IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 November 2023, accepted 24 November 2023, date of publication 27 November 2023,
date of current version 8 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3337092

RESEARCH ARTICLE

Enhancing Healthcare Efficacy Through IoT-Edge Fusion: A Novel Approach for Smart Health Monitoring and Diagnosis

MUHAMMAD IZHAR[1], SYED ASAD ALI NAQVI[1], ADEEL AHMED[2], SAIMA ABDULLAH[2], NAZIK ALTURKI[3], AND LEILA JAMEL[3]

[1]Department of Computer Science and Information Technology, Superior University, Lahore, Punjab 54000, Pakistan
[2]Department of Computer Science, Faculty of Computing, The Islamia University of Bahawalpur Pakistan, Bahawalpur, Punjab 63100, Pakistan
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

Corresponding author: Adeel Ahmed (adeelmcs@gmail.com)

This research is supported via funding from Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R333), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

ABSTRACT This paper presents an innovative framework that leverages cutting-edge technologies to revolutionize healthcare systems, focusing on data security, privacy, and efficient medical diagnosis. Our approach integrates distributed ledger technology (DLT), artificial intelligence (AI), and edge computing to create a robust and dependable medical ecosystem. In our proposed system, patients' health data is securely managed using a combination of elliptic curve cryptography-based identity-based cryptosystems and edge nodes, ensuring both privacy and integrity. These edge nodes, designed for low-power and short-range communication, play a pivotal role in in-vivo data collection and monitoring within the human body. The DLT model at the core of our framework utilizes peer-to-peer networks, enabling seamless information exchange while eliminating the need for centralized servers. We emphasize public edge DLTs, such as Ethereum, to ensure accessibility and data ownership for all stakeholders. Furthermore, our system incorporates a hybrid machine learning model for early detection and prediction of security threats, enhancing overall system efficiency. Our findings demonstrate a remarkable 99.7% accuracy in classification using this approach. In conclusion, this framework's multidisciplinary approach bridges the gap between healthcare, edge computing, and DLT, promising real-time data processing, enhanced security, and privacy preservation. With the rise of the Internet of Things, this innovation holds the potential to transform the future of healthcare technology.

INDEX TERMS Cloud computing, edge computing, IoT, ML, wireless sensor network.

I. INTRODUCTION

The ''Internet of Things'' (IoT) is a networked system that makes it possible for computing components that were previously separated to communicate with one another and interact with one another. This paves the way for the smooth gathering and transfer of data with as little intervention from humans as possible. The Internet of Things, sometimes known by its acronym IoT, is a subject of research that is still in its infancy but has the potential to exert a substantial influence on the development of other areas of technology. The repercussions of the technological improvements that were made feasible as a result of this can be felt throughout a diverse variety of business sectors. The ''Internet of Medical Things'' (sometimes abbreviated as ''IoMT'') is a subset of the Internet of Things that is experiencing significant expansion in the field of medicine.

Implanted medical devices (IMD) and wearable technology are two examples of applications of the Internet of Things that can assist in providing the highest quality of care possible in a healthcare setting that is based on IoT. This is achievable because IoT applications can help improve patient outcomes. Numerous pieces of research have demonstrated that remote patient monitoring presents a number of opportunities for improvement that should be pursued. Patients who are not currently in imminent danger can nevertheless reap

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

the benefits of remote monitoring thanks to the technological advancements that have been made in today's healthcare delivery systems.

As a result of this method, elderly folks won't have to be moved from their homes to clinics or hospitals for treatment. Treatment strategies for AAL, the management of diabetic complications, and rehabilitation are just a few examples of where IoMT has been effective [1]. The optimum course of treatment for persons who have suffered bodily harm can now be determined using a recently developed technology. Treatment and pharmaceutical suggestions are provided by the algorithm after comparing the patient's symptoms to those in the database. A strategy is considered successful if it results in a treatment plan that is accepted by at least 89% of the treating physicians. It has been shown that using IoMT technology to treat people with Parkinson's disease is effective. Medical wearables with vision-based technology may enhance our ability to monitor vital indications in real time.

The links between fat and diabetes and other diseases have been explored at length elsewhere. Given the particulars of this case, we need two distinct glucose measurements. In each of these examples, the risks of relying solely on self-measured blood sugar levels become abundantly clear. The system will issue a warning; however, who exactly receives the warning depends on the patient's state and the members of the medical staff. Prevention of cardiovascular disease and early diagnosis of disease are two other areas where IoMT could prove useful. The ECG sensor is currently monitoring the number of times your heart is beating every minute. Through the use of a microcontroller, the data is transmitted to the patient's mobile device. It's possible that a lot of lives could be saved if this method could help doctors detect an oncoming heart attack.

It has been proposed that the SPHERE technology could be utilized to provide treatment to elderly people without requiring those patients to leave the comfort of their own homes. Patients of advanced age may benefit from this method since it enables them to remain at home rather than make frequent visits to the hospital. It is more important than ever before to protect the privacy of patients' medical records, which may contain sensitive information about their health. There is an elevated risk of a data breach if there is communication of patient information via a wireless network and storage of such information in a database. If a patient were to misuse a gadget, both their privacy and their safety could be put in jeopardy. As a result of developments in information technology, modern healthcare is increasingly concerned about the efficacy of remote patient monitoring as well as the speed with which it can respond to an unexpected situation. The main contribution of this study is:

- Secure connectivity between edge nodes and protection of patient data is two of the main goals of designing edge-based computing for data collection.
- Use a novel hybrid model to foresee and prevent cyber-attacks on a healthcare system built on the Internet of Things and Edge Nodes.

II. RELATED WORK

Processing at the network's periphery, or "edge," is becoming increasingly popular. Traditional programs can benefit from cloud computing's distributed architecture and increased efficiency. There are still problems with edge networks that cloud computing can't fix, like insufficient resources, poor transmission, and a lack of useful features. When state-of-the-art gadgets work together, they create an unstable environment. An innovative method for bettering collaborative systems is described by Sureddy et al. [2]. In addition, it is possible to optimize cooperation between nodes located close to the network's edge. To prove the effectiveness of the proposed architecture, we evaluate data collected from actual seniors and their wearable sensors. The proposed optimization method can also be tested and evaluated through extensive experimentation.

When applied to the massive amount of raw sensor data produced by IoT devices, deep learning shows great promise. Given deep learning's decentralized nature, it finds its greatest utility at the periphery of a network. Edge computing has strict requirements. It would be helpful to have an IoT edge computing framework that is more flexible. To move deep learning to the edge, the suggested method makes use of several agents and a flexible edge computing architecture. Researchers [2] also design a novel offloading strategy to improve the performance of deep learning applications at the edge, given the current state of edge node processing capability. The FEC architecture is a concept for advanced IoT systems with the flexibility to adjust to new environments and user requirements. In this article, we investigate how well FEC architecture fares on deep learning tasks that include working at the edges. Our strategy has been shown to be the most efficient way to use deep learning with the IoT.

Wearables, the Internet of Things, and edge computing are just a few examples of the developing ICTs that are transforming healthcare into digital health. High-tech fitness trackers worn on the wrist are becoming increasingly popular as consumer devices for monitoring health and fitness. Even with all the progress that has been made, the healthcare system is not making the most of these tools to collect longitudinal behavioral trends. Data acquired from users in a secure manner has the potential to design a preventative and all-encompassing healthcare system. To retrain local machine learning models with user-generated data, the authors of this study [3] present a Federated Learning-powered Edge-assisted data analytics system. Pre-trained models could be used in this method to generate unique customer insights without compromising the security or scalability of the Cloud. The author does more than just list uses for the proposed paradigm; she also highlights knowledge gaps.

In IoT-based industrial applications, edge computing is preferable to cloud computing when it comes to managing scarce resources like power and battery life. This is due to the higher processing cost of the former and the longer delay introduced by the latter. Meanwhile, there has been a lot of talk about how AI can be used to enhance resource management in the business and industrial sectors. Coordinated edge AI can help industrial IoT devices reach further and analyze more data. Power-hungry, low-battery-life, zero-tolerance-for-delay portable electronics pose a serious threat to established norms of fair distribution. Power-saving and battery-extending techniques like predictive transmission power control (PTPC) and the industry standard Baseline are proved to be insufficient for maintaining a dynamic wireless channel in large-scale industrial datasets. By shifting when IoT-based mobile devices do their sensing and sending operations, this research [4] provides a forward central dynamic and availability solution (FCDAA) to this issue. The hybrid TPC/duty-cycle network data dependability paradigm is useful for AI-powered edge IoT devices. A battery model at the system level is used to examine energy loss in the Internet of Things. To aid in the efficient monitoring of industrial platforms, we present two crucial scenarios: the static scenario of product processing, and the dynamic scenario of vibration detection and problem discovery. The proposed FCDAA improves efficiency and battery life while keeping reliability at a manageable 0.95. This can be done by experimenting with different values for the duty cycle and TPC.

Decision-makers in the current pandemic can benefit from the use of cognitive computing, artificial intelligence, pattern recognition, chatbots, wearables, and the edge distributed ledger to collect and analyze medical data. Cognitive computing is a useful tool in medicine because of its speed and accuracy in analyzing massive data sets and offering individualized, smart recommendations for the diagnosis and treatment of disease. However, in light of the current worldwide epidemic of COVID-19, speedy diagnosis is crucial to reducing death tolls. A large library of chest radiographs can be analyzed by radiologists using DL models. However, a large amount of data must be gathered in one location for training to be effective. Therefore, the FL strategy can be used to construct a shared model for DL-based COVID-19 detection without the need for locally collected data. A COVID-19 (FDL-COVID) detection model is presented by Lydia et al. [5], which uses federated deep learning and is deployed on an IoT-enabled edge computing platform.

After gathering patient information from IoT devices, Squeeze Net is used to create a DL model. The cloud server collects encrypted data from IoT devices and applies FL to the most important variables using a Squeeze Net model to construct a global cloud model. In addition, the glowworm swarm optimization method is used to fine-tune the Squeeze Net architecture's hyper parameters. The studies' trustworthiness is measured against a standard CXR dataset in a number of ways. The FDL-COVID method outperformed its rivals in all test conditions.

In today's healthcare industry, patients are looking for a doctor who can work around their schedules without compromising on the quality of their treatment. By combining the lightning-fast speeds of 5G with cutting-edge computing power, we can create the low-latency, low-energy environment necessary for near-instantaneous health data collection and analysis. The bulk of studies have overlooked how crucial it is for healthcare organizations to implement optimal computing techniques like encryption, authentication, and classification on the devices deployed in an edge computing architecture. This study's [6] goals are twofold: first, to describe the unique requirements and challenges of devices for various use cases; and second, to give a thorough review of the most recent and cutting-edge edge computing architectures and techniques for healthcare applications. Vitals, activity, and fall monitoring all require the classification of health data, making edge computing particularly helpful. Other low-latency apps monitor disease-specific symptoms; such as gait issues in Parkinson's disease patients. Within the context of edge computing, the author explores in detail a number of data-related tasks, such as transfer, encryption, authentication, categorization, simplification, and forecasting. To achieve parity with Cloud-based alternatives while reducing computational complexity, edge computing requires extensive privacy and data minimization strategies. The use of edge computing in healthcare has opened up new, exciting research avenues.

There are major issues with data synchronization in the existing cloud-based architecture just before cutover and migration. Although cloud computing is on the rise, its limited scalability in regards to security issues has slowed the rollout of a centralized IoT's-based system. There is a growing burden on devices due to the complexity of health systems such as health monitoring, which require the processing of enormous volumes of data on a computer. Fog computing is the practice of integrating cloud and on-premises computing to enhance user experience [7]. This is a novel method for optimizing cloud services. Several problems exist in the existing fog computing models that must be fixed. If, for instance, a system is required to govern both the accuracy of data and an exaggerated response time, compatibility may be compromised. The new FETCH framework can help improve the treatment of heart disease and other real-world health care systems. This system uses edge computing devices to boost deep learning and streamline monitoring processes. The proposed Fog-enabled cloud computing system that utilizes Fog Bus has many advantages, including lower energy usage, reduced network latency and jitter, quicker process execution, and more reliable outputs.

Although cloud computing and the Internet of Things don't always work together, they both play crucial roles in our daily lives. Healthcare, security, assisted living, agriculture, and asset monitoring are just some of the fields that could benefit from the integration of these two technologies. Cloud computing, however, is not well suited for use with programs that require instantaneous answers because of network latency difficulties. In order to do computation closer to the "edge of the network," where latency may be lower, a ground-breaking technique known as "edge computing" was developed. Latency, energy consumption, bandwidth expenses, data privacy, and security are all issues that can be solved by using edge computing. The potential medical uses of edge computing and the Internet of Things are discussed.

In [8], Kumar and Majumder explore if and how a Distributed Computing–based Internet of Things architecture may incorporate cloud/edge computing and the Machine Learning paradigm. The ultimate goal of IoT gadgets is to mine the mountains of data generated by their front-end Sensor frameworks for useful insights. Intelligent data organization is now possible with improved front-end modules. A server connected to the Internet of Things could offer support in the background. It is recommended that a Machine Learning-based solution be included into the server's backend so that it can automatically recognize and zero in on signatures of interest in the data it has previously received.

Access to high-quality, cost-effective medical care is more crucial than ever in light of these changes. Innovative solutions are needed to address the difficulties that have surfaced as the demands placed on this important infrastructure increase. Bringing healthcare systems closer to the data sources using edge computing technology can minimize latency and energy consumption compared to conventional cloud and IoT-based systems. Early detection and prediction of high-risk diseases, together with decreased patient healthcare expenditures and increased treatment efficacy, are all possible because to artificial intelligence's capacity to automate insights into smart healthcare systems. The possibilities of AI and other forms of edge intelligence (EI) to enhance smart healthcare systems are explored in this article [9]. In order to improve healthcare delivery, we advocate for a shift toward "smart healthcare," in which AI and EC are widely implemented in healthcare IT. We also look into the pros and cons of mixing technologies. Authors [10] have suggested an Energy-Efficient Data Aggregation Mechanism (EEDAM) that is secured through blockchain to save energy.

The paper [11] depicted Threat Classification Model (TCM) using fuzzy logic (FL) for detection in real-time of a suitable privacy level for videos transmitting. Researchers [12], [13] discuss the recent developments in IoT privacy and security, points out unresolved problems, and offers areas for further research.To address [14] the issueswith response time, message failure, fault tolerance, and security offered by the blockchain, authors put forth heuristic methods.While reducing the reaction time for urgent communications and unloading the cloud infrastructure, the suggested method calls for only minor changes to the current Internet of Things ecosystem [15]. This study proposes a message scheduling for a blockchain-based architecture [16], and develop an efficient algorithm for cross-layer architecture at network and application level [17]. The use of IoT and Blockchain technology allows for a smart technique of detecting and preventing COVID-19 victims [18] and authors [19] suggest auto detects encoder and secure the video output of very encoder. In this paper [20] authors analyze the various ML techniques and predict the breast cancer.

This article [21] combines network coding with a negotiated WSN architecture to reduce the number of messages via message aggregation. Authors [22] proposed a novel feature selection method for malicious intrusion detection in IoT using ML algorithms. The new system "VQProtect" described in this work [23] focuses on the visual quality protection of compressed videos by identifying and fixing channel defects.

The paper [24] describe "A novel Energy Efficient Message scheduling algorithm EAAFTMS (An Energy-Aware Available and Fault-Tolerant System with Message Scheduling in IoT)" Researchers [25] design an edge node group based on task arrivals and use a decentralized approach to execute tasks in parallel mode in order to finish execution and the IoT based smart fire detection and deterrent system [26]. This study examines the development of AI-enhanced data technologies and how they have affected computing systems [27]. This study [28], [29] explores into the topic of Mobile Edge Computing, or MEC, networks, which are comprised of a large number of mobile devices that send their tasks for computing to a combination of edge servers and a central cloud node.IoT networks that use ML to solve security and privacy problems [30], [31] and give the concept of efficient, privacy-preserving medical diagnostic solution [32].

Researchers [33] also developed novel cipher scheme to enhance the security of transmitted dat.aTo overcome the problems such as power, memory, and life of battery multi-access edge computing has recently evolved [34]. Authors [35] introduce FTPipeHD, a fault-tolerant DNN training method for distributed heterogeneous devices, in this work.This study [36] presents FedMint, a game theory and bootstrapping-based intelligent client selection technique for IoT federated learning.In this study [37], researchers provide a novel computational offloading choice paradigm aimed at reducing the long-term payment associated with computing jobs that include mixed bound restrictions.

Table 1 shows the comparative analysis of previous state of the art studies:

Authors [35] introduce FTPipeHD, a fault-tolerant DNN training method for distributed heterogeneous devices, in this work. This study [36] presents FedMint, a game theory and bootstrapping-based intelligent client selection technique for IoT federated learning. In this study [37], researchers provide a novel computational offloading choice paradigm aimed at reducing the long-term payment associated with computing jobs that include mixed bound restrictions. A unique architectural framework was developed and executed, combining four deep learning techniques using edge computing devices [38]. The present study presents a novel framework for athlete healthcare that leverages IoT-edge computing technologies to enhance the provision of medical treatment [39]. As healthcare difficulties rise, ML, Edge AI,IoMT, 6G, and cloud

TABLE 1. Comparative analysis of previous studies.

References	Datasets	Techniques	Outcome
[1]	Real datasets obtained from elderly people and their wearable sensors	Using a new framework, optimize a network of cooperating edges.	construction of an ECN optimization framework
Sureddy et al., 2018		integrates deep learning with edge computing while also allowing for scalability	superior to alternative methods of optimizing deep learning for Internet of Things
Sodhro et al., 2019	large-scale industrial data sets	Model of data reliability for edge AI with forward-looking centralized dynamics and availability	By fine-tuning the duty-cycle, FCDAA increases energy economy and battery life while maintaining an acceptable level of reliability (0.95).
Laxmi Lydia et al., 2021	federated deep learning-based COVID-19 dataset	distributed systems for deep learning Model for detecting COVID-19 (FDL-COVID)	better results from using the FDL-COVID method
Hartmann et al., 2022)	Edge Nodes Dataset	recent developments in edge computing design and methodology	equivalent functionality to that of Cloud-based alternatives
(Verma et al., 2022	Edge Nodes Dataset	FETCH is a proposed framework	Standardization of sophisticated deep learning models for use in edge computing
Kumar, 2020	Edge Nodes Dataset	Edge computing	End point IoT device, such a system can also fetch information from the cloud and take care of any necessary offloading.
Hayyolaam et al., 2021	Edge Nodes Dataset	edge technology along with AI techniques	Edge technology is useful for smart healthcare systems because it reduces the systems' dependence on the network and the energy required by the network.

computing can help to solve issues [40], [41], [42] including deep learning [43].

The present research study introduces a conceptual framework for the design of Electronic Medical Record (EMR) that employs metaphoric elements in the context of periodic health examination (PHE) reports for patients [44]. In this study [45], hybrid genetic algorithm is proposed as a means of optimizing query path selection. This study [46] describes a hybrid deep-learning system for various cyber-attacks smart city platform. This work [47] optimizes a healthcare automation monitoring system supported by wearable computing, edge cloud, and IoT to improve patient rehabilitation.

The field of study [48] looks at why people use technology, how they do it, and when they do it. It includes IoT), behavioral science, and edge analytics. This study [49] introduced a flexible, IoT-aware, modular system design with several potential medical applications. In this study [50], scholars present an alternating technique based on low-complexity fractional programming (FP) to effectively address the optimization problems that exhibit non-convex characteristics.

III. PROPOSED EEDAM FRAMEWORK

Dependability is ensured via artificial intelligence. Figure 1 illustrates how a distributed ledger with a twist can revolutionize the medical field. User, wireless network, edge distributed ledger, trusted agent, and healthcare server are all parts of the system. Patients who use this product have a 50/50 chance of either being cured or having their condition worsen. His health is monitored by a plethora of apparatus, both external and internal. Smartphones and other PDAs are not alone in their ability to accept and retain medical data from sensors. When a patient's medical records are encrypted on their mobile device, they can be transferred to the edge distributed ledger in the form of a block on a regular basis. All of the citations in this section are carbon copies of one another in terms of content, creation date, and other relevant particulars.

Validating agents and recording agents are the two types of authorized agents. All financial dealings are checked for legitimacy by a network of computers known as validation agents (VA). A transaction's legitimacy must be confirmed by a validator in the network before it is recorded in the distributed ledger at the periphery of the network. After information has been checked, the agents that recorded it place it in encrypted blocks.

The hospital, physicians, and diagnostic expert system each have their own data storage systems. The outputs of diagnostic expert systems may be trusted to be correct, just as they would be from a human doctor. Data analysis has long been utilized by medical professionals to aid in the diagnosis of illness, long before the development of the encrypted edge distributed ledger. Sensors implanted in the patient's body allow for the remote delivery of possibly lifesaving drugs. Our proposed model is basically represented in this diagram.

In this section, we will present a mathematical model for the key components of the proposed study, which includes the security and privacy-preserving aspects, as well as the performance evaluation.

Security and Privacy-Preserving Model:

1. Elliptic Curve Cryptography (ECC) Encryption:

The security and privacy of patient data are achieved through the use of elliptic curve cryptography-based identity-based cryptosystems (ECC-IBC). The mathematical representation of ECC encryption can be expressed as follows:

$$E(P, k) = Q$$

where:

E represents the elliptic curve encryption function.

P denotes the patient's data.

k represents the encryption key.

Q is the resulting encrypted data.

Privacy-Preserving Strategy:

To assess the effectiveness of the privacy-preserving strategy, we can employ a mathematical model for quantifying data privacy. The model could be based on metrics such as Shannon's entropy or K-anonymity, and can be expressed as:

$$\text{Privacy} = \text{f(Data)}$$

where:

Privacy represents the degree of data privacy.

f is a privacy-preserving function.

Data refers to the patient's medical data.

Performance Evaluation Model

Distributed Ledger Transaction Throughput:

To evaluate the performance of the distributed ledger system, we can use a mathematical model to describe the transaction throughput (TPS) as a function of various parameters. This can be represented as:

$$\text{TPS} = \text{g}\left(\text{Block}_{\text{Size}}, \text{Network}_{\text{Latency}}, \text{Validation}_{\text{Agents}}, \ldots\right)$$

where:

TPS is the transaction throughput.

g represents the function that calculates throughput.

$\text{Block}_{\text{Size}}$ denotes the size of data blocks.

$\text{Network}_{\text{Latency}}$ is the time it takes for data to propagate across the network.

$\text{Validation}_{\text{Agents}}$ is the number of agents responsible for transaction validation.

Hybrid Machine Learning Model:

The performance of the hybrid machine learning model can be analyzed using standard classification metrics. One such metric is accuracy (ACC), which can be expressed as:

$$\text{ACC} = \text{TP} + \frac{\text{FP}}{\text{TP}}$$

where:

ACC represents accuracy.

TP is the number of true positives.

FP is the number of false positives.

A. MEDICAL HEALTHCARE SYSTEM

Both medical facilities and trained professionals are in short supply. Many people have lost their lives too soon because they were unable to receive a timely medical diagnosis. The proposed paradigm could aid in the response to a widespread disaster by allowing for the simultaneous monitoring and diagnosis of large groups of people. This innovation facilitates interaction between hospitals and their patients. The health records of Edge users are stored in a distributed database on the blockchain.

The public key cryptosystem safeguards the veracity, anonymity, and integrity of information. Artificial intelligence examines a patient's medical history, makes a diagnosis, and proposes a treatment plan.

B. SECURED AND PRIVACY PRESERVING

The method proposes protecting patients' medical records by employing elliptic curve cryptography-based identity-based cryptosystems. This will guarantee that the files will always be illegible. The IBC cannot be held liable for failing to verify the recipient's possession of a valid public key because it is not responsible for doing so. The speed with which computations can be performed with ECC arithmetic is roughly 20 times faster than using modular exponentiation. In terms of RSA, the security provided by a key with 1024 RSA bits is equivalent to that of a key with 128 bits of ECC. IBC and ECC are two areas of technology that may find several applications in the Internet of Things since they each have characteristics that cannot be found in the other.

C. PROPOSED EDGE NODES BASED HEALTHCARE IOT SYSTEM

Communication between EDGE NODES can be thought of as occurring in vivo or in vitro, depending on the location of the radio signal's reception. These days, novel in-vivo communication strategies like body-coupled communication are used to establish unique identities within the body domain network. Since most edge node devices are intended to be worn on the body, we refer to them in terms of low-power and short-range communication. A possible "external communication" is demonstrated by the following.

D. PROPOSED EDGE DISTRIBUTED LEDGER MODEL

Distributed ledger systems rely on P2P networks to ensure seamless information exchange at the network's periphery. If nodes are to be located everywhere in the world while maintaining full network connectivity, then this must be the case. Distributed ledger systems rely on P2P networks to ensure seamless information exchange at the network's periphery. There is no centralized server in a P2P network, therefore each node serves as both a content consumer and a content producer. Components of routing include connection setup and upkeep, the dissemination and verification of transactions, and the synchronization of data blocks. As you'll see, nodes constitute the foundation of a network, while blocks and transactions make up the distributed ledger's outermost layers. This is typical of P2P networks, which are horizontal and decentralized. Many edge applications built on distributed ledger technology rely on APIs in order to function. With these application programming interfaces (APIs),

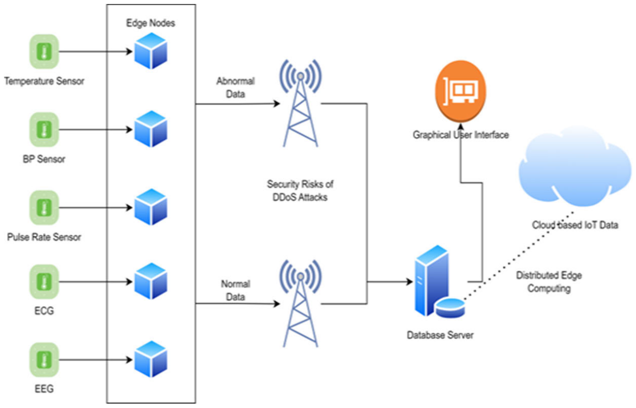

FIGURE 1. Proposed system architecture.

customers can interact with the service regardless of the technology they use.

E. PUBLIC EDGE DISTRIBUTED LEDGER TECHNOLOGY

We have made efficient use of the tools that allow public edge distributed ledger networks to rapidly expand their user bases without relying on a single administrator. Typically, anyone can join in on the good times. This means that everyone has a chance to weigh in on whether or not the ledger is accurate. Ethereum is a widely known blockchain platform. Since everyone has access to the public edge distributed ledger, no one can dictate how it develops. A public distributed ledger is a database that anybody can join at any time. Users of a public edge distributed ledger have unrestricted access to all data already stored on the ledger and can update it at any moment by adding new blocks of data. Traditionally, cryptocurrency transactions and mining have been carried out on the ledger's surface. Public Edge is a distributed ledger technology that can assist mitigate the effects of compromised data in cloud storage. The database will be a distributed ledger updated by nodes at the edge of the network.

F. CLOUD BASED EDGE DISTRIBUTED LEDGER

For a rising number of businesses, ensuring the security of their centralized database systems is becoming an increasingly critical priority. On the other hand, people's knowledge of the threat that hackers pose has increased in recent years. When cybercriminals are attempting to gain access to big amounts of data, one strategy that they will utilize is to launch assaults aimed at programmable databases. The utilization of technology known as distributed ledgers, which includes edge distributed ledgers in addition to other kinds of distributed ledgers, makes the problem even more complicated. Distributed ledgers are currently the subject of a substantial amount of cutting-edge research, all of which has the same overarching goal in mind, which is to increase the security of data storage. This purpose is to make distributed ledgers more secure. This has the potential to make a significant impact on how consumers perceive the website as a whole.

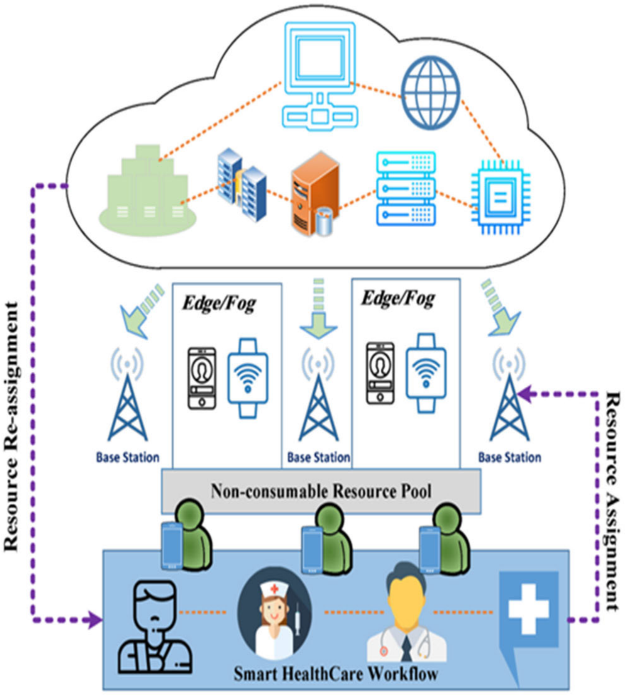

FIGURE 2. Edge based medical healthcare system.

The proponents of the edge distributed ledger highlight that users will retain full ownership of their own data even though it is possible that the technology might open the path for more secure kinds of data storage. This is in spite of the fact that edge distributed ledgers have the potential to usher in more trustworthy methods of data storage. On the market today, there are still a significant number of distributed ledger systems that use the coin it was originally based on. Users have been left with a number of concerns as a result of the recent string of large-scale data breaches. One of these concerns is an increased danger of identity theft. A further cause for concern is the heightened potential for other forms of breaches in security. For transactions on the peripheral of a distributed ledger, digital signatures can be used instead of traditional signatures in order to guarantee properties such as the non-repudiation of transactions and the integrity of communications. Cloud storage that makes use of distributed ledger technology at the network's edges performs at its highest level of efficiency while dealing with relatively tiny amounts of data.

After that is complete, supplementary precautions will be implemented all throughout the network. This is made possible thanks to the cooperation of a variety of distinct technologies, the most notable of which being hash algorithms, public-key and private-key encryption, and transaction logs, amongst others. Distributed ledgers that are stored close to the network's edge may be able to deliver superior levels of availability, reduced costs, and higher levels of security when compared to cloud-based alternatives.

It is common practice for cloud storage companies to generate several backup copies of their clients' data and

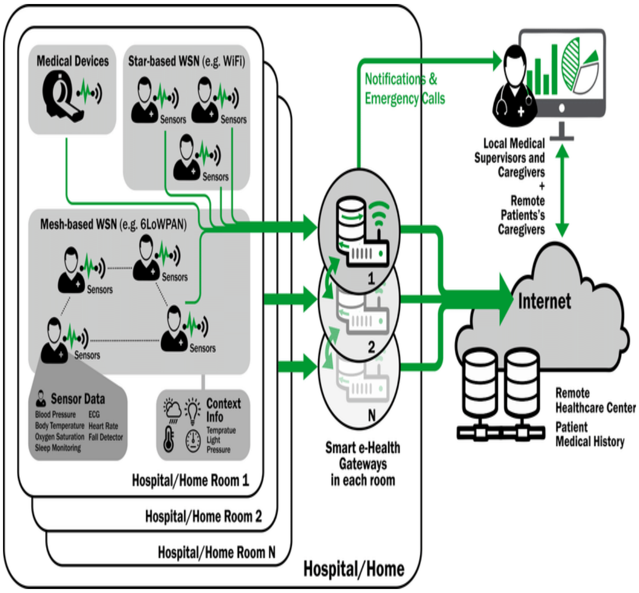

FIGURE 3. Proposed edge nodes sensors IoT based system.

to keep those copies in a number of different geographic locations. Previous research has shown that storing data in the cloud presents a number of inherent issues, one of which is the chance that the data may be altered. Another inherent challenge is the possibility that the data would be lost. Computing in the cloud, which centralizes all of your information in a single spot from which it can be accessed more easily, was the solution we opted to implement. Cloud storage companies make several copies of their customers' data and then store those copies in a number of different geographic locations to protect both the data's integrity and its customers' privacy.

G. PRIVACY PRESERVING STRATEGY

Three of the most popular algorithms in cryptography today are RSA, Blowfish, and AES. We compare and contrast these three approaches to privacy protection and suggest a fourth, hybrid approach based on our findings. Multiple layers of encryption are used by the EDGE NODE networks to keep your data secure. However, as state-of-the-art technology evolves, traditional methods will eventually become defunct. As computing has progressed, encryption has become easier to break. Constant assaults have worn away at the system's backing.

Thanks to cryptanalysis and other targeted mathematical attacks, it is now much easier for cryptographers to circumvent these safeguards. Existing systems lack essential components of security as well. The inability to safely store and transfer secrets is a major shortcoming of existing methods. Finding a balance between protecting user privacy and keeping systems up and running is essential. More robust encryption techniques sometimes employ keys with longer lifetimes, which may reduce the overall efficiency of the system.

Single-layer encryption methods are vulnerable to key compromise and information disclosure if used in isolation. Information security is compromised when a system is used in isolation. The variety of potential issues plaguing autonomous systems limits their efficacy. There is a growing need for a system that can handle speed and security concerns caused by the use of various cryptographic algorithms.

IV. RESULTS AND SIMULATIONS

We were concerned about the energy needed for the calculation of messages and their transmission across Edge Node Networks while considering the usage of distributed ledgers at the edge to secure patient data. The author relies on machine learning models to achieve the early detection goal for the safety of the system.

A. COMMUNICATION VS SECURITY LEVEL IN EDGE NODES

Sign encryption places a large workload burden on the system. The transmission overhead is mostly determined by the size of the signed message. In an EDGE NODE, users typically require only two bytes. Figure 5 displays the total cost and the level of security of our communications. As security measures become more stringent, people's desire for human connection increases.

B. EDGE DISTRIBUTED LEDGER PERFORMANCE

Here, the EDGE NODE platform was tested with the distributed ledger activated to show that it might survive in the long run. One authoritative node and four peers were put up to measure how well distributed ledger networks function at the network's edge. The optimal data transfer rate for the proposed EDGE NODE technology was determined via trial and error. There is a great deal of flexibility in how one can segment throughput. By consensus, transaction throughput is the rate at which a distributed ledger's edge nodes process transactions. In distributed ledger networks, read-through was employed by nodes in the periphery to keep track of how often data was viewed.

We were able to measure how adjusting the TPS's transmit and random machine utilization characteristics affected transaction read throughput.

C. PRIVACY PRESERVING

In this paper, we introduce a new method for protecting user privacy that combines aspects of the Advance Encryption Standard, the Blowfish, and the RSA cryptographic algorithms. Edge node networks (EDGE NODES) utilize numerous encryption algorithms to keep their customers' data secure. As sophisticated technology improve, however, the use of such antiquated techniques becomes less and less relevant. The time required to crack a cryptographic system has been drastically reduced thanks to recent technological advancements. Multiple assaults on the current defenses have been successful. Figure 7 shows the findings of the analysis of the Privacy Preserving Strategy.

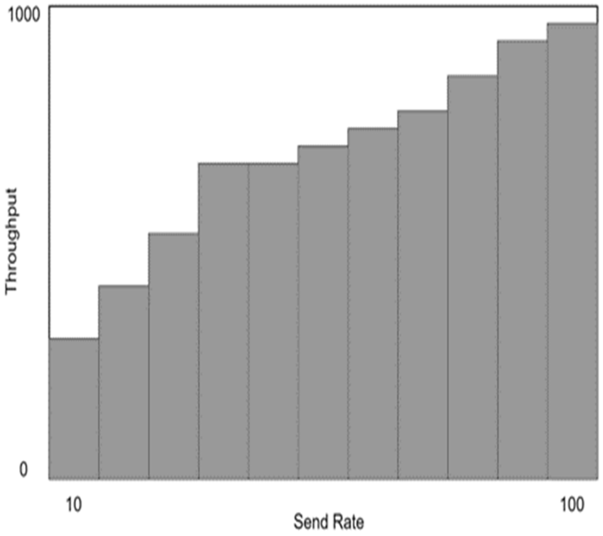

FIGURE 4. Performance of proposed system in communication.

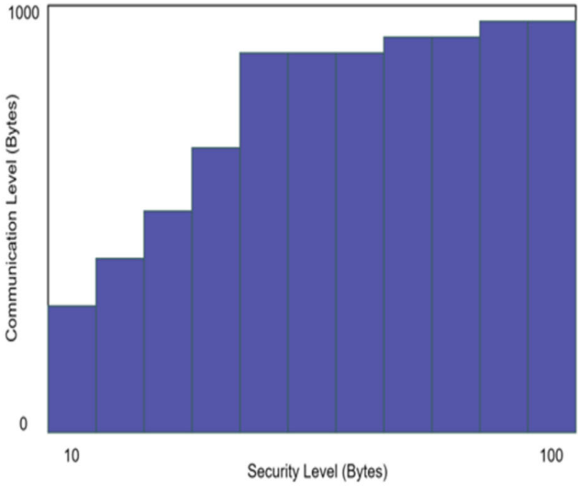

FIGURE 5. Read transaction throughout.

D. PREDICTION OF DDoS ATTACKS

The author has collected transaction data using the distributed ledger's edge nodes and trained a machine learning model to ensure patient privacy.

E. HYBRID MACHINE LEARNING MODEL

An example of an estimator used in machine learning is the Hybrid Voting classifier, which takes the predictions of multiple base estimators and merges them into a single prediction. The final grade will be decided by a simple majority of the raters. The Hybrid Voting classifier estimator integrates advantageous aspects of various models. A hybrid voting classifier can classify data using a simple majority vote, where each vote is weighted according to the likelihood of each class. The prediction of an ensemble classifier is depicted in the following diagram.

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

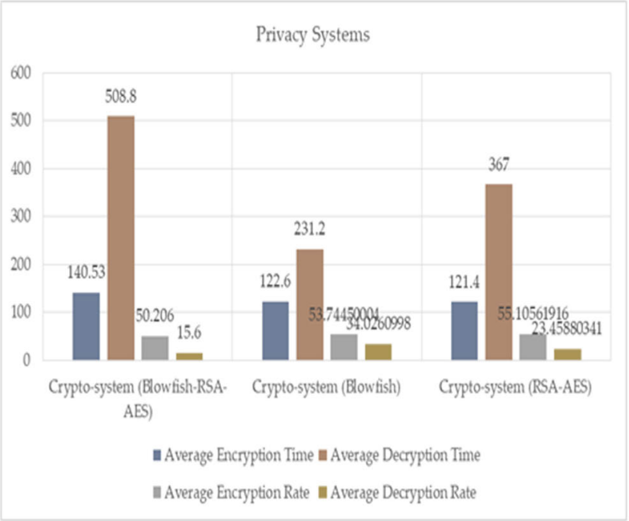

FIGURE 6. Performance analysis of privacy preserving strategy.

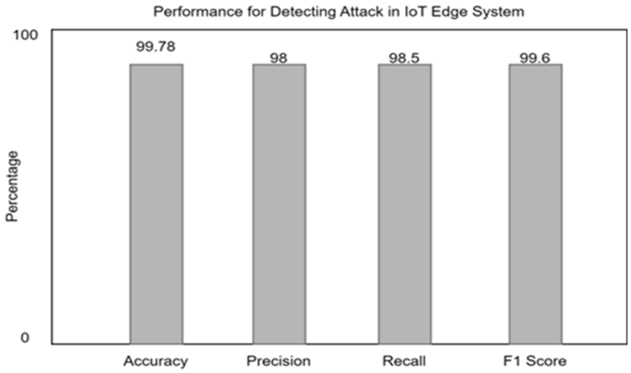

FIGURE 7. Hybrid classification model performance.

Classifier (Cj) is a variable, and the weight (wj) associated with its prediction is a constant in the aforementioned formula. Hybridization of the model with a distributed ledger results in the following formulation:

$$\psi y = \left[\text{arg} \frac{(max) \sum_{j=1}^{m} w_j X_A \left(C_{i,j}(\psi x) = i \right)}{t} \right] \tag{2}$$

Or it can be written as (3), shown at the top of the next page.

We employed the Hybrid Classifier to leverage the best features of both models. With the information in y, XGB will employ logistic regression to derive a probability function. Researchers observed that by employing a hybrid classifier, accuracy could be raised to 99.7 percent using Logistic Regression. Hybrid Model Classification Accuracy.

V. CONCLUSION

In conclusion, the proposed framework presents a holistic approach to revolutionizing the healthcare system by integrating cutting-edge technologies. The combination of edge

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

computing, distributed ledger technology, elliptic curve cryptography, and a hybrid machine learning model offers a comprehensive solution to enhance medical data security, patient privacy, and overall system performance. By leveraging elliptic curve cryptography-based identity-based cryptosystems, patient records are securely protected, ensuring data integrity and privacy preservation. The performance evaluation of the distributed ledger system indicates its potential to handle high transaction throughputs. The hybrid machine learning model's promising accuracy enhances the early detection and prediction capabilities, contributing to improved patient care. This multifaceted approach not only addresses the critical issues of dependability and data security but also fosters efficient and rapid information exchange among healthcare stakeholders. The integration of edge computing further enhances response times and network security. With the ever-increasing importance of data in healthcare, this framework holds the promise of significantly improving medical services, patient outcomes, and the overall healthcare ecosystem while providing a robust foundation for future research and development in the field.

ACKNOWLEDGMENT

This research is supported via funding from Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R333), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] J. S. Raj, "Optimized mobile edge computing framework for IoT based medical sensor network nodes," *March*, vol. 3, no. 1, pp. 33–42, May 2021, doi: 10.36548/jucct.2021.1.004.

[2] S. Sureddy, K. Rashmi, R. Gayathri, and A. S. Nadhan, "Flexible deep learning in edge computing for Internet of Things," *Int. J. Pure Appl. Math.*, vol. 119, no. 10, pp. 1–12, 2018.

[3] S. Hakak, S. Ray, W. Z. Khan, and E. Scheme, "A framework for edge-assisted healthcare data analytics using federated learning," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2020, pp. 3423–3427, doi: 10.1109/BigData50022.2020.9377873.

[4] A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial intelligence-driven mechanism for edge computing-based industrial applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4235–4243, Jul. 2019, doi: 10.1109/TII.2019.2902878.

[5] E. Laxmi Lydia, C. S. S. Anupama, A. Beno, M. Elhoseny, M. D. Alshehri, and M. M. Selim, "Cognitive computing-based COVID-19 detection on Internet of Things-enabled edge computing environment," *Soft Comput.*, vol. 2021, pp. 1–12, Nov. 2021, doi: 10.1007/s00500-021-06514-6.

[6] M. Hartmann, U. S. Hashmi, and A. Imran, "Edge computing in smart health care systems: Review, challenges, and research directions," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3710, Mar. 2022, doi: 10.1002/ett.3710.

[7] P. Verma, R. Tiwari, W.-C. Hong, S. Upadhyay, and Y.-H. Yeh, "FETCH: A deep learning-based fog computing and IoT integrated environment for healthcare monitoring and diagnosis," *IEEE Access*, vol. 10, pp. 12548–12563, 2022, doi: 10.1109/ACCESS.2022.3143793.

[8] M. Kumar S and D. Majumder, "Healthcare solution based on machine learning applications in IoT and edge computing," *Int. J. Pure Appl. Math.*, vol. 119, pp. 1473–1784, Jul. 2020.

[9] V. Hayyolalam, M. Aloqaily, Ö. Özkasap, and M. Guizani, "Edge intelligence for empowering IoT-based healthcare systems," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 6–14, Jun. 2021, doi: 10.1109/MWC.001.2000345.

[10] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An energy-efficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, pp. 11404–11419, 2022, doi: 10.1109/ACCESS.2022.3146295.

[11] A. Shifa, M. Naveed Asghar, A. Ahmed, and M. Fleury, "Fuzzy-logic threat classification for multi-level selective encryption over real-time video streams," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5369–5397, Nov. 2020, doi: 10.1007/s12652-020-01895-2.

[12] S. Nawaz, M. Tariq, S. Shah, and A. Iqbal, "Internet of Things (IoT) security and privacy," *J. Tianjin Univ. Sci. Technol.*, vol. 56, pp. 23–38, Mar. 2023, doi: 10.17605/OSF.IO/T8YCW.

[13] A. Rehman, S. Abdullah, M. Fatima, M. W. Iqbal, K. A. Almarhabi, M. U. Ashraf, and S. Ali, "Ensuring security and energy efficiency of wireless sensor network by using blockchain," *Appl. Sci.*, vol. 12, no. 21, p. 10794, Oct. 2022, doi: 10.3390/app122110794.

[14] A. Ahmed, S. Abdullah, S. Iftikhar, I. Ahmad, S. Ajmal, and Q. Hussain, "A novel blockchain based secured and QoS aware IoT vehicular network in edge cloud computing," *IEEE Access*, vol. 10, pp. 77707–77722, 2022, doi: 10.1109/ACCESS.2022.3192111.

[15] *IoT-Fog-Based Healthcare 4.0 System Using Blockchain Technology | SpringerLink*. Accessed: Sep. 13, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11227-022-04788-7

[16] I. Ahmad, S. Abdullah, M. Bukhsh, A. Ahmed, H. Arshad, and T. F. Khan, "Message scheduling in blockchain based IoT environment with additional fog broker layer," *IEEE Access*, vol. 10, pp. 97165–97182, 2022, doi: 10.1109/ACCESS.2022.3205592.

[17] S. Abdullah, M. N. Asghar, M. Ashraf, and N. Abbas, "An energy-efficient message scheduling algorithm with joint routing mechanism at network layer in Internet of Things environment," *Wireless Pers. Commun.*, vol. 111, no. 3, pp. 1821–1835, Apr. 2020, doi: 10.1007/s11277-019-06959-x.

[18] *Detection and Prevention COVID-19 Patients Using IoT and Blockchain Technology | SpringerLink*. Accessed: Sep. 13, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-19968-4_10

[19] M. A. Ejaz, "Intelligent video encoder selection system for smart devices," *Pakistan J. Sci.*, vol. 70, no. 2, p. 2, 2018, doi: 10.57041/pjs.v70i2.167.

[20] S. Shah, A. Jaffar, S. Nawaz, W. Arshad, and A. Iqbal, "Early detection and classification of breast cancer using machine learning and deep learning techniques," *Tianjin DaxueXuebao/J. Tianjin Univ. Sci. Technol.*, vol. 55, pp. 102–120, Jul. 2022, doi: 10.17605/OSF.IO/9FYTS.

[21] S. Abdullah, M. N. Asghar, M. Fleury, and Z. Mushtaq, "Network-coding-enabled and QoS-aware message delivery for wireless sensor networks," *Wireless Pers. Commun.*, vol. 132, no. 1, pp. 329–359, Sep. 2023, doi: 10.1007/s11277-023-10613-y.

[22] S. Iftikhar, "A supervised feature selection method for malicious intrusions detection in IoT based on genetic algorithm," *Int. J. Comput. Sci. Netw. Secur.*, vol. 23, no. 3, p. 49, Mar. 2023.

[23] S. M. Gillani, M. N. Asghar, A. Shifa, S. Abdullah, N. Kanwal, and M. Fleury, "VQProtect: Lightweight visual quality protection for error-prone selectively encrypted video streaming," *Entropy*, vol. 24, no. 6, p. 755, May 2022, doi: 10.3390/e24060755.

[24] M. Bukhsh, S. Abdullah, A. Rahman, M. N. Asghar, H. Arshad, and A. Alabdulatif, "An energy-aware, highly available, and fault-tolerant method for reliable IoT systems," *IEEE Access*, vol. 9, pp. 145363–145381, 2021, doi: 10.1109/ACCESS.2021.3121033.

[25] M. Bukhsh, S. Abdullah, and I. S. Bajwa, "A decentralized edge computing latency-aware task management method with high availability for IoT applications," *IEEE Access*, vol. 9, pp. 138994–139008, 2021, doi: 10.1109/ACCESS.2021.3116717.

[26] A. Rehman, M. A. Qureshi, T. Ali, M. Irfan, S. Abdullah, S. Yasin, U. Draz, A. Glowacz, G. Nowakowski, A. Alghamdi, A. A. Alsulami, and M. Węgrzyn, "Smart fire detection and deterrent system for human savior by using Internet of Things (IoT)," *Energies*, vol. 14, no. 17, p. 5500, Sep. 2021, doi: 10.3390/en14175500.

[27] S. Tuli, F. Mirhakimi, S. Pallewatta, S. Zawad, G. Casale, B. Javadi, F. Yan, R. Buyya, and N. R. Jennings, "AI augmented edge and fog computing: Trends and challenges," *J. Netw. Comput. Appl.*, vol. 216, Jul. 2023, Art. no. 103648, doi: 10.1016/j.jnca.2023.103648.

[28] K. M. Hosny, A. I. Awad, M. M. Khashaba, M. M. Fouda, M. Guizani, and E. R. Mohamed, "Enhanced multi-objective gorilla troops optimizer for real-time multi-user dependent tasks offloading in edge-cloud computing," *J. Netw. Comput. Appl.*, vol. 218, Sep. 2023, Art. no. 103702, doi: 10.1016/j.jnca.2023.103702.

[29] Y. He, M. Yang, Z. He, and M. Guizani, "Computation offloading and resource allocation based on DT-MEC-assisted federated learning framework," *IEEE Trans. Cognit. Commun. Netw.*, early access, Jul. 26, 2023, doi: 10.1109/TCCN.2023.3298926.

[30] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for IoT communications," *IEEE Internet Things J.*, early access, Aug. 4, 2023, doi: 10.1109/JIOT.2023.3302065.

[31] J. Tang, J. Nie, Y. Zhang, Z. Xiong, W. Jiang, and M. Guizani, "Multi-UAV-Assisted federated learning for energy-aware distributed edge training," *IEEE Trans. Netw. Service Manage.*, early access, Jul. 24, 2023, doi: 10.1109/TNSM.2023.3298220.

[32] S. Abdelfattah, M. M. Badr, M. Mahmoud, K. Abualsaud, E. Yaacoub, and M. Guizani, "Efficient and privacy-preserving cloud-based medical diagnosis using an ensemble classifier with inherent access control and micro-payment," *IEEE Internet Things J.*, early access, Aug. 9, 2023, doi: 10.1109/JIOT.2023.3303429.

[33] R. A. Shah, M. N. Asghar, S. Abdullah, N. Kanwal, and M. Fleury, "SLEPX: An efficient lightweight cipher for visual protection of scalable HEVC extension," *IEEE Access*, vol. 8, pp. 187784–187807, 2020, doi: 10.1109/ACCESS.2020.3030608.

[34] K. M. Hosny, A. I. Awad, M. M. Khashaba, M. M. Fouda, M. Guizani, and E. R. Mohamed, "Optimized multi-user dependent tasks offloading in edge-cloud computing using refined whale optimization algorithm," *IEEE Trans. Sustain. Comput.*, early access, Jul. 11, 2023, doi: 10.1109/TSUSC.2023.3294447.

[35] Y. Chen, Q. Yang, S. He, Z. Shi, J. Chen, and M. Guizani, "FTPipeHD: A fault-tolerant pipeline-parallel distributed training approach for heterogeneous edge devices," *IEEE Trans. Mobile Comput.*, early access, Jun. 1, 2023, doi: 10.1109/TMC.2023.3272567.

[36] O. Wehbi, S. Arisdakessian, O. A. Wahab, H. Otrok, S. Otoum, A. Mourad, and M. Guizani, "FedMint: Intelligent bilateral client selection in federated learning with newcomer IoT devices," *IEEE Internet Things J.*, vol. 10, no. 23, pp. 20884–20898, Dec. 2023, doi: 10.1109/JIOT.2023.3283855.

[37] K. Li, X. Wang, Q. He, Q. Ni, M. Yang, and S. Dustdar, "Computation offloading for tasks with bound constraints in multiaccess edge computing," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15526–15536, Sep. 2023, doi: 10.1109/JIOT.2023.3264484.

[38] S. S. Tripathy, M. Rath, N. Tripathy, D. S. Roy, J. S. A. Francis, and S. Bebortta, "An intelligent health care system in fog platform with optimized performance," *Sustainability*, vol. 15, no. 3, p. 1862, Jan. 2023, doi: 10.3390/su15031862.

[39] S. Alsubai, M. Sha, A. Alqahtani, and M. Bhatia, "Hybrid IoT-edge-cloud computing-based athlete healthcare framework: Digital twin initiative," *Mobile Netw. Appl.*, vol. 2023, pp. 1–20, Aug. 2023, doi: 10.1007/s11036-023-02200-z.

[40] M. M. Kamruzzaman, I. Alrashdi, and A. Alqazzaz, "New opportunities, challenges, and applications of edge-AI for connected healthcare in Internet of Medical Things for smart cities," *J. Healthcare Eng.*, vol. 2022, pp. 1–14, Feb. 2022, doi: 10.1155/2022/2950699.

[41] F. Firouzi, S. Jiang, K. Chakrabarty, B. Farahani, M. Daneshmand, J. Song, and K. Mankodiya, "Fusion of IoT, AI, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 3686–3705, Mar. 2023, doi: 10.1109/JIOT.2022.3191881.

[42] V. Hayyolalam, M. Aloqaily, Ö. Özkasap, and M. Guizani, "Edge-assisted solutions for IoT-based connected healthcare systems: A literature review," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9419–9443, Jun. 2022, doi: 10.1109/JIOT.2021.3135200.

[43] S. Aminizadeh, A. Heidari, S. Toumaj, M. Darbandi, N. J. Navimipour, M. Rezaei, S. Talebi, P. Azad, and M. Unal, "The applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things," *Comput. Methods Programs Biomed.*, vol. 241, Nov. 2023, Art. no. 107745, doi: 10.1016/j.cmpb.2023.107745.

[44] S. A. Alamer, Q. M. Ilyas, M. Ahmad, and D. Irfan, "A metaphoric design of electronic medical record (EMR) for periodic health examination reports: An initiative to cloud's medical data analysis," *Int. J. Cloud Appl. Comput.*, vol. 12, no. 1, pp. 1–18, Jan. 2022, doi: 10.4018/ijcac.2022010110.

[45] Q. M. Ilyas, M. Ahmad, S. Rauf, and D. Irfan, "RDF query path optimization using hybrid genetic algorithms: Semantic web vs. data-intensive cloud computing," *Int. J. Cloud Appl. Comput.*, vol. 12, no. 1, pp. 1–16, Jan. 2022, doi: 10.4018/IJCAC.2022010101.

[46] M. W. Iqbal, G. F. Issa, M. Yousif, and M. Atif, "Detection and replay of distributed denial of service attacks in smart cities using a hybrid deep learning approach," in *Proc. Int. Conf. Bus. Anal. Technol. Secur. (ICBATS)*, Mar. 2023, pp. 1–7, doi: 10.1109/ICBATS57792.2023.10111332.

[47] Z. Lv and A. K. Singh, "Edge-Cloud-Based wearable computing for automation empowered virtual rehabilitation," *IEEE Trans. Autom. Sci. Eng.*, early access, Jul. 3, 2023, doi: 10.1109/TASE.2023.3289908.

[48] Z. Amiri, A. Heidari, M. Darbandi, Y. Yazdani, N. Jafari Navimipour, M. Esmaeilpour, F. Sheykhi, and M. Unal, "The personal health applications of machine learning techniques in the Internet of Behaviors," *Sustainability*, vol. 15, no. 16, p. 12406, Aug. 2023, doi: 10.3390/su151612406.

[49] A.-T. Shumba, T. Montanaro, I. Sergi, L. Fachechi, M. De Vittorio, and L. Patrono, "Leveraging IoT-aware technologies and AI techniques for real-time critical healthcare applications," *Sensors*, vol. 22, no. 19, p. 7675, Oct. 2022, doi: 10.3390/s22197675.

[50] Z. Wang, J. Hu, K. Yang, and K.-K. Wong, "Wideband waveforming for integrated data and energy transfer: Creating extra gain beyond multiple antennas and multiple carriers," *IEEE Trans. Wireless Commun.*, early access, Aug. 15, 2023, doi: 10.1109/TWC.2023.3303415.

MUHAMMAD IZHAR received the M.C.S. degree from COMSATS University Islamabad, Islamabad, Pakistan, in 2015, and the M.S. degree in CS from the University of South Asia, Lahore, Pakistan, in 2019. He is currently pursuing the Ph.D. degree in CS with the Department of Computer Science and Information Technology, Superior University Gold Campus, Lahore. He is a Subject Specialist in CS with the Government Higher Secondary School Fazilpur, Rajanpur District, Pakistan. His research interests include the IoT edge computing and machine learning.

SYED ASAD ALI NAQVI received the Ph.D. degree in computer science from Lancaster University, in 2015. He is currently with Superior University, Lahore, Pakistan, and the HOD of the Department of Information Technology. He has a number of publications in international high-ranked journals and conferences. His research interests include cyber security, risk analysis, and mixed methods research. Security of data, internet, computer crime, computer games, cyber-physical systems, decision making, fault trees, and formal specification.

ADEEL AHMED received the master's degree in computer science from The Islamia University of Bahawalpur Pakistan, Pakistan, and the M.S. degree in computer sciences from the Virtual University of Pakistan. He is currently pursuing the Ph.D. degree with The Islamia University of Bahawalpur Pakistan. His main research interests include edge computing, the IoT systems, energy efficiency, fuzzy logic, wireless networks, and blockchain. He serves as a reviewer for international journals.

SAIMA ABDULLAH received the Ph.D. degree from the Department of Computer Science and Electronic Engineering, University of Essex, U.K. She is currently an Assistant Professor with the Department of Computer Science and Information Technology, The Islamia University of Bahawalpur Pakistan. She is a member with the Multimedia Research Group, DCS, where she has been involved in efficient and secure communication of multimedia data over future-generation network technologies. Her main research interests include wireless networks and communications, future internet technology, and network performance analysis. She has authored around ten articles in the above research areas. She serves as a reviewer for international journals.

NAZIK ALTURKI is currently an Esteemed Researcher affiliated with the Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. With a deep passion for advancing the field of information systems, she has made significant contributions in areas, such as data management, decision support systems, and information security. Her expertise lies in the application of data analytics and machine learning techniques to extract meaningful insights from large datasets. She is also dedicated to exploring the challenges and opportunities presented by emerging technologies, including cloud computing, the Internet of Things (IoT), and blockchain. Her work has been published in prestigious journals and presented at international conferences, solidifying her reputation as a respected scholar. Furthermore, she actively participates as a reviewer for reputable academic journals, ensuring the high quality and rigor of scientific publications. Driven by her passion for research and her commitment to academic excellence, she continues to contribute to the field of information systems, making valuable contributions that advance knowledge and drive innovation. Her research interests include leveraging technology to enhance organizational processes and improve decision-making efficiency.

LEILA JAMEL (MENZLI) received the Engineering degree in computer sciences and the Ph.D. degree in computer sciences and information systems. She was the Program Leader of the IS Program and the ABET and NCAAA Accreditation Committees, CCIS, Princess Nourah bint Abdulrahman University (PNU), Saudi Arabia. She was the HOD of information systems security of the Premier Ministry of Tunisia. She is currently an Assistant Professor with the College of Computer and Information Sciences, PNU. She is a Researcher with the RIADI Laboratory, Tunisia. Her research interests include business process modeling, business process management/re-engineering and quality, context-awareness in business models, data sciences, ML, process mining, e-learning, and software engineering. She was a member of the Steering and Scientific Committees of the IEEE International Conference on Cloud Computing. She is a reviewer of many international journals and conferences.