Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 2958–2964

ENHANCED SECURITY MODEL FOR HEALTHCARE USING IOT SENSORS

Mukesh Kumar Bhardwaj [1], Manish Saraswat [1]

[1] Faculty of Science and Technology ICFAI University, Baddi, Himachal Pradesh, India

Corresponding Author

Mukesh Kumar Bhardwaj,
mukeshbhardwaj85@gmail.com

DOI
10.29121/shodhkosh.v5.i6.2024.6076

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

While cutting-edge technologies have revolutionized healthcare delivery and enabled transformative progress benefitting patients, operational efficiencies, and resource utilization, their widespread application and data-driven methods have introduced new complications endangering critical patient information's integrity, privacy, and availability. To tackle such threats, academics pushed for abbreviated processing periods, fortified security using cryptographic techniques to deter assaults, and energy-efficient algorithms minimizing energy expenditure during calculations. However, these frameworks continue experiencing prolonged processing, susceptibility to assaults, extravagant energy usage, and inadequate protection. The proposed model was tested using genuine patient health records amassed by IoT sensors and simulated diverse attack scenarios in Python to validate the suggested approach. The model strives to balance security, expediency, and conservation for a sustainable and trustworthy system. This paper evaluates the state of the arts related to security threats in Healthcare IoT and demonstrates significant improvements in the security and efficiency of the model.

Keywords: Security, Model, Healthcare, IOT Sensors

1. INTRODUCTION

The Internet of Things (IoT) has been a major trend in healthcare in recent years. It has made it possible to automate complex cardiology procedures, collect and analyse data continuously, monitor patients remotely, conduct risk-free remote surgeries, consult via telemedicine over long distances, and streamline general healthcare administration—all of which have a significant positive impact on patient outcomes and quality of life. However, the sensitive and invaluable patient health records residing in these systems, containing intimate details of one's medical history, are under persistent threat due to the expansive network of interconnected devices that enable the transmission of such vulnerable data to centralized servers for processing. Unfortunately, the very digital connectivity that empowers healthcare providers to better serve patients from afar simultaneously exposes the mission-critical infrastructure to nefarious threats seeking illegitimate access and exploitation of personal medical facts. Furthermore, healthcare has notably evolved into a prominent domain for industrial innovation, as IoT now pervades diverse medical sectors including blood glucose monitoring, diagnostic technologies, biometric signal analysis, and more, each providing innovative solutions but likewise multiplying interfaces that could potentially be breached to impair patient privacy and trust in the system. and electroencephalography, which are all tracked by several Internet of Things sensors and devices as well as medical

sensing devices [4,5]. To improve healthcare environments and overcome geographical barriers, the Internet of Things (IoT) is specifically used for automated manufacturing, remote monitoring, and giving current data to end users [6]. The Internet of Things (IoT) is particularly important in the healthcare industry because wearables, actuators, and sensors gather physiological data, such as heart rate, blood pressure, temperature, and electrocardiograms (ECGs) [7, 8]. Thus, a wide range of sectors employ the Internet of Things. An Internet of Things (IoT)-based healthcare system is shown in Figure 1, which also describes how the collected data is subsequently sent to nearby servers or devices. The crucial problem of scalability and capacity, however, faces IoT healthcare and leads to the generation of a lot of data in real-time applications while also cutting integration costs [9]. Since the security and safety of healthcare data are strongly correlated with the accurate identification of IoT devices [10], weak authentication gives hackers and intruders the chance to take advantage of the devices and produce bogus values [11].

The number of elderly people worldwide is growing at a rapid rate, which has increased the prevalence of chronic conditions like cancer, heart failure, diabetes, chronic respiratory diseases, stroke, hypertension, neurological disorders, asthma, autoimmune diseases, and osteoarthritis. As a result, there is a high demand for medical services from traditional healthcare systems. Smart healthcare is a result of the global scarcity of health professionals and the development of new technology, which has benefited the healthcare sector [12][13]. Wells and Usman [14] and Bu et al. [15] defined smart healthcare as a healthcare system that integrates and uses various emerging technologies to monitor patients and instantly access their medical information remotely, connect healthcare stakeholders, and automatically diagnose and detect diseases at an early stage. In SHSs, wearable or nonwearable sensors are implanted in patients to monitor and collect physiological data such as cardiac activity, pulse rate, blood pressure, electrocardiogram, temperature, heart rate, respiratory rate, oxygen volume in the body, activity level, and brain waves, which help in monitoring patients' health conditions or environmental data such as air quality, temperature, humidity, etc. [16]. To meet the needs of the medical ecosystem and facilitate simple decision-making and resource allocation, these physiological data and patient profiles are combined to form electronic health records, which are then stored in the cloud as medical cloud data [17]. Patients, healthcare providers, medical institutions, and other stakeholders can easily share this data. To improve patient outcomes by utilizing available resources, ambient control and wellness, safe and effective patient data management, telemedicine consultations, personalized patient treatment, real-time patient monitoring, and real-time medical data analysis, smart healthcare systems have been developed [18].

2. LITERATURE REVIEW

An increasing number of scientists have focused on cryptography algorithms based on optimization, in the literature to increase the safety and confidentiality of the health system. However, there are still certain problems to solve, such as high energy consumption, high cost of high calculation, low stability in defects and severe traffic. Mohammed Amin et al. [19] proposed a lightweight authentication and storage system that provides distributed authentication among authorized devices. The developed model is evaluated against other similar techniques and the results are used to reduce the latency between connected devices and communication statistics within the technique.In the literature, optimization-based encryption algorithms have attracted the attention of many researchers aiming to improve security and privacy in healthcare systems. However, it is necessary to solve some problems, such as high energy consumption, high general cost, low resistance to failure, and intense traffic. Mohammed Amin et al. [19] proposed a slight authenticated system and the maintenance of data to ensure decentralized authentication among the authorized devices. Using the results of the assessment of the model created about other similar methods, they reduce the delay between connected devices and statistics in their methodology.

Sybil Watch performs better than existing methods in terms of accuracy, efficiency, and scalability, according to analyses comparing simulation findings with real-world datasets; nonetheless, maintaining a high number of keys requires a significant amount of storage space. A blockchain-based fog-computing architecture was proposed by Shukla, Saurabh et al. [28] to allow privacy-preserving authentication and authorization.

Compared to other similar methods, minimize the delay between the relevant devices and the approach of the approach. SybilWatch works better than existing methods from the accuracy, efficiency, and scalability viewpoint, compared to the actual datasets of the modeling with the actual datasets. Nevertheless, maintaining a large number of keys requires a considerable number of storage space. Shukla, Saurabh et al. [28] proposed a blockchain -based fog computing architecture for healthcare IoT permission and authentication to enable privacy authentication and approval. This concept uses a distributed authentication mechanism supported by a blockchain consortium., To achieve the main

goal of ensuring secure data transmission, this study used real medical datasets and simulations. The results showed that the recommended method could accurately identify malicious nodes, with a success rate of about 91%, although the throughput remained quite low. An improved authentication based on hyperelliptic curve public key cryptography was proposed by Kavita et al. [22] for IoT applications in healthcare. This system uses a generalized group key agreement mechanism to enhance security and authentication. Its effectiveness was evaluated using strict security metrics and compared with other relevant models. As a result, we found that although fault tolerance is significantly lower due to the reduced communication volume, the performance is improved compared to existing methods.

3. PROPOSED MODEL

The proposed architecture for patient monitoring using IoT-based edge sensors (see Figure 1) uses asymmetric key encryption to enable the transmitter and receiver to securely encrypt and decrypt the patient medical records received from the IoT-based edge sensors. Encryption of characteristics such as IP addresses, URLs, or MAC addresses in the patient medical record data is made secure using the proposed Whale-based attribute encryption process. We also periodically calibrate the whale suitability to generate corresponding public and private master keys, which ensures that the data is protected from unauthorized access or modification as it is transmitted to remote locations for analysis to inform medical decisions. Therefore, a model will be developed that has appropriate features to ensure secure data transfer and protect medical records from unauthorized access.

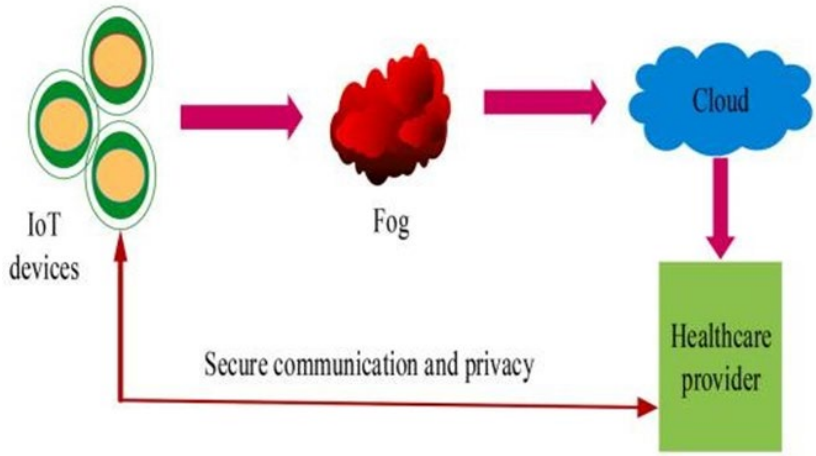

Figure 1 IoT for secure communication in healthcare system

Healthcare IoT provides many advantages, such as better as a better result of patients, higher caliber treatment and cost reduction. This allows medical experts to examine the transmitted data and take appropriate measures. As a result of these changes, many security-enhancing technologies have been created, but there are still high attack rates and insufficient protection and privacy. These issues include the lack of secure communication channels, vulnerability to cyber-attacks, and privacy concerns related to unauthorized disclosure of personal medical data. As can be seen in Fig. 2, it is essential to use a strong authentication mechanism and an encryption method that can provide a secure communication channel to ensure that a secure communication protocol is established between the various devices involved in the process. It illustrates how wearable IoT sensors are embedded into the human body to monitor vital signs such as temperature, heart rate, and blood pressure. Before the collected data is securely transmitted wirelessly to cloud servers, it is encrypted using cryptographic techniques to ensure its safety. Encrypted personal data is stored in the cloud so that medical professionals can access it in case of an emergency. Moving a patient's medical records from IoT sensors to the cloud and then to doctors and clinicians for decision-making is particularly sensitive due to the large number of networked middleware devices and shared wireless communication links. We provide optimization-based encryption technology that generates secure keys to protect your data while efficiently managing network traffic.

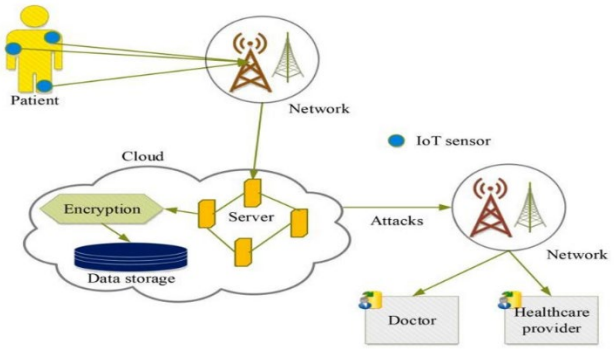

Figure 2 Proposed Security framework in IoT-based healthcare system.

In the field of medicine, where IoT sensors control the vital signs of patients and send updates to the cloud via local and extended networks connected with an area, the main objective of the proposed model is to ensure the transfer and data storage. Given the vulnerability of safety on the network according to sensors based on the screen of the Internet of Things, it is very important to recognize reliable authorities, data users, data owners, their rights and rights and rights unauthorized users and their access [24]. The proposed security algorithm consists of three main steps: encryption, decryption, and key creation. Fig. The overall process of implementing attribute-based encryption for medical data modifications is shown in Figure 3. A user must first be authenticated and authorized to edit a medical record.

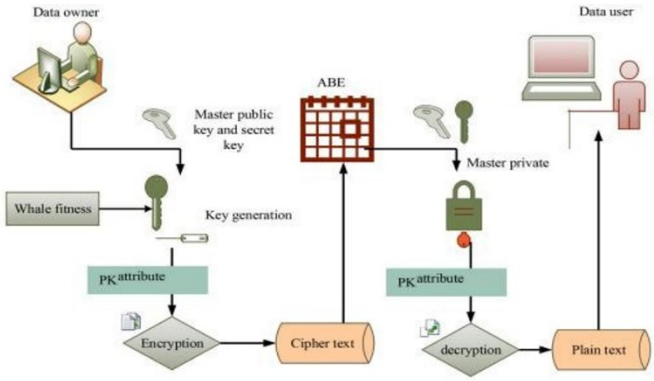

Figure 3 Encryption and decryption in the Proposed Framework

The encrypted data is decrypted using the same encryption key and sent back to the database for secure storage after the user makes any changes. Establishing a new hash value is the final step to ensure the accuracy of the updated medical data. This value can be used to verify that all modifications have been made correctly and accurately. The proposed methodology uses a robust two-layer security procedure to protect medical data during transmission and storage. The first level of authentication ensures that only authorized data can be accessed. The attribute-based

encryption method used to encrypt medical data is the second encryption level [25]. During transmission, health data is protected at this level. The Whale optimization algorithm was used in the proposed methodology to optimize the encryption level key generation procedure. WOA simplifies the key generation and selection procedure, improving efficiency and security. WOA is a metaheuristic strategy inspired by the hunting tactics of humpback whales. For meals, whales pursue Krill and small fish. These fish and Krill emphasize important aspects for important generations. The WOA method allows to dynamic modifying of the physical shape of the whale and identify ideal key qualities, as well as improving the key generation procedure.

4. COMPARISON OF EXISTING MODELS IN HEALTHCARE IOT SECURITY

The total number of CPU cycles (also called clock cycles) required by the processor to execute the instructions associated with a particular program or function is known as the execution time, which includes the time required for

the instructions to complete, plus any wait time incurred by memory accesses, I/O activity, etc. The execution time measured by Hertz is the maximum number of operations per second that can be executed by the processor. The execution time of the proposed model contrasts to DPLA, DLSB, FCTTP, and HECC in Table 2. Fig. 4 demonstrates that the proposed model outperforms DPLA, DLSB, FCTTP, and HECCS in terms of execution time for all sizes of IoT edge-based sensor networks. Specifically, when five sensors were used, the FCTTP model achieved 27.5 ms, the DLSB approach achieved 20 ms, and the DPLA strategy required a run time of 40 ms. Furthermore, when 20 sensors were used, the DLSP model lagged behind the recommended model, while the HECCS model ran at 25 ms for five IoT edge-based sensors.

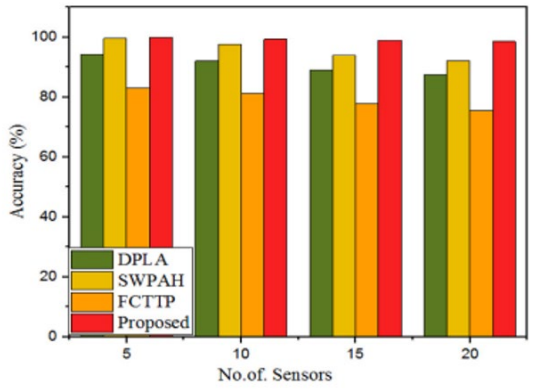

Figure 4 Comparison of accuracy of different models over varying numbers of IoT sensors

The term "throughput" refers to the amount of data a security algorithm can process in a given period. Often specified in bits or packets per second, it is used to quantify the speed of a particular computer system or network. It gauges how long an algorithm takes to do a task involving encryption or decryption; faster and more effective security techniques are indicated by higher throughput. As shown in Table 3, the designed model\'s increased throughput performance is contrasted with that of the PPDA, SWPAH, FCTTP, and suggested model. Considering the smallest network size with five Edge-based IoT sensors, the FCTTP model achieved a throughput of 318 Kbps, the PPDA model achieved a throughput of 432 Kbps, and the SWPAH model had a throughput of 260 Kbps. At 850 kbps, the fastest throughput was predicted. For the larger network size of 20 sensors, as shown in Fig. 5, the proposed design had a better throughput of 812 kbps compared to the existing security measures, which improved the system performance.

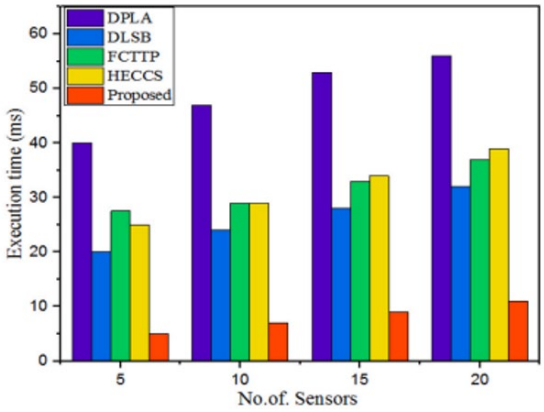

Figure 5 Comparison of different models' execution times over varying numbers of IoT sensors

The proposed research combines the advantages of Whale attribute encryption system and optimization. The combination of the two methods improves the security and efficiency of data transmission. The presented work provides a fine particle approach for data encryption and uses attribute encryption architecture to provide flexibility. Improve the secrets of the data, accurately control the data access, and select a function suitable for data encryption. Moreover, the use of asymmetric master keys balances security and efficiency, ensuring effective encryption and decryption for real-time applications.Furthermore, we integrate a whale adaptation mechanism to dynamically update the whale's fitness,

thereby optimizing the encryption process. Furthermore, the system can identify features that pose a risk to data security by adding an additional security layer.The proposed method secures an IoT-based patient monitoring architecture enabled by edge sensors. Using private keys created, the properties of the system, such as Mac addresses, IP addresses and URLs, are encrypted before sending the patient's data to the recipient. Then, the performance of the suggested method is contrasted with that of the most advanced DPLA.

5. CONCLUSION

The proposed model protects security data by combining the advantages of WOA and Abe. The WOA included in the recommended approach optimizes the main generation process, the ABE provides effective encryption, and the patient's health data obtained from the Python library, which contains data accumulated from IoT -based sensors. Evaluated using PHR) patients and various attacks on the ground The study findings are also evaluated and compared with currently implemented security measures, such as DLSB, FCTTP, and PPDA, in terms of processing speed, energy consumption, data transmission rate, accuracy, and computational cost. The system displays impressive performance parameters, such as short execution times, low energy consumption, high throughput, and low computational costs. These features make it suitable for real-time healthcare applications.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

B. Ahmed, M. Imtiaz, M. Arshad, Adaptive personalized healthcare using IoT environments: challenges and opportunities, IEEE Transactions on Network Science and Engineering 3 (3) (2016) 243–255.

Lee, An Hsiu, An architecture and management platform for blockchain-based personal health record exchange: development and usability study, J. Med. Internet Res. 22 (6) (2020), e16748.

Ali, Aitizaz, Security, privacy, and reliability in digital healthcare systems using blockchain, Electronics 10 (16) (2021) 2034.

A.S.M. Shamsul Arefin, K.M. Nahiyan, Mamun Rabbani, The Basics of Healthcare IoT: Data Acquisition, Medical Devices, Instrumentations and Measurements.A Handbook of Internet of Things in Biomedical and Cyber Physical System, Springer, Cham, 2020, pp. 1–37.

Kadhim, Takleef Kadhim, An overview of patient's health status monitoring system based on internet of things (IoT), Wireless Pers. Commun. 114 (3) (2020) 2235–2262.

Munirathinam, Sathyan. Industry 4.0: industrial internet of things (IIOT), Advances in computers Elsevier 117 (2020) 129–164.

Awotunde, Bamidele Joseph, Disease Diagnosis System for IoT-Based Wearable Body Sensors with Machine Learning Algorithm. Hybrid Artificial Intelligence and IoT in Healthcare, Springer, Singapore, 2021, pp. 201– 222.

Martinez-Ríos, Erick, A review of machine learning in hypertension detection and blood pressure estimation based on clinical and physiological data, Biomed. Signal Process Control 68 (2021), 102813.

Reyna, Ana, On blockchain and its integration with IoT. Challenges and opportunities, Future Generat. Comput. Syst. 88 (2018) 173–190.

Banerjee, Syagnik, Thomas Hemphill, Phil Longstreet, Wearable devices and healthcare: data sharing and privacy, Inf. Soc. 34 (1) (2018) 49–57.

A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, A. Alazab, A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks, Electronics 8 (11) (2019) 1210.

Z. Tang, L. Jiang, X. Zhu, and M. Huang, "An Internet of Things-Based Home Telehealth System for Smart Healthcare by Monitoring Sleep and Water Usage: A Preliminary Study," Electronics, vol.12, no.17, pp.1-14, August 2023. https://doi.org/10.3390/electronics12173652

M. A. Elhosseini, N. K. Gharaibeh and W. A. Abu-Ain, "Trends in Smart Healthcare Systems for Smart Cities Applications," In Proceedings of International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 23-25 January 2023, pp.1–7. https://doi.org/10.1109/icaisc56366.2023.10085212

A. Wells and A. B. Usman, "Privacy and biometrics for smart healthcare systems: attacks, and techniques," Information Security Journal: A Global Perspective, vol.33, no.3, pp.307–331, October 2023. https://doi.org/10.1080/19393555.2023.2260818

15. F. Bu, M. Wang, and L. "Tian, Research on Medical Big Data Mining and Intelligent Analysis for Smart Healthcare," In proceedings of International Conference on 3D Immersion, Interaction and Multi-sensory Experiences (ICDIIME), Madrid, Spain, 27-29 June 2023, pp.394–39. https://doi.org/10.1109/icdiime59043.2023.00082

S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. Shetty, and A. Alqahtani, "Design of Robust BlockchainEnvisioned Authenticated Key Management Mechanism for Smart Healthcare Applications," IEEE Access, vol.11, pp.93032–93047, August 2023. https://doi.org/10.1109/access.2023.3310264

G. Sandi, S. H. Supangkat, Ermawati, "Smart Healthcare for Personalized Healthcare: Literature Review," In Proceedings of International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, 06-07 September 2023, pp.1–7. https://doi.org/10.1109/iciss59129.2023.10291631

M.-H. Lee, I-H. Liu, and J.-S. Li, "Cyber Security in a 5G-Based Smart Healthcare Network: A Base Station Case Study," Engineering Proceedings, vol.55, no.1, pp.1-6, December 2023. https://doi.org/10.3390/engproc2023055050

M.A. Almaiah, F. Hajjej, A. Ali, M.F. Pasha, O. Almomani, A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS, Sensors 22 (4) (2022) 1448.

A. Ali, M.F. Pasha, J. Ali, O.H. Fang, M. Masud, A.D. Jurcut, M.A. Alzain, Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: a novel approach to cryptography, Sensors 22 (2) (2022) 528.

S. Vaishnavi, T. Sethukarasi SybilWatch, A novel approach to detect Sybil attack in IoT based smart health care,

J. Ambient Intell. Hum. Comput. 12 (6) (2021) 6199–6213.

S. Shukla, S. Thakur, S. Hussain, J.G. Breslin, S.M. Jameel, Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model, Internet of Things 15 (2021), 100422.

S. Kavitha, P.J.A. Alphonse, Y. Venkataramana Reddy, An improved authentication and security on efficient generalized group key agreement using hyperelliptic curve-based public key cryptography for IoT health care system, J. Med. Syst. 43 (8) (2019) 1–6.

Singh, M.K., Singh, A.K., Singh, P., Kalpana, Rishi, O.P. (2023). Artificial Intelligence Enabled IOT System for Football Identification in a Football Match. In: Garg, D., Narayana, V.A., Suganthan, P.N., Anguera, J., Koppula, V.K., Gupta, S.K. (eds) Advanced Computing. IACC 2022. Communications in Computer and Information Science, vol 1782. Springer, Cham. https://doi.org/10.1007/978-3-031-35644-5_37