time period. Transaction-read throughput variations were calculated using different TPS transmission and random machine utilization settings. Figure 5 depicts the entire transaction being read, and Figure 6 depicts the same thing being done. In Figure 7, we can see the total number of committed blocks from concurrent transactions. Figure 8 displays the average throughput of the proposed edge-distributed ledger per parallel transaction.

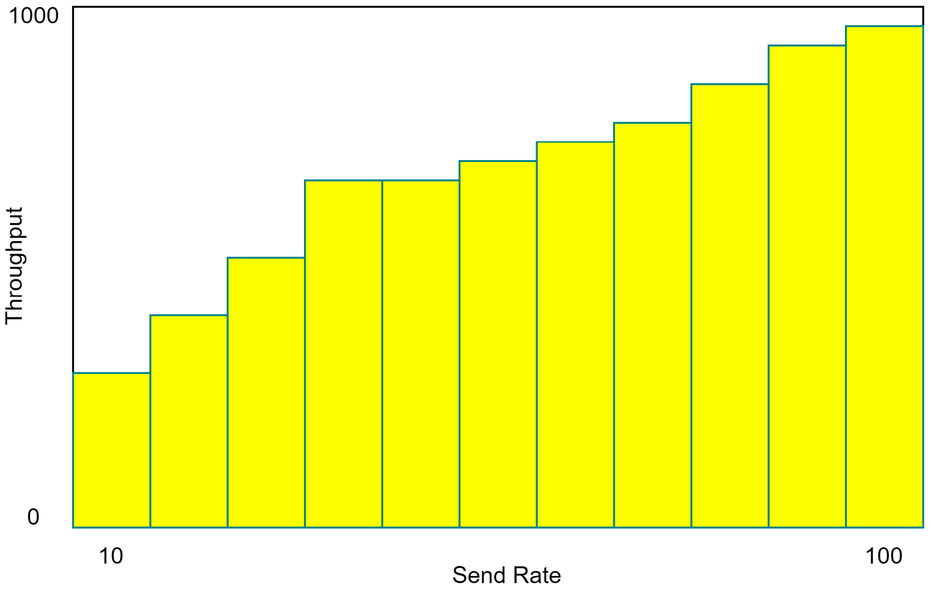

Figure 6. Read transaction throughput.

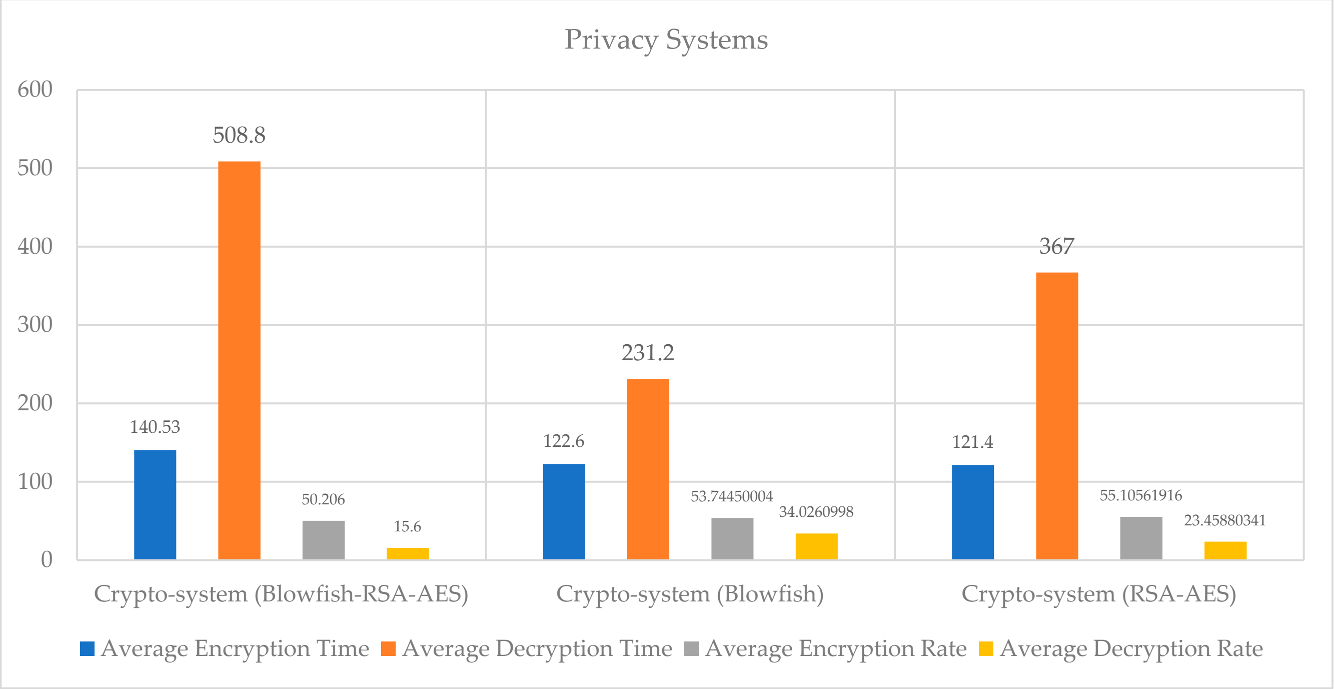

Figure 7. Performance analysis of the privacy preservation strategy.

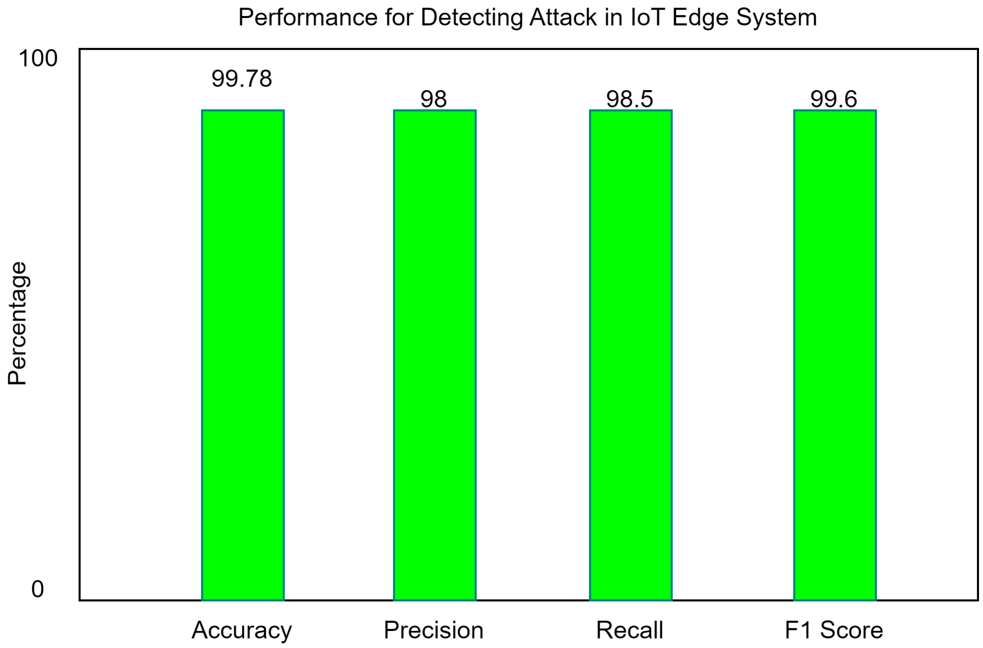

Figure 8. Hybrid classification model performance.

4.3. Privacy Preservation

In this research, we have proposed a hybrid algorithm for privacy preservation consisting of three main cryptography algorithms, i.e., the Advanced Encryption Standard, Blowfish, and RSA. Various encryption algorithms are used in edge node networks (EDGE NODEs) to secure data. However, the advent of new and sophisticated technologies is making these existing systems obsolete. Advancements in hardware have significantly reduced the time required to break a cryptographic system. Various kinds of attacks have weakened the existing systems. Figure 7 shows the results and performance analysis of the privacy preservation strategy.

4.4. Prediction of DDoS Attacks

We collected transaction data and trained a machine learning model to identify attacks on the edge-node-based edge-distributed ledger's privacy preservation solution for healthcare.

Hybrid Machine Learning Model

Estimators in the field of machine learning known as hybrid voting classifiers combine the outputs of several different base estimators into a single prediction [14–27]. The aggregated score can be decided by a simple majority of the estimators. By combining several different classification models into one, the hybrid voting classifier estimator is able to overcome the limitations of its individual components. Using weights assigned to each class or class likelihood, a hybrid voting classifier can label records with the majority vote. The ensemble classifier forecast is expressed mathematically as follows:

$$y = \left[\begin{matrix} \arg^{(max)} \sum_{j=1}^{m} w_j X_A \left(C_{i,j}(x) = i \right) \\ t \end{matrix} \right] \tag{1}$$

where the classifier (Cj) is a variable, and the weight associated with its prediction (wj) is a constant.

When the model is hybridized with a distributed ledger, it will be formulated as follows:

$$\psi y = \begin{bmatrix} \arg^{(max)} \sum_{j=1}^{m} w_j X_A \left(C_{i,j}(\psi x) = i \right) \\ t \end{bmatrix} \tag{2}$$

Or it can be written as follows:

$$\psi y = \begin{bmatrix} \arg^{(max)} \sum_{j=1}^{m} \left(\begin{matrix} w_j X_A \\ C_{i,j}(\sigma(h_0 w_0 + h_1 w_1 + h_2 w_2 + \cdots + h_n w_n)) \\ = i \end{matrix} \right) \\ t \end{bmatrix} \tag{3}$$

The hybrid classifier was used to combine the best features of both models. The information in y is used by XGB as an input for the logistic regression probability function. The results of a separate logistic regression investigation showed that a hybrid classifier significantly improved the accuracy to 99.7%.

5. Conclusions

The amount of data that medical sensors can capture can be overwhelming, which makes it difficult to extract the information that is most pertinent. It is necessary to have an algorithm for a body sensor network in order to identify anomalies in the information that has been gathered. The research process can make use of a variety of methodologies, including statistical sampling and machine learning. Real-time response optimization is a field that is expanding as more and more jobs that need a significant amount of computational power are offloaded to the backend. A lot of research goes into finding ways to make data transfers more efficient. The capacity for computation is distributed throughout a wide variety of fields. As more and more devices are equipped to communicate over the Internet of Things, computation will become a bottleneck in the network. It is essential to make use of parallel processing at the task level, as well as distributed computing. The conventional method to prevent the device's battery from running down too quickly is to offload the work to a server in the background.

People all over the world are becoming increasingly concerned about their privacy and safety as a result of the widespread deployment of Internet-of-Things (IoT) devices. Because of the exponential growth of online dangers, the privacy and safety precautions that we currently take are no longer sufficient. This indicates that hackers stand to benefit from the use of the Internet by anyone. The dependability of the findings that machine learning (ML) methods provide is one of the reasons that they are rising in popularity. These approaches can be used to predict and detect vulnerabilities in systems that are based on the Internet of Things (IoT). Edge computing can reduce the amount of time that it takes for a network to respond, while simultaneously boosting decentralization and security. "Edge nodes", which are often in communication with the cloud, are now able to manage a sizeable amount of the computing that is mission-critical. Using the cloud in such a way does not come with any negative consequences. With the help of this technology, it is possible to achieve solutions that are both real-time and very efficient.

In order to achieve this goal, we studied how machine learning (ML) can be coupled with cloud and edge computing by employing a distributed-edge-computing-based Internet-of-Things (IoT) framework. Internet-of-Things devices that make use of sensor frameworks are able to collect huge volumes of data that can then be analyzed. When identifying what information is most important, the front-end component could benefit from some careful planning and consideration. An Internet-of-Things server operating in the background can provide guidance and recommendations to help achieve this goal. The plan is to employ machine learning in the backend servers in order to search for data signatures that are of interest. We intend to apply the resulting concepts as a case study in the field of medicine. We are studying ways to combine the benefits of machine learning with those of cloud computing and edge computing through the use of a framework that is based on the Internet of Things (IoT) and distributed edge computing. In future, we can work on real-time systems and deep learning models.

Author Contributions: Conceptualization, A.K.A. and A.M.A.; methodology, A.K.A. and A.M.A.; software, A.M.A.; validation, A.M.A.; formal analysis, A.K.A. and A.M.A.; investigation, A.K.A. and A.M.A.; resources, A.M.A.; data curation, A.M.A.; writing—original draft preparation, A.K.A.; writing—review and editing, A.K.A. and A.M.A.; visualization, A.K.A.; supervision, A.K.A.; project administration, A.K.A.; funding acquisition, A.K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. GRANT2729).

Data Availability Statement: Not applicable. This study does not report any data.

Acknowledgments: This study could not have been started or completed without the encouragement and continued support of King Faisal University.

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

References

1. Al-Qarafi, A.; Alrowais, F.; S. Alotaibi, S.; Nemri, N.; Al-Wesabi, F.N.; Al Duhayyim, M.; Marzouk, R.; Othman, M.; Al-Shabi, M. Optimal Machine Learning Based Privacy Preserving Blockchain Assisted Internet of Things with Smart Cities Environment. *Appl. Sci.* **2022**, *12*, 5893. [CrossRef]
2. Hartmann, M.; Hashmi, U.S.; Imran, A. Edge computing in smart health care systems: Review, challenges, and research directions. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3710. [CrossRef]
3. Ray, P.P. Internet of things for smart agriculture: Technologies, practices and future direction. *J. Ambient Intell. Smart Environ.* **2017**, *9*, 395–420. [CrossRef]
4. Quy, V.K.; Van Hau, N.; Van Anh, D.; Quy, N.M.; Ban, N.T.; Lanza, S.; Randazzo, G.; Muzirafuti, A. IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. *Appl. Sci.* **2022**, *12*, 3396. [CrossRef]
5. Singh, A.K.; Verma, K.; Raj, M. IoT based Smart Agriculture System. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021. [CrossRef]
6. Shahzadi, R.; Ferzund, J.; Tausif, M.; Asif, M. Internet of Things based Expert System for Smart Agriculture. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 070947. [CrossRef]
7. Huang, J.; Kong, L.; Dai, H.N.; Ding, W.; Cheng, L.; Chen, G.; Jin, X.; Zeng, P. Blockchain-Based Mobile Crowd Sensing in Industrial Systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6553–6563. [CrossRef]
8. Hrovatin, N.; Tošić, A.; Mrissa, M.; Kavšek, B. Privacy-Preserving Data Mining on Blockchain-Based WSNs. *Appl. Sci.* **2022**, *12*, 5646. [CrossRef]
9. Zhong, G.; Xiong, K.; Zhong, Z.; Ai, B. Internet of things for high-speed railways. *Intell. Converg. Netw.* **2021**, *2*, 115–132. [CrossRef]
10. Bovenzi, G.; Aceto, G.; Ciuonzo, D.; Persico, V.; Pescape, A. A hierarchical hybrid intrusion detection approach in IoT scenarios. In Proceedings of the 2020 IEEE Global Communications Conference (GLOBECOM), Taipei, Taiwan, 8–10 December 2020. [CrossRef]
11. Khan, M.A.; Khan, M.A.; Jan, S.U.; Ahmad, J.; Jamal, S.S.; Shah, A.A.; Pitropakis, N.; Buchanan, W.J. A deep learning-based intrusion detection system for mqtt enabled iot. *Sensors* **2021**, *21*, 7016. [CrossRef]
12. Iyapparaja, M.; Alshammari, N.K.; Kumar, M.S.; Krishnan, S.S.R.; Chowdhary, C.L. Efficient resource allocation in fog computing using QTCS model. *Comput. Mater. Contin.* **2022**, *70*, 2225–2239. [CrossRef]
13. Lei, K.; Du, M.; Huang, J.; Jin, T. Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing. *IEEE Trans. Serv. Comput.* **2020**, *13*, 252–262. [CrossRef]
14. Ali, M.H.; Jaber, M.M.; Abd, S.K.; Rehman, A.; Awan, M.J.; Damaševičius, R.; Bahaj, S.A. Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). *Electronics* **2022**, *11*, 494. [CrossRef]
15. Parra, J.A.; Gutiérrez, S.A.; Branch, J.W. A Method Based on Deep Learning for the Detection and Characterization of Cybersecurity Incidents in Internet of Things Devices. *arXiv* **2022**, arXiv:2203.00608v1.
16. Fadda, G.; Fadda, M.; Ghiani, E.; Pilloni, V. *Communications and Internet of Things for Microgrids, Smart Buildings, and Homes*; Elsevier Inc.: Amsterdam, The Netherlands, 2019; ISBN 9780128177747.
17. Mir, U.; Abbasi, U.; Mir, T.; Kanwal, S.; Alamri, S. Energy Management in Smart Buildings and Homes: Current Approaches, a Hypothetical Solution, and Open Issues and Challenges. *IEEE Access* **2021**, *9*, 94132–94148. [CrossRef]
18. Hanafizadeh, P.; Amin, M.G. *The Transformative Potential of Banking Service Domains with the Emergence of FinTechs*; Palgrave Macmillan: London, UK, 2022; ISBN 0123456789.
19. Jo, O.; Kim, Y.K.; Kim, J. Internet of Things for Smart Railway: Feasibility and Applications. *IEEE Internet Things J.* **2018**, *5*, 482–490. [CrossRef]

20. Huang, J.; Kong, L.; Chen, G.; Wu, M.Y.; Liu, X.; Zeng, P. Towards secure industrial iot: Blockchain system with credit-based consensus mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
21. Wang, C.; Tan, X.; Yao, C.; Gu, F.; Shi, F.; Cao, H. Trusted Blockchain-Driven IoT Security Consensus Mechanism. *Sustainability* **2022**, *14*, 5200. [CrossRef]
22. Dai, Y.; Xu, D.; Maharjan, S.; Qiao, G.; Zhang, Y. Artificial Intelligence Empowered Edge Computing and Caching for Internet of Vehicles. *IEEE Wirel. Commun.* **2019**, *26*, 12–18. [CrossRef]
23. Liu, X. Resource Allocation in Multi-access Edge Computing: Optimization and Machine Learning. In Proceedings of the 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 27-30 October 2021; pp. 365–370. [CrossRef]
24. Huh, J.H.; Seo, Y.S. Understanding Edge Computing: Engineering Evolution with Artificial Intelligence. *IEEE Access* **2019**, *7*, 164229–164245. [CrossRef]
25. Pu, C. A Novel Blockchain-Based Trust Management Scheme for Vehicular Networks. In Proceedings of the 2021 Wireless Telecommunications Symposium (WTS), Virtual, 21–23 April 2021. [CrossRef]
26. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N. Blockchain-Based Trust Management for Internet of Vehicles. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1397–1409. [CrossRef]
27. Saeedi, K. Machine Learning for Ddos Detection in Packet Core Network for IoT. *Comput. Sci. Eng.* **2019**.
28. Ali, F.; El-Sappagh, S.; Islam, S.M.R.; Ali, A.; Attique, M.; Imran, M.; Kwak, K.S. An intelligent healthcare monitoring framework using wearable sensors and social networking data. *Futur. Gener. Comput. Syst.* **2020**, *114*, 23–43. [CrossRef]
29. Raj, J.S. Optimized Mobile Edge Computing Framework for IoT based Medical Sensor Network Nodes. *J. Ubiquitous Comput. Commun. Technol.* **2021**, *3*, 33–42. [CrossRef]
30. Sureddy, S.; Rashmi, K.; Gayathri, R.; Nadhan, A.S. Flexible Deep Learning in Edge Computing for Internet of Things. *Int. J. Pure Appl. Math.* **2018**, *119*, 531–543.
31. Hakak, S.; Ray, S.; Khan, W.Z.; Scheme, E. A Framework for Edge-Assisted Healthcare Data Analytics using Federated Learning. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 3423–3427. [CrossRef]
32. Sodhro, A.H.; Pirbhulal, S.; De Albuquerque, V.H.C. Artificial Intelligence-Driven Mechanism for Edge Computing-Based Industrial Applications. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4235–4243. [CrossRef]
33. Laxmi Lydia, E.; Anupama, C.S.S.; Beno, A.; Elhoseny, M.; Alshehri, M.D.; Selim, M.M. Cognitive computing-based COVID-19 detection on Internet of things-enabled edge computing environment. *Soft Comput.* **2021**, *6*, 1–12. [CrossRef] [PubMed]
34. Verma, P.; Tiwari, R.; Hong, W.C.; Upadhyay, S.; Yeh, Y.H. FETCH: A Deep Learning-Based Fog Computing and IoT Integrated Environment for Healthcare Monitoring and Diagnosis. *IEEE Access* **2022**, *10*, 12548–12563. [CrossRef]
35. Kumar, M. Healthcare Solution based on Machine Learning Applications in IOT and Edge Computing Edge Computing View project Cloud Computing System Models View project. 2020, 119, 1473–1484. *Int. J. Pure Appl. Math.* **2020**, *119*, 1473–1484.
36. Hayyolalam, V.; Aloqaily, M.; Ozkasap, O.; Guizani, M. Edge Intelligence for Empowering IoT-Based Healthcare Systems. *IEEE Wirel. Commun.* **2021**, *28*, 6–14. [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.