Boosting Data Communication: Studying Health Information Security Using Digital and IoT Technologies for Public Health

Dr. Abhijeet Madhukar Haval[1], Md Afzal[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.*

KEYWORDS

IoT Technologies, cloud Storage, Public health, Data security

ABSTRACT

The integration of Internet of Things (IoT) technologies in healthcare has revolutionized data management, yet challenges in data security and efficient communication persist. Existing solutions often struggle with balancing security and performance, particularly under varying conditions. To address these limitations, we propose a novel approach using Homomorphic Fuzzy Identity-Based Encryption (HFIE) to enhance both data security and communication efficiency in healthcare IoT systems. Our implementation includes a robust architecture that securely collects and transmits health data from sensor nodes to cloud storage, employing a three-tier user access system. HFIE combines homomorphic encryption for secure data processing and FIBE for flexible, error-tolerant access control. This combination addresses the limitations of traditional methods by providing enhanced privacy and performance. Evaluation metrics, including decryption time, energy consumption, and execution time, demonstrate the effectiveness of our approach. HFIE's ability to ensure secure and efficient data management in public health makes it a significant advancement in healthcare IoT technology.

1. Introduction

The growth of digital and IoT technologies has become a part of healed business systems over the last couple of decades, bringing improvements in the communication of information to public health systems. These technologies allow for timely information sharing and patient monitoring at a distance and enable healthcare accessibility and effectiveness [1]. However, the exponential increase in the technological integration of devices complicates the protection of health information from cyber threats. Preserving the health information systems' integrity is vital when it comes to safeguarding clients' secure information [2]. The importance of developing protective systems and controls to deal with security issues in the healthcare sector [12]. Emerging technologies in digital systems and IoT devices enhance the healthcare system and the surveillance of disease spread for early interventions [4]. Digital platforms increase data communication in public health and overall health information transfer and utilization, hence improving results [5]. This paper focuses on developing a secure architecture for medical data management in IoT for public health, leveraging Homomorphic Fuzzy Identity-Based Encryption (HFIE) to ensure confidentiality, accuracy, and controlled access in both normal and emergency conditions.

Related Work

A blockchain-assisted secure data management framework (BSDMF) was presented in a study of Abbas et al. [13] to improve patient data exchange and scalability in public healthcare [3]. Healthcare systems were connected to a smart medical infrastructure known as the Internet of Medical Things (IoMT). Privacy, security, scalability, and accessibility were all significant IoT problems [6]. Those modes might be disrupted by blockchain technology. The suggested BSDMF outperformed when compared with existing methods.

The IoT with AI System (IoT-AIS), which bridges the digital and physical worlds, was presented in the Ghazal [7] for healthcare security. IoT-AIS tracks and encrypts patient data before storing it in the cloud for remote access. Each patient may retain their information using a customized user interface that the dashboard offers. IoT-AIS outperformed alternative techniques in terms of data transfer, delivery, and performance rates, allowing for customized access to medical records.

An AI-based structure with a 6G connection for safe data transmission was proposed in the research of Chaudhary et al. [8], which also included a variety of medical technologies, such as medical devices, online healthcare, and skin networks. The change from specialist-centric to patient-focused healthcare

has resulted in the development of smart healthcare technologies that enable remote diagnosis [9]. Machine learning techniques were used to test the design's efficiency, and the RF algorithm for classification outperformed traditional algorithms by 98%.

To increase data security and privacy in healthcare applications, Liu et al. [14] developed a Distributed Ledger-based Improved Biomedical Security system (BDL-IBS). Strong permission procedures for data sharing were to be established, as well as the ability for patients to use medical data for therapy. Platforms built on blockchain technology facilitate quick, simple, and seamless interactions between data providers, improving data security and privacy.

Using layered modeling and the Modular Encryption Standard (MES), the study of Shabbir et al. [10] concentrated on requirement-oriented health data security [15]. There were privacy and security issues with mobile cloud computing (MCC) in the healthcare industry, which called for immediate action. An examination of performance revealed that the suggested approach performed better than other algorithms in terms of both security measures and overall quality.

2. Methodology

Architectures for the proposed method

The following part addresses the structure that allows healthcare IoT enterprises such as healthcare organizations and hospitals to handle nodes of sensors for data collection. The recommended design is efficient at storing large amounts of data acquired by nodes of sensors. Because this data is extremely secret, we created a security approach to ensure the accuracy of data, confidentiality, and access control. To meet the aforementioned aims, we created the structure depicted in Figure 1. The structure has three types of users: users, general users, and healthcare experts, and it includes various components. Nodes of sensors observe their health and well-being and collect information at certain times. Healthcare providers use software for monitoring to get the information. The Healthcare Authority (HA) oversees hospitals or healthcare facilities and establishes security procedures. Cloud-based storage is used to store healthcare data and ensure its security.

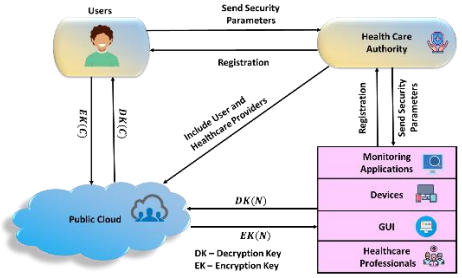

Figure 1 Structure for Healthcare IoT

The recommended design involves attaching compact sensor nodes to each patient. Nodes of sensors continuously monitor and gather information about patients, including movements, heartbeats, and physiological signals. Sensor nodes provide information to the gateway, which aggregates it and encrypts it with a randomly generated symmetric key (RSK). Private information is stored on the cloud. Systems for monitoring allow hospitals and healthcare providers to track the wellness of patients from any place. Healthcare providers retrieve and decrypt data from a cloud server using an encrypted key. Systems for surveillance employ RSK for health information encryption and HA for control of access.

Healthcare IoT security model

The next section describes the recommended architecture's safety features and functions. The recommended protection paradigm consists of three elements: HA, members, and cloud. Transport Security Layer (TSL) protocol provides safe connections among HA, members, and cloud. TSL ensures that information remains secure and intact during transmission. However, encryption at the user's level is required for cloud storage. A public encryption infrastructure maintains each party's private and

public key pairs.

Security implementation: The HA sets an attribute set and uses the HFIE method to create the public key (PUK) and master key (MK). The PUK, which is required for data decryption and encryption, is freely shared with all users. As a result, the MK is safely saved and not revealed to patients. To safely transmit the PUK, HA encodes it with a private key (PRK) and sends it to cloud service providers (CSP). Clients obtain and validate the encoded PUK to ensure a safe connection. This approach assures that critical health data is protected by encryption using HFIE, ensuring strong privacy and reliability throughout data movement and retention in healthcare IoT contexts.

Authentication and authorization for healthcare providers: Patients in the healthcare IoT may participate and exit the connection at any moment. If a fresh user joins the connection, the HA must issue them the secret key (SK) to obtain rights. The access privileges (AP) allow new users to encode and decode information before transmitting it to the public cloud. Healthcare providers and patients have various security criteria. Patients should encrypt their health information before transmitting it to a cloud storage, which is only accessible in read mode. Healthcare providers must encrypt health information sent in both writing and reading modes. HA offers many ways to connect for both healthcare providers and patient providers. A healthcare provider's access rights are divided into two groups: one for write mode encryption and another for protecting medical data.

Management of public health Data: Nodes with sensors gather public health information, which can only be accessible in read mode. Nodes with sensors continually transmit the information they collect to the gateway (G). When a gateway delivers encrypted information to the CSP, patients can decrypt it using the secret key SK. If there are anomalies in the decrypted data, users should notify the HA. Public health information includes medication, diagnoses, and observations from healthcare providers. To prevent unauthorized access, every document requires login credentials. Healthcare providers use a similar process for reading healthcare information from cloud servers as they do for health information. To gain write accessibility, healthcare providers have to provide the document's login credentials (LS) to the CSP. Once the CSP confirms the login credentials, healthcare providers can access information for adjustments.

Homomorphic encryption

Homomorphic encryption is a special encryption algorithm. The homomorphic encryption technique may be stated cryptographically as equation (1), where $\mathcal{C}$ and $\mathcal{M}$ represent both ciphertext and plaintext spaces, respectively.

$$\forall n_b, n_a \in \mathcal{M}, Enc_{pk}(n_b) \odot_{\mathcal{C}} Enc_{pk}(n_a) = Enc_{pk}(n_b \odot_{\mathcal{M}} n_a) \quad (1)$$

The operators in this case are represented by $\odot_{\mathcal{C}}$ and $\odot_{\mathcal{M}}$, respectively, on both ciphertext and plaintext spaces. Both addition and multiplication homeomorphisms are used in encrypted form, and they are distinguished by the characters $\odot_{\mathcal{M}}$. To put it briefly, the procedure is known as multiplication homomorphism if $\odot_{\mathcal{M}}$ is operator "$*$" and addition homomorphism if $\odot_{\mathcal{M}}$ is operator "$+$". ElGamal algorithm founded on the Diffie-Hellman key agreement is categorized as an asymmetric cryptosystem. It possesses additive homomorphism characteristics. There are 4 fundamental stages in the algorithm.

The initialization process: G is a group of cycles with a big primal r and generator h. Key generation center creates the public variables (r, h, G) with an encrypted variable l. The process of key generation involves the key generation center selecting at random an amount $\mu \in Z_r^*$ as the PRK and calculating $y = h^{\mu} \in G$ as the PUK. The PUK z is used for encrypting it while the PRK μ is utilized for decryption. Encryption: For encryption of the plaintext m, the person who sent the message chooses an arbitrary number $q \in Y_r^*$, determines $c_1 = h^q$, $c_2 = mz^S$, and subsequently transmits a ciphertext (c_1, c_2) to the destination. Decryption: Upon obtaining the ciphertext (c_1, c_2), the recipient computes $m = \frac{c_2}{c_1^{\mu}} = \frac{my^S}{(h^S)^{\mu}}$ using the PRK μ to decode the plaintext m.

Nonetheless, the federated instructional system often gains the ability to apply additive aggregating to regional models with ciphertext form. All that has to be done is convert the plaintext m into the exponential form, where the base is the number 2, such that $c_2 = 2^n y^S$. The improved ElGamal method fulfills additive homomorphism, as can be demonstrated from equation (2). A decryption equation can be used to recover the sum of the plaintexts following aggregation using the ciphertext form (3).

$$\forall n_b, n_a \in \mathcal{M}, Enc\,(n_b) \times Enc\,(n_a) = (d_{1b}.d_{1b}, d_{2b}.d_{2b}) = (h^{q_b+q_a}, 2^{n_b+n_a} z^{q_b+q_a}) = Enc(n_b + n_a) \quad (2)$$

$$n_b + n_a = log_2[(d_{2b}.d_{2b})/(d_{1b}.d_{1b})^{\mu}]\,, log_2[2^{n_b+n_a} z^{q_b+q_a}/(h^{q_b+q_a})^{\mu}] \quad (3)$$

It is essential to recall that the foundation of homomorphic encryption requires that several plaintexts be encoded using the same PUK. Therefore, rather than merely encrypting the local variables using the server's PUK, each client needs to integrate additional precautions with the ElGamal method to provide security and preserve privacy in learning through federation.

Fuzzy Identity-Based Encryption (FIBE)

A specific system known as FIBE was also introduced by the idea of attribute-based encryption. The Fuzzy-IBE structure utilizes techniques from Identity-Based Encryption. In FIBE, individuality is considered a collection of qualities. FIBE supports a secret key for establishing an identity, ω, to decode ciphertext encoded with an identity, ω 0. This is only possible if each identity, ω and ω', are sufficiently adjacent to one another as determined using the "set overlapping" proximity metric.

$$|\omega \cap \omega'| \geq d \quad (4)$$

If their characteristics overlap by a minimum of c attributes, then this equation guarantees that the PRK for identity ω can decode a message encrypted using identification ω'. To decryption ciphertext C encryption using identification ω', the PRK for identity ω must be used.

$$Decrypt(C, PRK_{\omega}) = M \;\; |\omega \cap \omega'| \geq d \quad (5)$$

Homomorphic Fuzzy Identity-Based Encryption (HFIE)

In the paper, we employ HFIE to improve the security and privacy in healthcare IoT. HFIE, at the same time, makes use of homomorphic encryption that enables computations on encrypted information, and FIBE, which offers tolerance to errors, as well as flexible access control in accordance to attribute similarity. By employing the HFIE, it is possible to provide multiple levels of access and confidentiality for patient records and ensure the necessary security standards both in normal and critical situations. The proposed method, utilizing HFIE, ensures secure and privacy-preserving data processing and access control in public healthcare IoT systems.

3. Results and discussion

valuation and Result

The system setup includes Intel servers, client devices with Intel Core i7 processors, and sensor nodes running Windows, respectively. Utilizing TSL supports secure and efficient healthcare data management. The effectiveness of the proposed technique (HFIE) may be evaluated by utilizing many metrics, including decryption time, execution time, and energy consumption. These measures were compared to the existing approach discrete decision tree hashing algorithm with ant colony optimization (DDTHA+ACO) [11].

Accuracy and loss: In evaluating our HFIE method, we assess accuracy by measuring how effectively it maintains data integrity and precision in encrypted form. The loss metric reflects any degradation in data quality during encryption and decryption. HFIE demonstrates high accuracy and minimal loss, ensuring reliable and secure data management in healthcare IoT systems (Figure 2).

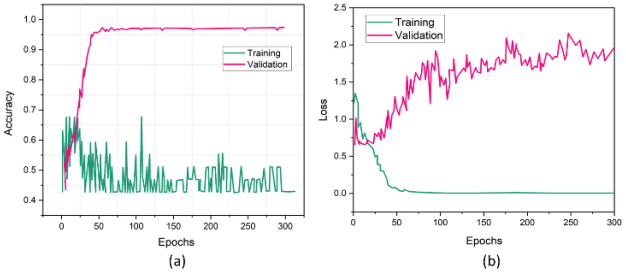

Figure 2 Outputs of Accuracy and Loss

Decryption time: To preserve system performance under both regular and emergency settings and to ensure prompt access to encrypted public healthcare data, which is essential for fast healthcare decision-making the decryption time measure assesses the effectiveness of HFIE. Figure 3 and Table 1 illustrate that the HFIE achieves a decryption time of 51 seconds, compared to 58 seconds for the existing method.

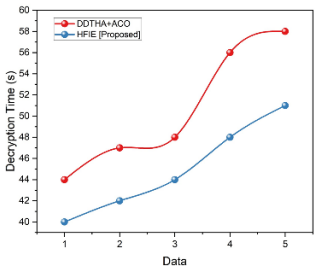

Figure 3 Comparison of Decryption time

Execution time: In crucial public healthcare situations, the execution time metric ensures system efficiency and timely data access by measuring the total amount of time required for the encryption, transmission, and decryption of healthcare data using HFIE. Figure 4 and Table 1 illustrate that the HFIE achieves an execution time of 53 seconds, compared to 57 seconds for the existing method.

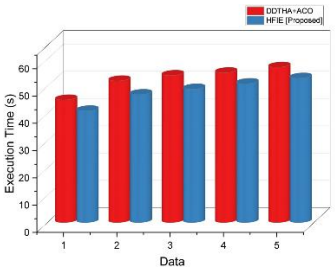

Figure 4 Comparison of Execution time

Energy consumption: For sensor nodes to have longer battery lives and to continue operating sustainably in IoT contexts related to healthcare, the energy consumption measure evaluates the power efficiency of HFIE. Figure 5 and Table 1 illustrate that the HFIE achieves an energy consumption of 57 percent, compared to 60 percent for the existing method.

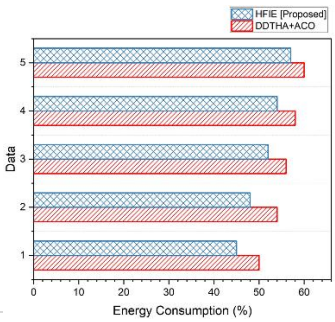

Figure 5 Comparison of energy consumption

Table 1: Result of Output

Methods	Decryption Time (s)	Execution Time (s)	Energy Consumption (%)
DDTHA+ACO	58	57	60
HFIE [Proposed]	51	53	57

4. Conclusion and future scope

In this paper, our proposed methodology using HFIE greatly enhances the secure and efficient management and protection of data in healthcare IoT systems. Incorporating the traditional homomorphic encryption with fuzzy identity based encryption; our method not only improves the security of data and control of access but also improves the performance under different conditions. This solution is free from some of the failures of automation, where, for instance, the balance between security and operation or work control and work input can be attained and errors can be allowed at times. Future work could build on the potential of incorporating new technological advancements such as edge computing and AI to enhance the real-time processing and analysis on HFIE. However, there exist some obstacles to implementing the system in a large-scale network and controlling the computational complexity of encryption algorithms. Solving these questions will become even more critical for the further development of safe and effective healthcare IoT.

Reference

[1] N.Y. Philip, J.J. Rodrigues, H. Wang, S.J. Fong, and J. Chen, "Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges, and Future Directions," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 300-310, 2021.

[2] J. Budd, B.S. Miller, E.M. Manning, V. Lampos, M. Zhuang, M. Edelstein, G. Rees, V.C. Emery, M.M. Stevens, N. Keegan, and M.J. Short, "Digital Technologies in the Public Health Response to COVID-19," *Nature Medicine*, vol. 26, no. 8, pp. 1183-1192, 2020.

[3] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[4] S. Goyal, N. Sharma, B. Bhushan, A. Shankar, and M. Sagayam, "IoT Enabled Technology in Secured Healthcare: Applications, Challenges and Future Directions," in *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications*, pp. 25-48, 2021.

[5] S.C. Ratzan, S. Sommarivac, and L. Rauh, "Enhancing global health communication during a crisis: lessons from the COVID-19 pandemic,", 2020.

[6] Stephen, K. V. K., Mathivanan, V., Manalang, A. R., Udinookkaran, P., De Vera, R. P. N., Shaikh, M. T., & Al-Harthy, F. R. A. (2023). IOT-Based Generic Health Monitoring with Cardiac Classification Using Edge Computing. *Journal of Internet Services and Information Security*, *13*(2), 128-145.

[7] T.M. Ghazal, "Internet of Things with Artificial Intelligence for Health Care Security," *Arabian Journal for Science and Engineering*, 2021.

[8] S. Chaudhary, R. Kakkar, N.K. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, M.D. Alshehri, R. Sharma, G. Sharma, and I.E. Davidson, "A Taxonomy on Smart Healthcare Technologies: Security Framework, Case Study, and Future Directions," Journal of Sensors, 2022(1), p. 1863838, 2022.

[9] Mohamed, K.N.R., Nijaguna, G.S., Pushpa, Dayanand, L.N., Naga, R.M., & Zameer, AA. (2024). A Comprehensive Approach to a Hybrid Blockchain Framework for Multimedia Data Processing and Analysis in IoT-Healthcare. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 94-108. https://doi.org/10.58346/JOWUA.2024.I2.007

[10] M. Shabbir, A. Shabbir, C. Iwendi, A.R. Javed, M. Rizwan, N. Herencsar, and J.C.W. Lin, "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," IEEE Access, 9, pp. 8820-8834, 2021.

[11] A.M. Al Shahrani, A. Rizwan, M. Sánchez-Chero, C.E. Rosas-Prado, E.B. Salazar, and N.A. Awad, "An Internet of Things (IoT)-Based Optimization to Enhance Security in Healthcare Applications," Mathematical Problems in Engineering, vol. 2022, p. 6802967, 2022.

[12] L.H. Yeo and J. Banfield, "Human factors in electronic health records cybersecurity breach: an exploratory analysis," Perspectives in Health Information Management, 19(Spring), 2022.

[13] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F.M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Personal and Ubiquitous Computing*, 28(1), pp. 59-72, 2024.

[14] H. Liu, R.G. Crespo, and O.S. Martínez, "Enhancing Privacy and Data Security Across Healthcare Applications Using Blockchain and Distributed Ledger Concepts," Healthcare, vol. 8, no. 3, pp. 243, 2020.

[15] Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.