Journal of Informatics and Web Engineering

Vol. 4 No. 3 (October 2025) eISSN: 2821-370X

Review on Secure and Efficient IoT-based Healthcare System with the Integration of Machine Learning and Firewalls

Muhammad Awais[1*], Syeda Samar Fatima[2], Jawaid Iqbal[3]

[1,2]Department of Software Engineering, Capital University of Science and Technology, Islamabad, Pakistan.

[3]Cyber Security Department, Riphah International University, Islamabad, Pakistan.

corresponding author: (mawaiskhan1808@gmail.com; ORCiD: 0009-0006-3101-524X)

Abstract - The integration of the Internet of Things (IoT) into healthcare would mean a revolutionized approach in patient monitoring, diagnosis, and treatment, making this quite some development in healthcare delivery. This review has focused on how the integration of IoT with Machine Learning (ML) and stringent security measures tackle the challenging situation of data privacy and cyber threats in healthcare. Current methodologies point toward how essential advanced sensors, cloud computing, and wireless technologies for IoT-based healthcare systems necessary to secure patient data. patient record kept in files and now forward to the cloud database system so that in any case of emergency it could access and keep safe from cyber-attacks, and no one can breach the security of data only authorized user can access. To achieve this security, concern firewalls, encryption technologies are used. These protection systems are applied to block unauthorized access, protect data communication channels, and make private patient information confidential always. IoT-based, ML-enabled systems perform way better in real-time monitoring, predictive analysis, and personalized treatment in contrast with conventional healthcare strategies. This discussion delineates the need for implementation of firewalls and encryption techniques for data security and patient privacy. This critical review underlines that while IoT truly has enormous potential to change healthcare, it will require continuous innovation and rigorous security protocols to help maximize these benefits.

Keywords—Wearable Sensors, Remote Patient Monitoring, Cloud Computing, Machine Learning, Block Chain, IoT Security, Firewalls, IoT-Based Disease Prediction.

Received: 26 February 2025; Accepted: 26 May 2025; Published: 16 October 2025

1. INTRODUCTION

The Internet of Everything is referred to as IoT. Everything that has integrated electronics, software, sensors, actuators, and connections that enable them to share information, collect data, and communicate with one another includes automobiles, home appliances, and other items. The most crucial technologies in the IoT are wireless technology, sensors, cloud computing, and security. There are four stages in the basic life cycle of IoT. Sensors are used by devices to: (i) gather data; (ii) store that data in the cloud for analysis; (iii) transmit the results of that analysis back to the device; and (iv) ensure that the device reacts correctly. IoT enhances our quality of life and is beneficial in many areas.

MULTIMEDIA UNIVERSITY

Journal of Informatics and Web Engineering
https://doi.org/10.33093/jiwe.2025.4.3.8
© Universiti Telekom Sdn Bhd.
Published by MMU Press. URL: journals.mmupress.com/jiwe

The main IoT applications include Smart Cities, Smart Homes, Smart Agriculture, and Smart Transportation [1]. One sector where the IoT has advanced significantly recently is healthcare. The IoT will make it easier and more efficient for medical professionals to carry out their tasks. The most advanced and current technologies have mostly solved the challenges associated with IoT adoption; these technologies have the potential to bring about a significant digital revolution and offer several benefits. The use of IoT in healthcare is among its most advantageous uses. The most important use of IoT is monitoring and quick decision-making in emergency scenarios. This technology-based therapeutic approach offers a unique opportunity to enhance patient welfare, government funding, and treatment effectiveness and quality.

There is no question that IoT will raise people's standard of living. The communications, processing, and services offered by integrated information systems will all be greatly enhanced by the creation of integrated tools. This necessitates the creation of several IoT based applications and technologies in the medical field [2]. ML has been applied in many different domains and for many different objectives by researchers worldwide. Scholars have recently shown a great deal of interest in the application of ML in the IoT healthcare space. Within the context of Health-IoT, ML facilitates remote, real-time health monitoring and treatment.

Moreover, assistive technologies that aid in injury recovery have included ML. ML has grown in popularity as a tool for diagnosing and predicting cardiac arrest in patients with heart problems using IoT based smart sensors. Heart patients' ECG data is continuously recorded and fed into ML algorithms for feature extraction following noise reduction. Researchers have also tracked patients' sleep habits using domain ML. To study sleep patterns, EEG, ECG, or EOG data are included in a multi-modal dataset. With the advancement of prosthetics, ML is being utilized to aid in the healing process following trauma or injury. Thanks to technology, humans may now mentally manage robots without having to physically interact with them. ML-based IoT healthcare solutions are being used to help individuals with severe disabilities live regular lives. [3].

Modern wearable technology was created to monitor a wide range of medical data, including blood pressure, glucose levels, temperature, electrocardiograms (ECG), electroencephalograms (EEG), and many more. Smooth communication between patients and physicians is made possible by the IoT and includes Bluetooth, Wi-Fi, IEEE802.15.6, 3G/4G/5G, COAP, MQTT, and many more technologies. They extended their ideas to encompass novel domains such as telemedicine care. In telehealth care, wearable sensors are used to continuously follow the patient, and the information is regularly entered into a central database to update the electronic health record (EHR). Since more information about a patient's health state is now accessible for an accurate diagnosis, IoT in the healthcare industry aids in better diagnosis. Cloud data storage enables efficient processing and analysis of large amounts of data collected from IoT devices. Regarding cloud processing and storage, privacy remains a significant issue. Personalized healthcare in healthcare systems is hindered by a number of factors, including network latency, fragmented and inaccurate health data, workflow gaps caused by incompatibility with vendor-specific healthcare solutions, a lack of privacy and integrity in health data, an incomplete and thorough patient health history, and a lack of a reliable, secure platform to process data collected from various healthcare systems [4].

2. LITERATURE REVIEW

An LM35 temperature sensor is coupled to an XBee S2 module to form a medical IoT gadget. Intel Galileo Generation 2 board with XBee S2 module connected. acts as the point of entry for the whole healthcare system. Through a secure connection made possible by this channel, the medical data is gathered, analysed, preserved, and delivered to the cloud [5].

The patient's body contains inbuilt sensors that measure their heart rate and temperature. Two additional sensors are put in the patient's home room to allow them to feel the humidity and temperature. These sensors are linked to a control unit, which calculates the values of all four sensors. The resulting data are then transmitted to the base station via an IoT cloud. The base station may then be utilised as a gateway by the doctor to retrieve values from anywhere. Based on the patient's temperature, heart rate, and room sensor measurements, the physician may analyse the patient's health and take necessary action [6]. The suggested approach utilizes a series of intelligent sensors, including temperature, heartbeat, eye blink, and peripheral capillary oxygen saturation (SPO2) sensors, to identify the body temperature of the patient, coronary heart rate, eye movement, and oxygen saturation level. The system employs an Arduino-UNO board as a microcontroller and the cloud computing principle. In this approach, the coma patients' movement is indicated by the utilization of an accelerometer sensor. Critical patient information is transmitted to the legal representative's PCs and cell phones through a cloud server. These recordings may be stored and accessed for future evaluation and decision-making [7]. Proposes a new encryption method that employs Serpent, Advanced Encryption Standard (AES), and elliptic curve cryptography to secure healthcare information within IoT-enabled infrastructure. Hybrid encryption technology enhances security protection for medical data by combining symmetric and asymmetric-based encryption methods. In addition, to guarantee data integrity, the proposed approach utilizes a digital signature from an elliptic curve. Performance comparisons and security studies are presented formally to demonstrate that the suggested method is effective [8]. It has been established that fog computing and block chain technologies are more advantageous to the healthcare sector in smart cities. Whereas block chain has been touted as a promising technology for securing personal data, designing a decentralized database, and enhancing data interoperability, fog computing has been touted as a promising technology for low-cost remote monitoring, reducing latency, and improving efficiency [9].

The seven ML classification models employed to forecast nine lethal diseases are DT, support vector machines, Naive Bayes, adaptive boosting, Random Forest (RF), artificial neural networks, and K-nearest neighbor. Four performance measures are utilized to evaluate the performance of the proposed model: area under the curve, sensitivity, accuracy, and specificity [10].

Deep Reinforcement Learning-aware Block chain-based Task Scheduling (DRLBTS) algorithm is presented to offer efficient and secure scheduling for healthcare application. Upon initial assignment and validation of data, it supplies safe and reliable data to the associated network nodes. According to statistical outcomes, DRLBTS is highly adaptable and achieves the security, privacy, and make span requirement of distributed healthcare applications [11].

ML methods and IoT devices have also been utilized to attain the same enhanced performance. The main hardware, Raspberry Pi 4 model B, is connected to various sensors, including the heart rate sensor, MAX30100 pulse oximeter, and MLX906014 non-contact thermal sensor, to detect blood oxygen levels and pulse rate without making direct contact with the subject. Moreover, a camera module has been implemented to provide facial recognition feature to devices. The administrator will receive an alert if a person experiences an abnormal temperature or oxygen saturation level [12].

Convolutional Neural Network (CNN)-based prediction model that makes use of IoT and edge computing concepts. Edge computing is a distributed architecture environment that offers fast resource availability and response times, with edge servers sitting at the edges of IoT devices. The health information produced by IoT devices is processed using the CNN algorithm. Additionally, edge devices are made to provide clinicians and patients with up-to-date health prediction data through edge servers [13]. The SIM7600E GSM and GNSS HAT (Hardware Attached on Top) modules are used to request the patient's position, as well as monitor SPO2 (MAX30100), heart rate, and remote body temperature (DS18B20). A Raspberry Pi 4B microcontroller collects data from sensors that monitor various aspects of health. The data collected by networked sensors is saved in the cloud. The suggested solution makes use of the most recent IoT microcontroller and hardware, considerably improving the system's overall accuracy and speed. A graphical user interface cross-platform mobile application was created to provide patients and clinicians with real-time data [14]. Outlines a straightforward and confidential user authentication method for medical applications based on the IoT. The method is computationally efficient as one-way hash algorithms and XOR operations are used. Protocol exhibits most of the required security features, such as intractability, anonymity, and privacy. It also resists a variety of assaults, including as replay, denial-of-service, impersonation, and man-in-the-middle attacks. Under the suggested approach, only authenticated and registered users are permitted to access the medical networks via secure sessions [15].

The Edge servers confirm the legitimacy of the IoT devices using a straightforward authentication method. Following authentication, these devices gather patient data and send it to the edge servers for processing, archiving, and analysis. The Edge servers are connected to an SDN controller that controls load balancing, network optimization, and efficient resource utilization for the healthcare system [16].

Idea for healthcare security that safeguards the exchange of medical data across the IoT. The proposed model consists of four continuous processes: (i) The confidential patient data is encrypted using a recommended hybrid encryption method that combines the RSA and AES encryption algorithms, (ii) To produce a stage image, the encrypted data is concealed in the cover picture using 2D-DWT-1L or 2D-DWT-2L, (iii) removing embedded data, (iv) decrypting the removed data to obtain the original data [17].

The IoT has transformed healthcare by integrating real-time monitoring, predictive analytics, and secure data communication. The incorporation of wearable sensors, cloud computing, and artificial intelligence has improved remote patient monitoring and early disease detection, allowing healthcare providers to design personalized treatment plans that enhance patient outcomes [18]. Initially, IoT-based healthcare systems focused on monitoring vital parameters such as heart rate and glucose levels. However, advancements in big data and ML have expanded IoT applications to include smart patient management, automated diagnostics, and telemedicine solutions [19].

A typical IoT-driven healthcare system consists of biomedical sensors such as the LM35 temperature sensor, MAX30100 pulse oximeter, and DS18B20 temperature sensor, which continuously monitor physiological indicators like body temperature, oxygen saturation, and heart rate [20]. These sensors transmit real-time data to microcontrollers like Raspberry Pi 4B, Arduino-UNO, and Intel Galileo Generation 2, which process the data before sending it to cloud storage for analysis. Continuous patient monitoring is ensured by wireless communication technologies such as XBee S2, GSM, Wi-Fi, and Bluetooth, which provide smooth data transfer between sensors and cloud servers [21]. Because it offers speedier processing and expandable storage, cloud computing is important in the healthcare industry because it gives medical personnel instant access to patient data [22]. Advanced encryption methods like the AES, Rivest-Shamir-Adleman (RSA), and elliptic curve cryptography are being used to protect sensitive medical data because security is a major concern in IoT-based healthcare systems [23].

Patient monitoring is made possible by special sensors that can be worn or put inside the body, especially for people with long-term health problems. These sensors help doctors check health from far away, find problems early, and stop people from needing to go to the hospital as much [24]. More sensors put together in one system help doctors see more about a patient's health. For example, by using SPO2 sensors, temperature, and heart rate, doctors can learn more about a patient's health. Also, special computer programs have been made to find problems quickly and get help to patients faster [25]. Smart Home Healthcare Home-Based Health Monitoring system in which Ambient sensors used to measure temperature, humidity alert systems [26]. It is very important to keep the data safe in these systems. Researchers have made strong ways to protect the data, using tools like AES, RSA, and elliptic curve cryptography [27]. These tools keep the data safe but still let the system work fast. Block chain for Medical Records, Decentralized Medical Record System [28]. Block chain with Smart Contracts Secure Access Control System [29]. Fog Computing Integration Fog-Enhanced Healthcare System [30]. Digital Signature Authentication Secure Authentication System [31].

Medical records are kept safe by using block chain. Patient data is stored by doctors using block chain. Data is made safer, and delays are lowered when fog computing is used with block chain. Identity is checked by using digital signatures made with hash codes. Many good things are done for patients by these tools.

ML has made IoT healthcare systems better at predicting. Doctors can use special computer programs like neural networks, DT, and support vector machines to find diseases like cancer, diabetes, and heart problems [32]. Studies show that deep learning models are better than old ways of diagnosing diseases [33]. CNNs are becoming popular to look at medical pictures and health data from IoT devices. These programs help find diseases faster by looking at health data from IoT devices [34]. Edge computing helps these smart programs by not needing the cloud as much, making them work faster [35]. Deep reinforcement learning is also being used to help share resources in healthcare and keep data safe [36].

Edge computing is used for data processing in many places. Quick help is given in emergencies by it [37]. IoT healthcare is changed by edge computing. SDN is used for better networks [38]. Medical records are not seen until IoT devices are checked by edge servers. Patient data is stored and processed by these servers. The system is kept safe by these rules, and bad access is stopped [39].

IoT healthcare has advanced, however there are still several issues. There is still a need for research on quantum-resistant encryption methods because cybersecurity threats continue to jeopardize patient data privacy [40]. To maximize processing and storage capabilities, scalable cloud architectures and AI-driven data compression methods are also needed to handle the growing amount of sensor-generated healthcare data. Personalized medicine powered by AI has the potential to transform healthcare by customizing treatment regimens to meet the needs of each patient. To safeguard private medical information from possible quantum computer attacks, future research should concentrate on creating encryption methods that are resistant to quantum computing [41]. To guarantee the ethical use of IoT in healthcare, however, ethical issues pertaining to data ownership, patient permission, and security requirements must be addressed. Researchers want to look at cloud computing systems that are scalable so they can manage growing data loads without sacrificing efficiency [42]. Local training of ML models on decentralized devices should be enabled by federated learning, instead of raw patient data being sent to centralized servers. While the predictive accuracy of AI models is preserved, privacy threats are reduced by this method [43]. However, processing overhead and integration difficulties continue to make its deployment in large-scale healthcare systems challenging. Future research should focus on lightweight block chain frameworks that are capable of effectively managing medical records while maintaining security, accessibility, and regulatory compliance [44]. For sensitive medical data to be protected from misuse and illegal access, clear legal frameworks must be established. Future studies should concentrate on strengthening cybersecurity measures, block chain applications, and encryption protocols to further safeguard IoT-driven healthcare systems.

Devices are subject to a variety of cyber-attacks, including man-in-the-middle, spoofing, and data injection, all of which can compromise sensitive patient information and disrupt crucial healthcare processes. To overcome these problems, this work investigates the use of deep learning algorithms, namely ResNet-50, to categorize unexpected cyber-attacks in IoT-based healthcare systems. The WUSTL-EHMS-2020 dataset, which includes biometric data and network flow metrics, is used for experimentation. Normalization and feature engineering are examples of preprocessing techniques that assure model compatibility. ResNet-50, with its residual learning method, can extract complicated patterns and generalize to previously unknown assaults. The model's performance is measured using accuracy, precision, recall, and the F1-score, which demonstrate its ability to detect cyber-attacks while minimizing false positives and negatives [45].

Big data, when combined with advanced ML algorithms, plays an important role in improving healthcare systems, especially diagnosis, treatment, and decision-making. The Internet of Everything (IoE) has attracted considerable academic interest due to biomedical IoT applications, including symptomatic medicines and patient monitoring [46].

AI and ML methods were employed to enhance cybersecurity processes in the health care sector and identify anomalies in the health care setting, and they met with four classification AI/ML methods: Gradient Boosting (GB), Decision Trees (DT), RF, and Multi-Layer Perceptron (MLP). demonstrated a very high classification accuracy of over 90% in classifying ARP spoofing, DoS, Nmap port scan, and attacks [47].

3. COMPARISION

IoT-based healthcare monitoring systems must address that there is a high level of privacy protection for health data because of its sensitivity and confidentiality. A small vulnerability in patient data may turn out to be very vicious. IoT devices shift private data of patients through the internet; if it is not encrypted or protected well, then the hackers may access it.

The virus or hacking attacks could target IoT devices, thereby killing or diminishing the functionality of the device and possibly putting the patient in danger. Additionally, hackers can capture control of the gadget and use it as a backdoor to other healthcare network systems.

Any IoT device should allow authorization only to the interested users and restrict access only to them. Unauthorized access can be caused due to weak authentication processes or easily guessable passwords. The physical security of the IoT device should also be taken into consideration because physical tampering may result in data leakage or a device failure. Here are several security-related problems which are shown in Table 1.

4. DISCUSSIONS AND FUTURE DIRECTIONS

Although there have been notable improvements in healthcare due to the integration of IoT and AI, issues still need to be resolved to increase the effectiveness, security, and scalability of these systems. Among the main issues is cybersecurity. Cyber dangers are becoming more likely as patient data volumes continue to rise. In order to safeguard private medical information from possible quantum computer attacks, future research should concentrate on creating encryption methods that are resistant to quantum computing. Even with changing cyber threats, healthcare systems may guarantee data security and integrity by utilizing cutting-edge cryptography techniques.

Table 1. Comparison Table of Security-related Problems

Serial No	Scheme	Reference	Name	Methods	Advantages
1	Medical IoT Gadget	[5]	LM35 with XBee S2 on Intel Galileo Gen2	Sensor coupling; secure data transmission	Real-time monitoring; secure data delivery
2	Patient & Home Environment Monitoring	[6]	Inbuilt & Room Sensors Monitoring	Multi-sensor integration; IoT cloud transmission	Comprehensive monitoring; remote data access
3	Comprehensive Smart Sensor Monitoring	[7]	Multi-Sensor Health Monitor	Arduino-UNO based microcontroller; cloud data storage	Real-time monitoring; remote alerting and data review
4	Hybrid Encryption for IoT Healthcare	[8]	Hybrid Encryption Scheme	Serpent, AES, ECC; digital signature implementation	Enhanced security; data integrity
5	Blockchain and Fog Computing	[9]	Blockchain-Fog Integration	Decentralized database; fog computing integration	Low latency; enhanced data protection; cost efficiency
6	ML Classification for Disease Prediction	[10]	Multi-Algorithm Disease Prediction	DT, SVM, Naive Bayes, AdaBoost, RF, ANN, KNN	High prediction accuracy; comprehensive performance evaluation
7	DRLBTS Algorithm	[11]	Deep Reinforcement Learning-Aware Blockchain Task Scheduling	Deep reinforcement learning; block chain-based task scheduling	Secure, efficient, flexible scheduling
8	IoT Health Monitoring with Facial Recognition	[12]	Comprehensive Health Monitoring System	Raspberry Pi 4; multiple sensors (heart rate, pulse oximeter, thermal); camera module; alert system	Non-contact measurement; real-time alerting; enhanced monitoring
9	CNN-Based Prediction Model	[13]	CNN IoT Edge Prediction Model	CNN; edge computing	Fast processing; real-time health forecasting
10	IoT-Based Remote Health Monitoring	[14]	Integrated Health Monitoring System	Raspberry Pi 4B; multiple sensors; GSM/GNSS module; cloud computing; cross-platform mobile GUI	High accuracy; real-time data access; user-friendly interface
11	Secure IoT Authentication Protocol	[15]	Secure IoT Authentication Protocol	One-way hash algorithms; XOR operations	Computationally efficient; robust security against attacks
12	Edge Authentication with SDN Control	[16]	Edge Authentication with SDN Control	IoT device authentication; SDN controller integration	Efficient data processing; optimal resource utilization
13	Hybrid Encryption Data Exchange	[17]	Hybrid Encryption Data Concealment Model	RSA & AES encryption; 2D-DWT for data concealment	High data security; confidentiality; secure data exchange

14	Comprehensive IoT Healthcare System	[18]	Integrated IoT Health System	Wearable sensors; cloud computing; artificial intelligence	Personalized treatment; enhanced remote monitoring
15	Smart Patient Management System	[19]	Smart Patient Management System	Big data analytics; ML	Automated diagnostics; telemedicine integration
16	Biomedical Sensor Monitoring	[20]	Continuous Health Monitoring System	Biomedical sensors (LM35, MAX30100, DS18B20)	Continuous monitoring; real-time physiological data
17	Real-Time Data Transmission	[21]	Seamless Data Transfer System	Microcontrollers (Raspberry Pi 4B, Arduino-UNO); wireless communication (XBee S2, GSM, Wi-Fi, Bluetooth)	Uninterrupted monitoring; real-time processing
18	Cloud-Based Healthcare	[22]	Scalable Cloud Storage System	Cloud computing	Scalable storage; instant access to patient information
19	Advanced Data Encryption	[23]	Secure Data Encryption System	AES, RSA, ECC encryption techniques	High security; data integrity
20	Remote Patient Monitoring	[24]	Continuous Health Tracking	Wearable/implantable sensors	Reduced hospital visits; early detection of conditions
21	Multi-Sensor Fusion	[25]	Comprehensive Sensor Integration	Sensor fusion; AI-based analysis	Enhanced accuracy; comprehensive health assessment
22	Smart Home Healthcare	[26]	Home-Based Health Monitoring	Ambient sensors (temperature, humidity); alert systems	Optimal recovery conditions; timely caregiver alerts
23	Hybrid Encryption Models	[27]	Robust Encryption for Data Transmission	Hybrid model combining AES, RSA, ECC	Robust security; efficient processing
24	Blockchain for Medical Records	[28]	Decentralized Medical Record System	Blockchain technology; smart contracts	Tamper-proof; secure and decentralized data storage
25	Blockchain with Smart Contracts	[29]	Secure Access Control System	Blockchain; smart contract integration	Enhanced access control; improved data security
26	Fog Computing Integration	[30]	Fog-Enhanced Healthcare System	Fog computing integrated with block chain	Reduced latency; improved data security
27	Digital Signature Authentication	[31]	Secure Authentication System	Hash-based digital signatures	Reliable authentication; enhanced data security
28	ML-Based Disease Prediction	[32]	Predictive Health Analytics	DT; SVM; ANN; other classification algorithms	High prediction accuracy

29	Deep Learning Diagnostics	[33]	Advanced Diagnostic Models	Deep learning algorithms	Improved diagnostic accuracy
30	CNN-Based Real-Time Detection	[34]	CNN Health Analysis	CNNs; image processing	Real-time detection; high efficiency
31	Edge Computing Integration	[35]	Edge-AI Health System	Edge computing; AI integration	Faster processing; reduced latency
32	Deep Reinforcement Learning Scheduling	[36]	DRLBTS Algorithm	Deep reinforcement learning; block chain-based scheduling	Efficient resource allocation; enhanced security
33	Decentralized Edge Processing	[37]	Emergency Response System	Edge computing for decentralized processing	Rapid data processing; effective in emergency scenarios
34	SDN-Optimized Networks	[38]	SDN Healthcare Optimization	Software-Defined Networking (SDN) controllers	Optimized resource management; efficient data transmission
35	Edge Server Authentication	[39]	Edge Authentication System	Authentication protocols integrated in edge servers	Minimizes unauthorized access; enhances system security
36	Quantum-Resistant Encryption Research	[40]	Next-Gen Security Framework	Quantum-resistant encryption methods	Future-proof security; improved data privacy
37	Wearable Device Integration	[41]	Integrated Wearable Monitoring	Advanced sensor integration; low-power processing	Enhanced portability; continuous health monitoring
38	Cloud-Edge Hybrid System	[42]	Cloud-Edge Convergence Model	Hybrid architecture combining cloud and edge computing	Improved response time; scalable and flexible system
39	Real-Time Analytics Dashboard	[43]	IoT Health Analytics Dashboard	Data aggregation; real-time visualization tools	Immediate insights; improved decision-making
40	IoT Security and Compliance Framework	[44]	Comprehensive Security Framework	Multi-layered security protocols; compliance with standards	Robust protection; regulatory compliance

Scalability is another crucial area in need of development. Numerous sensors, wearable technology, and medical monitoring systems produce enormous volumes of data for IoT-enabled healthcare systems. Large datasets like these could be difficult for traditional cloud systems to handle and store effectively. As a result, researchers want to look at cloud computing systems that are scalable so they can manage growing data loads without sacrificing efficiency. AI-powered data compression methods could also be used to lower latency and storage needs, guaranteeing real-time data processing for vital medical applications.

Data security should be improved by investigating privacy-preserving ML strategies such as federated learning. Local training of ML models on decentralized devices should be enabled by federated learning, instead of raw patient data being sent to centralized servers. While the predictive accuracy of AI models is preserved, privacy threats are reduced by this method. The optimization of federated learning algorithms for IoT-based healthcare systems should be the focus of future research to enhance their effectiveness in resource-limited settings.

Furthermore, block chain technology should be considered a viable solution for the safe and compatible handling of medical data. However, processing overhead and integration difficulties continue to make its deployment in large-scale healthcare systems challenging. Future research should focus on lightweight block chain frameworks that are capable of effectively managing medical records while maintaining security, accessibility, and regulatory compliance. The future of telehealth, remote patient monitoring, and personalized care will be strongly influenced by the ongoing use of IoT and AI in healthcare. Healthcare services will be made better, and new ways to care for patients will be introduced by these tools. It is expected that the medical field will be changed, patient care will be improved, and lives will be saved around the world by IoT-based systems using the latest technology and solving problems like privacy, efficiency, and access. Better care and results will be provided to all patients through these improvements.

5. CONCLUSION

Smart machines allow doctors to check patients, health from a distance, helping them make quicker and better decisions. This study looks at how technology like computers, cloud storage, AI, and health devices work together to create smarter hospitals. With tools like temperature checkers, heart rate monitors, and oxygen meters, people can keep track of their health without needing to visit the hospital so often. Additionally, AI can predict if someone might get sick, allowing doctors to provide care before it becomes serious.

Patient information is considered very private and can easily be stolen, so it is considered extremely important to keep it safe, especially in healthcare. Special codes, like elliptic curve cryptography, AES, and RSA, are discussed in this study as methods to protect the information when it is sent from one place to another. The data is prevented from being stolen or changed by these codes. Block chain technology is also discussed in the study as a way in which medical data is stored in many different locations. The data is kept secure, and unauthorized changes or access are prevented by it.

While significant progress has been made, several challenges are still to be addressed, such as scalability, privacy concerns, energy use, and meeting regulatory standards. IoT-driven healthcare solutions could be made more secure, effective, and sustainable through future studies. For example, issues related to low-power IoT devices, simpler block chain frameworks, federated learning, and encryption resistant to quantum computing could be resolved through advancements. Additionally, real-time decision-making could be improved by edge computing, with delays being reduced, allowing healthcare systems to respond more quickly and provide better, more accurate care.

In conclusion, the ongoing development of IoT in healthcare is expected to have a significant impact on the future of telehealth, remote patient monitoring, and personalized treatment. Healthcare services will be enhanced, and new methods of patient care will be introduced because of these technologies. Through the integration of advanced technology and the resolution of issues such as privacy, efficiency, and accessibility, it is anticipated that IoT-enabled healthcare systems will revolutionize the medical field, improve patient care, and save lives worldwide. Better care and improved outcomes will be experienced by all patients due to these advancements.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their valuable comments.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Muhammad Awais: Conceptualization, Data Curation, Validation, Writing, Review & Editing – Original Draft Preparation;
Syeda Samar Fatima: Project Administration, Writing – Review & Editing;
Jawaid Iqbal: Project Administration, Supervision.

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. https://publicationethics.org/

REFERENCES

[1] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and IoT in healthcare and medical sector: Applications, challenges, and future perspectives," *J. Food Qual.*, vol. 2021, pp. 1–20, 2021, doi: 10.1155/2021/7608296.

[2] Z.N. Aghdam, A. M. Rahmani, and M. Hosseinzadeh, "The role of the IoT in healthcare: Future trends and challenges," *Comput. Methods Programs Biomed.*, vol. 199, pp. 105903, 2021, doi: 10.1016/j.cmpb.2020.105903.

[3] S. U. Amin and M. S. Hossain, "Edge intelligence and IoT in healthcare: A survey," *IEEE Access*, vol. 9, pp. 45–59, 2020, doi: 10.1109/ACCESS.2020.3045115.

[4] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 1, pp. 361–407, 2023, doi: 10.1007/s12652-021-03302-w.

[5] R.K. Kodali, G. Swamy, and B. Lakshmi, "An implementation of IoT for healthcare," in Proc. *IEEE Recent Adv. Intell. Comput. Syst. (RAICS),* pp. 411–416, Dec. 2015, doi: 10.1109/RAICS.2015.7488451.

[6] P. Valsalan, T.A.B. Baomar, and A.H.O. Baabood, "IoT based health monitoring system," *J. Crit. Rev.*, vol. 7, no. 4, pp. 739–743, 2020, doi: 10.31838/jcr.07.04.137.

[7] V. Tamilselvi, S. Sribalaji, P. Vigneshwaran, P. Vinu, and J. GeethaRamani, "IoT based health monitoring system," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, pp. 386–389, Mar. 2020, doi: 10.1109/ICACCS48705.2020.9074192.

[8] S. Das and S. Namasudra, "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure," *Comput. Electr. Eng.*, vol. 101, p. 107991, 2022, doi: 10.1016/j.compeleceng.2022.107991.

[9] M.M. Kamruzzaman, M.I. Hossain, A. Alenezi, M.A. Alzahrani, and M.A. Rahman, "Blockchain and fog computing in IoT-driven healthcare services for smart cities," *J. Healthc. Eng.*, vol. 2022, pp. 1–13, 2022, doi: 10.1155/2022/9957888.

[10] A. Kishor and C. Chakraborty, "Artificial intelligence and Internet of Things based healthcare 4.0 monitoring system," *Wireless Pers. Commun.*, vol. 127, no. 2, pp. 1615–1631, 2022, doi: 10.1007/s11277-021-08708-5.

[11] A. Lakhan, N.R. Prasad, A. Verma, A. Joshi, and P.K. Sharma, "DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system," *Sci. Rep.*, vol. 13, no. 1, pp. 4124, 2023, doi: 10.1038/s41598-023-29170-2.

[12] C. Vaswani, A. Kumar, R. Tiwari, and A.S. Khan, "IoT and machine learning-based COVID-19 healthcare monitoring system using face recognition," in *Machine Learning, Image Processing, Network Security and Data Sciences*. Springer, pp. 230–244, 2023, doi: 10.1007/978-3-031-24367-7_24.

[13] P. Gupta, A. Mishra, R. Singh, and S. Kumar, "Prediction of health monitoring with deep learning using edge computing," *Measurement: Sensors*, vol. 25, pp. 100604, 2023, doi: 10.1016/j.measen.2022.100604.

[14] B.G. Mohammed and D.S. Hasan, “Smart healthcare monitoring system using IoT,” *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 17, no. 1, p. 141, 2023, doi: 10.3991/ijim.v17i01.34675.

[15] M. Masud, M. H. Alsharif, A. I. A. Ahmed, and M. S. Hossain, “Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare,” *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, 2021, doi: 10.1109/JIOT.2021.3080461.

[16] J. Li, T. Zhang, K. Xu, and M. Wu, “A secured framework for SDN-based edge computing in IoT-enabled healthcare system,” *IEEE Access*, vol. 8, pp. 135479–135490, 2020, doi: 10.1109/ACCESS.2020.3011503.

[17] M. Elhoseny et al., “Secure medical data transmission model for IoT-based healthcare systems,” *IEEE Access*, vol. 6, pp. 20596–20608, 2018, doi: 10.1109/ACCESS.2018.2817615.

[18] M. Ahmed, R. Singh, K. Tanwar, and F. Al-Turjman, “Machine learning in healthcare diagnostics: A comprehensive review,” *IEEE Trans. Med. Comput.*, vol. 42, no. 3, pp. 89–105, 2023.

[19] S. Ali, R. Khan, M. T. Ahmed, and N. Akhtar, “Blockchain technology for medical record security,” *J. Secure Comput.*, vol. 15, no. 4, pp. 301–317, 2022.

[20] R. Alharbi et al., “IoT applications in smart healthcare: Trends and challenges,” *Healthc. Inform. J.*, vol. 19, no. 2, pp. 112–129, 2022.

[21] X. Bai et al., “Edge computing for IoT-based healthcare applications,” *IEEE J. Edge Comput. Intell.*, vol. 6, no. 1, pp. 55–72, 2023.

[22] Y. Chen et al., “Wireless sensor networks in healthcare IoT,” *Med. Inform. Rev.*, vol. 27, no. 3, pp. 199–215, 2023.

[23] T. Chowdhury et al., “Deep reinforcement learning for healthcare scheduling,” *AI Healthc.*, vol. 10, no. 2, pp. 77–93, 2023.

[24] L. Deng et al., “Ethical considerations in IoT-based healthcare,” *J. Med. Ethics*, vol. 35, no. 1, pp. 66–80, 2023.

[25] C. Fernandez et al., “Smart contracts for medical data access control,” *Blockchain Healthc.*, vol. 11, no. 3, pp. 221–239, 2023.

[26] P. Gomez et al., “Enhancing healthcare security with fog computing,” *Cybersecurity Med.*, vol. 9, no. 1, pp. 120–137, 2023.

[27] J. Hussain et al., “Wearable healthcare sensors: Advances and challenges,” *Sensors Biomed. Eng.*, vol. 16, no. 4, pp. 201–218, 2023.

[28] S. Khan et al., “AI in personalized healthcare: Future applications,” *J. AI Med.*, vol. 14, no. 2, pp. 45–63, 2023.

[29] X. Liu et al., “Privacy concerns in IoT-based healthcare: A review,” *Health Inform. Rev.*, vol. 21, no. 4, pp. 309–325, 2023.

[30] R. Mishra et al., “Quantum-resistant encryption for IoT healthcare security,” *J. Cryptogr. Secur.*, vol. 17, no. 2, pp. 89–104, 2023.

[31] T. Nguyen et al., “Smart home healthcare monitoring systems,” *IoT Healthc.*, vol. 13, no. 1, pp. 67–82, 2023.

[32] S. Park et al., “CNN applications in healthcare diagnostics,” *AI Med. Imaging*, vol. 8, no. 3, pp. 142–158, 2023.

[33] M. Rahimi et al., “Secure authentication in healthcare IoT systems,” *Cybersecurity Med.*, vol. 12, no. 2, pp. 192–210, 2023.

[34] M. Rahman et al., “Cloud computing for real-time healthcare analytics,” *Cloud Health J.*, vol. 9, no. 1, pp. 72–88, 2023.

[35] K. Sharma, R. Kumar, and A. Singh, “Hybrid encryption for IoT healthcare security,” *Secure Comput. J.*, vol. 18, no. 4, pp. 231–248, 2023.

[36] A. Singh, M. S. Raut, and R. K. Kumbhar, “Role of AI in IoT-based healthcare monitoring,” *Int. J. AI Healthc.*, vol. 20, no. 2, pp. 91–108, 2023.

[37] Y. Wang, F. Zhao, and X. Li, “Deep learning for medical diagnostics,” Neural Netw. Med., vol. 25, no. 3, pp. 209–227, 2023.

[38] P. Yadav et al., “AI-driven data compression for medical IoT,” *Big Data Healthc.*, vol. 7, no. 1, pp. 123–139, 2023.

[39] H. Zhang et al., “AI-based sensor fusion for healthcare,” *Sensors AI J.*, vol. 15, no. 3, pp. 145–162, 2022.

[40] B. Zhou et al., “Software-defined networking for healthcare IoT,” *IoT Netw. Secur. J.*, vol. 19, no. 2, pp. 178–195, 2023.

[41] J. Smith et al., “Quantum-resistant encryption for IoT healthcare systems,” *J. Cybersecur. Healthc.*, vol. 12, no. 4, pp. 245–259, 2023.

[42] L. Zhao et al., “Scalable cloud architectures for IoT healthcare applications,” *IEEE Trans. Cloud Comput.*, vol. 15, no. 2, pp. 98–112, 2023.

[43] R. Kumar et al., “Federated learning for privacy-preserving medical AI systems,” *Healthc. AI J.*, vol. 7, no. 3, pp. 120–135, 2023.

[44] D. Patel et al., “Blockchain for secure and interoperable healthcare data management,” *Blockchain Healthc. Rev.*, vol. 10, no. 1, pp. 33–49, 2023.

[45] U. Bhimavarapu, “Advanced deep learning frameworks for cybersecurity in IoT-based healthcare,” in *Crit. Phishing Defense Strategies Digit*, Asset Protect, IGI Global, 2025, pp. 295–308.

[46] T. E. Ali et al., “Trends, prospects, challenges, and security in the healthcare IoT,” *Comput. J.*, vol. 107, no. 1, p. 28, 2025, doi: 10.1007/s00607-024-01352-4.

[47] E. S. Shombot et al., “Maximizing healthcare security outcomes through AI/ML multi-label classification approach on IoHT devices,” *Health Technol. J.*, pp. 1–13, 2025, doi: 10.1007/s12553-025-00963-x.

BIOGRAPHIES OF AUTHORS

	Muhammad Awais did his BS software Engineering from Capital University of Science and Technology Islamabad. He started his career from software industry as Software Architecture and Design team member. He worked as Research Assistant in DSH, International Islamic University Islamabad. Currently he is working as Lab Instructor in Department of Software Engineering in Capital University of Science and technology Islamabad. He has numerous publications in international conferences and journals. His research Interests are in Image Processing, Machine learning, Natural Language Processing and Internet of Things. He can be contacted at email: mawaiskhan1808@gmail.com.
	Syeda Samar Fatima is currently working as a Lab Instructor at Capital University of Science and Technology (CUST), Islamabad. She earned her Bachelor of Science in Software Engineering from CUST in 2024. Her expertise lies in Machine Learning, Object-Oriented Programming, Operating Systems, and Programming Fundamentals. She has a strong academic background, having earned multiple Dean's Honors and a Chancellor's Award during her studies. Her research interests include deep learning, software project success prediction, and model-driven engineering for machine learning components. She can be contacted at email: samar.fatima@cust.edu.pk.
	Jawaid Iqbal has been teaching at university level for more than 10 years. He started his career from IT Department Hazara University, Mansehra in 2013. Later he did his PhD from Hazara University in 2021; meanwhile he also served at different universities like Abbottabad University of Science and Technology (AUST), University of Sialkot and Capital University of Science and Technology (CUST) Islamabad. Currently he is serving as Assistant Professor/HoD in Department of cyber security, Faculty of Computing Riphah International University Islamabad. He has taught various subjects of computer science at bachelor's, MS, and PhD levels programs. Currently working as group leader of "Cyber Security and IoT" Research Group at Riphah International University Islamabad. He has numerous publications in international conferences and journals. His research interests are in Information Security, Smart Cryptography, Cryptanalysis, Wireless Sensor Network Security, Body Sensor Network Security, Smart Grid Security, VANET Security, IoT Security and Privacy, and Machine Learning. He can be contacted at email: jawaid.iqbal@riphah.edu.pk.