JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 6 No. 1 (2025) 35-57
https://publisher.uthm.edu.my/ojs/index.php/jscdm

Advanced LWAVF Framework Based on Neural Network Security in IoMT for Managing Patient Data Authentication and Integrity Validation with Consensus Mapping

Taher M. Ghazal[1]*, Taj-Aldeen Naser Abdali[2], Mosleh M. Abualhaj[1], Ali Q Saeed[3], and Munir Ahmad[4]*

[1] *Department of Networks and Cybersecurity, Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, 19111, JORDAN*
[2] *Mathematics Department, College of Basic Education, University of Misan, Misan, IRAQ*
[3] *Computer Center, Northern Technical University, Ninevah, IRAQ*
[4] *University College, Korea University, Seoul, 02841, REPUBLIC OF KOREA*

*Corresponding Author: ghazal1000@gmail.com, munirahmad@ieee.org
DOI: https://doi.org/10.30880/jscdm.2025.06.01.003

Article Info

Received: 27 January 2025
Accepted: 23 April 2025
Available online: 30 June 2025

Keywords

AES-256, consensus mechanism, data authentication, integrity verification, IoMT, neural network

Abstract

The Internet of Medical Things (IoMT) is vital for modern health care, enabling continuous patient monitoring, health record management, and disease diagnosis. However, the sensitive nature of health data requires robust security measures, particularly when decentralized cloud-based data sharing is employed. Current systems often struggle to maintain data integrity, authentication, and protect privacy. Hence, the research proposes the Lightweight Authentication and Validation Framework (LWAVF), which is designed to securely authenticate and validate patient data at both the sender and receiver ends. The framework uses AES-256 encryption to format and protect data during transfer. It incorporates a consensus mechanism to track key parameters from both parties, such as time, agreement status, and data counts, ensuring accurate validation. A unique one-track neural learning model simplifies its verification process by analyzing mapping parameters over time. The research results demonstrate the framework's efficiency, achieving 416.35 ms for data sharing, 3.22 ms for authentication, 5.98 ms for integrity verification, a latency of 455.55 ms, and a complexity of 20.14 ms, highlighting its suitability for secure, real-time IoMT applications. This research contributes to the development of enhanced, secure, and low-latency data authentication and validation for real-time healthcare applications within the IoMT ecosystem.

1. Introduction

A patient monitoring system tracks patients' health conditions to facilitate diagnosis processes. A remote patient monitoring system, primarily for patient monitoring, uses wearable devices to collect patient data via an internet connection [1]. The patient's vital signs, movements, and healthcare details are monitored via a monitoring system. The Internet of Medical Things (IoMT) is used in applications for remote healthcare systems [2]. IoMT uses internet-connected wearable sensor devices that provide feasible medical data for various services [3].

Securing patient monitoring is a crucial task that requires proper data management policies for the network [4]. The ioMT-based patient monitoring model mainly captures patients' real-time healthcare data via devices. The model provides the required data security services to protect users' data from attackers [5]. The monitoring model uses cyberattack detection to detect attacks during the monitoring process. The model also provides effective data sharing and communication policies that elevate the performance range of the systems. The IoMT-based monitoring model securely manages the patient data and produces feasible user diagnosis services [6, 7].

Blockchain (BC) technology allows the network to share secure data in a distributed ledger. BC technology is used for IoMT-based secure patient monitoring systems [8]. In this, BC is used to transfer patient data from one end to another in a safe way. An integrated patient monitoring system using IoMT is used in healthcare applications [9]. The integrated system collects healthcare data from the devices, which are secured and stored in memory space. User data is identified, and extra safeguard services are provided to ensure the data's safety [10]. The BC-based system enhances data security and privacy levels against third-party access. A blockchain-based patient monitoring model is also used in healthcare systems [11]. The monitoring model analyzes the data gathered from the devices. The model also protects patients' data privacy and integrity [12]. The monitoring model generates effective policies to secure data from unauthorized requests and parties. It prevents confidential information during data sharing and communication services. The monitoring model enlarges the efficiency range of the healthcare systems [13, 14].

Machine learning (ML) algorithms are used in BC and IoMT-based patient monitoring systems. ML enhances the precision rate in the detection processes of monitoring systems, specifically, BC-based personalized federated learning (FL) for IoMT-enabled monitoring systems [15]. The data collected from the systems is analyzed for the training process. The FL trains on the uploaded user's private data [16]. The trained data are encrypted to prevent unwanted attacks from third parties. The FL is used here to block the threats that lead to data leakage [17]. The FL algorithm identifies the precise types of data to implement preventive measures for the information. The BC-based method enhances the overall security level, thereby improving the quality of service (QoS) range of the monitoring systems [18]. A deep learning (DL) assisted IoMT-enabled patient monitoring model is also used to secure third-party data. The DL algorithm extracts optimal personal data from the datasets [19]. The algorithm designs a safe and secure policy to protect data from attackers. The DL algorithm identifies the threats and categorizes them according to severity. The DL-based model improves the functional quality and security range of data in patient monitoring systems [20]. Nevertheless, the IoMT paradigm faces significant privacy and security challenges when handling sensitive patient information. Conventional methods face challenges such as validation, authentication, and robust security metrics, which are crucial in IoMT-based data transmission due to the limited energy and computational resources of the devices. In addition, traditional security measures often lack adequate procedures to handle unauthorized access, impersonation attacks, and data breaches. This means that, despite the growing popularity of IoMT, there is no single solution that guarantees security, efficiency, and cost-effectiveness. Existing methods primarily focus on a single criterion, overlooking the associated architectural costs.

Furthermore, the authentication frameworks tend to be more secure but increasingly complex, rendering them unsuitable for the current generation of devices. The IoMT still has a considerable gap to fill to be suitable for research and advancement. The aim of this investigation stems from the aspiration to facilitate trustworthy and resourceful patient information exchange while leveraging easy-to-implement solutions to mitigate the weaknesses of IoMT devices. The motivation is derived from the healthcare industry's need to maintain patient privacy and security without negatively impacting functionality and usability.

The primary motivation behind this research is the increasing adoption of IoMT in healthcare systems, which enables continuous patient monitoring and efficient data management. However, existing research models struggle to maintain the security and privacy of sensitive health information, which raises concerns about data integrity and unauthorized access. The use of authentication and privacy measures often lacks robustness, while many solutions compromise security and are not adapted for these resource-limited conditions using IoMT devices. These existing research gaps underscore the need for a practical authentication framework that strikes a balance between security, efficiency, and cost-effectiveness.

The proposed LWAVF utilizes lightweight cryptographic algorithms, such as AES-256, in a resource-optimized manner, enabling secure operations on low-power medical devices. The model's uniqueness lies in its integration of a built-in consensus mechanism that validates time synchronization, data count, and agreement status between the sender and receiver, ensuring real-time integrity. A one-track neural learning model simplifies authentication and integrity validation, thereby enhancing adaptability and responsiveness without incurring computational overhead.

The research contributions of the LWAVF are listed as follows:

1. To develop an effective LWAVF to enhance the security of sensitive health data while minimizing computational overhead.
2. To integrate a resource-efficient encryption technique to ensure data authenticity, confidentiality, and integrity, which employs computational resource constraints in IoMT devices.

3. To analyze and implement energy optimization and scalability strategies, ensuring the framework can handle large data-sharing requirements as IoMT networks become complex.
4. To validate performance analysis of LWAVF with existing research models in terms of data sharing speed, complexity, and latency, achieving efficiency improvements by 7.93%, a reduction in complexity by 1.03%, and a decrease in latency by 7.45%.

These contributions help to answer the following research questions listed as follows.

1. How can the LWAVF ensure that confidentiality and data integrity are preserved in IoMT systems without incurring significant computational or energy overhead?
2. What strategies can be implemented within LWAVF to optimize energy consumption and support scalability as IoMT networks expand in size and complexity?
3. How does the proposed LWAVF compare to existing authentication frameworks in terms of data sharing speed, computational complexity, and latency in resource-constrained IoMT environments?

The research questions are addressed by introducing the Lightweight Authentication and Validation Framework (LWAVF), which facilitates the management of data security, privacy, and authentication in the IoMT environment. These contributions help improve data sharing by 7.93%, reduce complexity by up to 1.03%, and decrease latency by 7.45% compared to conventional methods.

2. Related Work

Ali et al. [21] developed a hybrid deep learning-enabled homomorphic encryption (HE) model for the Industrial Internet of Medical Things (IIoMT). The model utilizes consortium blockchain (BC) technology to analyze statistical operations for encryption. The developed model pre-trains the datasets collected from the medical storage system. It also classifies health records to obtain feasible information for further processing. The developed HE model improves the efficiency and performance rate of the systems. Chen et al. [22] proposed a BC-based mutual authentication protocol for IoT-enabled decentralized healthcare environments. It is used to ensure the accessibility and integrity level of patient data. The protocol provides secure and safe authentication services for users when accessing personal data. It provides secret keys to users that are used during the authentication process. The proposed protocol reduces the communication cost and latency of medical systems.

Khan et al. [23] developed a new security model utilizing blockchain (BC) for IoT-enabled health applications. The developed mode examines, analyzes, preserves, and captures users' data transaction services. BC technology is used here to encrypt the data, which contains the personal details of the patients. The model enhances the overall QoS ratio of the security process. The designed model reduces the storage rate of the data, which increases the effectiveness level of the system. Wang et al. [24] introduced a Blockchain-Based personalized access control scheme for Electronic Health Records (EHRs) in IoT environments. The introduced scheme is used during the sharing of EHR data among users. The scheme safeguards the key information of data owners (DO) from third parties. It uses adequate authenticity verification to access data. Experimental results show that the introduced scheme increases the accuracy range while accessing HER.

Qi et al. [25] developed a new BC-based IoT framework for stress detection in healthcare applications. The developed framework uses a bidirectional long short-term memory (Bi-LSTM) algorithm and a convolutional neural network (CNN) algorithm to classify the emotional features of the patients. It is used as an early detection framework that reduces the complexity of diagnosis for patients. The developed framework maximizes the accuracy level of stress detection in IoT-enabled healthcare. Alsaeed et al. [26] proposed a lightweight group authentication framework (LWGA) for IoMT. Fog computing and blockchain technologies are utilized in the framework to analyze relevant data for authentication. The computing model is used here to evaluate the key characteristics that produce feasible authentication information. Compared with others, the proposed framework improves the safety and security level of users' data.

Fiaz et al. [27] designed a two-phase BC-enabled framework for IoMT. The framework's goal is to secure the data from data loss and leakage. The BC technology is employed here to identify security risks associated with communication services. The framework is also used to provide users with secure data-sharing services. The designed framework enhances the overall QoS and performance range of the Internet of Medical Things (IoMT) networks. Hu et al. [28] introduced a privacy-preserving system for healthcare and medical data collaboration. The introduced system uses BC and the federated learning (FL) algorithm to extract the necessary features for the process. It also provides users with trustable collaborative healthcare services. The introduced system ensures the reliability and feasibility range of medical data. The introduced system reduces the computational cost and delay ratio of healthcare applications. In Table 1, the rest of the references are tabulated with the features and findings.

Table 1 *Reference tabulation*

Author	Work	Features	Techniques	Results	Research Gaps
Ali et al. [21]	A hybrid deep learning-enabled HE model for IIoMT	Encrypts and classifies health records; pre-trained on medical storage data	Homomorphic Encryption + Consortium Blockchain	Improved system efficiency and performance rate	Lacks real-time adaptability and lightweight integration for constrained IoMT devices
Chen et al. [22]	Mutual authentication protocol for decentralized IoT healthcare	Ensures data accessibility and integrity; user-specific secret keys	Blockchain-based Authentication Protocol	Reduced communication cost and system latency	The protocol does not address energy or computational constraints in IoMT nodes.
Khan et al. [23]	Security model for IoT-enabled healthcare applications	Encrypts personal patient data; transaction analysis	Blockchain	Improved QoS and reduced data storage rate	Scalability and energy efficiency remain unexplored
Wang et al. [24]	Personalized access control scheme for EHR in IoT	Safeguards data owner info; enables secure data sharing	Blockchain-based Access Control	Increased access accuracy for EHR	High computation cost and lack of lightweight adaptability for edge IoMT scenarios
Qi et al. [25]	Framework for stress detection in IoT healthcare	Classifies emotional features; supports early detection	Bi-LSTM + CNN + Blockchain	High detection accuracy; reduced diagnostic complexity	Focused on emotional health, lacks general applicability, and resource efficiency for IoMT
Alsaeed et al. [26]	LWGA for IoMT	Uses fog computing for group-based authentication; analyzes data characteristics	Blockchain + Fog Computing	Improved data safety and security	Limited validation against existing frameworks in large-scale IoMT networks
Fiaz et al. [27]	Two-phase BC-enabled framework for secure IoMT communication	Detects risks during transmission; prevents data loss/leakage	Blockchain	Enhanced QoS and network performance	Lacks energy-aware encryption mechanisms and efficiency metrics
Hu et al. [28]	Privacy-preserving collaborative healthcare using BC and FL	Ensures trust, reliability, and data privacy	Blockchain + Federated Learning	Lower computational cost and delay	The FL model lacks integration with lightweight authentication under IoMT constraints
Pei et al. [29]	A Proxy Re-Encryption Framework for Data Sharing in IoMT.	It identifies the hash, which is used for key generation during data sharing.	BC technology is used here to pair the feasible functions for encryption.	Enhances the security range of the networks.	Lacks a lightweight computational model suitable for constrained IoMT devices

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

Lin et al. [30]	A New Mutual User Authentication Protocol for IoMT.	It is used to protect patients ' data from third parties.	An ECMQV-MAC is employed to analyze the keys for authentication.	Reduces the private data leakage rate.	Does not address energy efficiency or scalability in dense IoMT scenarios
Abbas et al. [31]	A data management framework for healthcare information analysis in IoMT.	It is used to elevate the scalability level of healthcare data during sharing and transactions.	BC technology is utilized here to provide secure data exchange services to the users.	Maximizes the accuracy range of the data-sharing process.	Absence of latency reduction and real-time performance validation Needs broader evaluation across diverse IoMT health data scenarios
Zitouni et al. [32]	A lightweight energy-efficient block cipher-based DNA cryptography model for IoMT.	It is designed to secure users' data.	DNA cryptography is used to analyze the key values for the encryption process.	Enhances the performance level of the networks.	Requires optimization for processing delay and resource consumption
Jebrane and Lazaar [33]	A new lightweight authentication protocol for IoMT.	It is used to prevent attacks on healthcare devices.	CP-ABE is used to protect information from unauthorized access by attackers.	Increases the precision range of the authentication process.	Requires optimization for processing delay and resource consumption
Zhong et al. [34]	Intrusion Detection and Neural Key Exchange for IoMT.	It is developed to ensure the security of patients' data in healthcare applications.	FL and ANN algorithms are implemented in the model to detect unwanted attacks.	Elevates the overall effectiveness level of the systems.	Limited interpretability of detection models and scalability in real-world deployments
Cheikhrouhou et al. [35]	A remote patient monitoring system.	It provides effective diagnostic services to the patients.	BC and fog computing technologies are enabled to detect security issues.	Improves the efficiency range of the monitoring systems.	Real-time performance and lightweight integration remain underexplored.
Khan and AbaOud [36]	A real-time patient monitoring for IoMT.	It is used as a security system that improves the lifespan of the patients.	The FL algorithm is used here to prevent attacks during monitoring.	Maximizes the performance of the systems.	FL integration lacks evaluation under highly resource-constrained IoMT nodes.
Li et al. [37]	Group blind signature (GBS) scheme for anonymous data authentication in BC-enabled IoMT.	It elevates the key services during authentication.	The GBS scheme is used to provide users with effective access keys.	Enlarges the effectiveness rate of the systems.	Scalability and communication overhead need further optimization in practical deployments.

Blockchain, homomorphic encryption, federated learning, and fog computing have been used in IoMT security models [21–37] to improve data privacy, authentication, and access control. Despite these advances, many research gaps remain. Many models have considerable computational overhead and are therefore unsuitable for resource-constrained IoMT. Others lack real-time adaptability, lightweight encryption, and scalable integration with medical devices. Some approaches enable mutual authentication and secure data sharing, but they struggle to process efficiently under latency or energy constraints. The Lightweight Authentication and Validation Framework (LWAVF) uses AES-256 encryption, consensus-based integrity validation, and one-track neural learning to overcome these restrictions. This integrated solution provides dynamic, adaptive authentication and synchronization between communicating devices, reducing complexity and resource consumption, making it ideal for secure and scalable real-time IoMT applications.

3. Lightweight Authentication and Validation Framework

3.1 Framework Model

The proposed LWAV framework provides a brief explanation of the generation and sharing of keys for security, ensuring better signcryption and data integrity in IoMT. The influencing factors, such as modification of sensitive health information and anonymous access, are supported by signcryption key sharing security in a synchronized manner. This authentication ensures the integrity validation of patient-monitored data at both the sender and receiver ends, protecting sensitive patient health data. The process of lightweight key authentication is different from cluster-based security requirements. The proposed framework is introduced using Fig. 1.

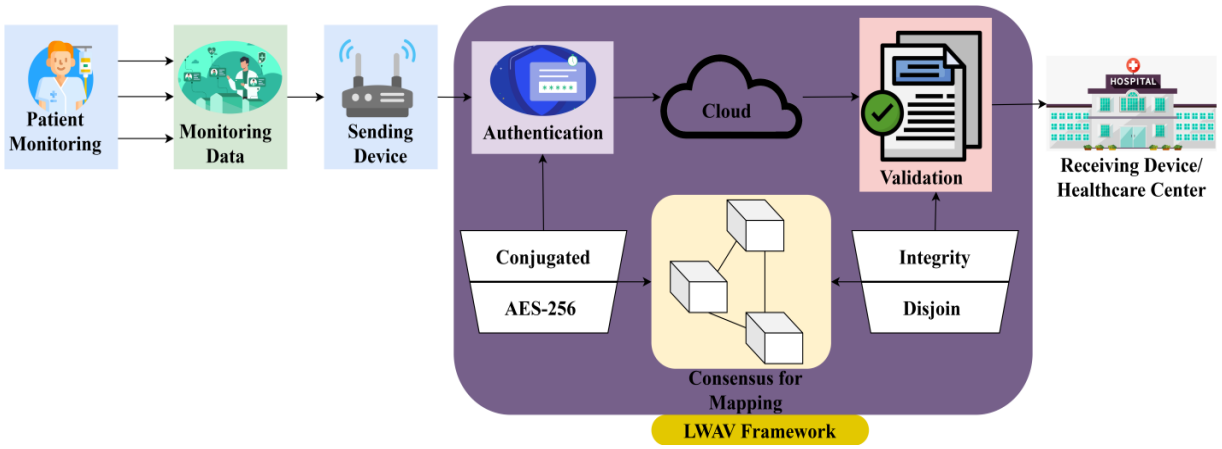


Fig. 1 *Proposed LWA framework illustration*

In smart healthcare systems, patient health record management, patient monitoring, and disease diagnosis support are pursued through the cloud platform. Therefore, this decentralized cloud is responsible for generating and sharing sender-receiver conjugated keys using AES-256-bit encryption in a synchronized manner, with reduced time and complexity. The sender and receiver conjugation times and agreement are modeled for the data authentication signature, which checks data integrity at the receiver end. The generated key is reliable enough to be used for all available patient-monitored data within the same device. Based on this conjugation time and agreement, the integrity at the receiver end is verified.

3.2 Data Authentication

The patient-monitored data in both sender and receiver ends are authenticated through the validation of AES-256 bit authentication and integrity with the aid of the proposed framework. Let $\mathbb{C}_K$ represent the conjugated keys using AES-256-bit authentication. Those keys are shared for the available patient-monitored data. Initially, the proposed framework generates keys are illustrated as in equation (1)

$$\left.\begin{aligned} \mathbb{C}_{K_1} &= \mu\left[P\left(M_{pd_1} \oplus r_1\right)\right] \\ \mathbb{C}_{K_2} &= \mu\left[P\left(M_{pd_2} \oplus r_2\right)\right] \\ &\vdots \\ \mathbb{C}_{K_N} &= \mu\left[P\left(M_{pd_N} \oplus r_N\right)\right] \end{aligned}\right\} \tag{1}$$

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

Such that

$$\left.\begin{array}{c} sck_{gt} = \sum_{i=1}^{\mathbb{C}_K} r_{gt} - \left(1 - \frac{\exists_t}{p_{gt}}\right) \\ for\ all\ M_{pd_N} = \mathbb{C}_{K_N}\ or\ M_{pd_N} < \mathbb{C}_{K_N} \\ and\ M_{pd_N} \in sharing\ of\ sck \end{array}\right\} \quad (2)$$

Where r is a random integer, M_{pd} is the monitored data and μ and P are the data authentication signature and prime integer. In above equation (2), sck_{gt} is the secret key generation time with $\mathbb{C}_{K_N}$ and r_{gt} is the time for generating random numbers, p_{gt} is the time for generating prime numbers. If $\exists_t$ represents the data sharing time in the cloud. In the above equation (1b), the condition of $M_{pd_N} \leq \mathbb{C}_{K_N}$ is to be satisfied for all patient-monitored data in the security sharing time sck_{gt} (i.e.) the conjugation time $\mathbb{C}_t$ and agreement $\mathbb{A}$ gives the delay dly_t at the time of authentication that is expressed as $dly_t > sck_{gt}$. A sender and receiver conjugated key makes use of private keys and public keys for protecting sensitive patient health data. This secret key is shared to reduce the anonymous access and changes of patient-monitored data at the time of transmission through the cloud platform. The data is converted into cipher texts using an appropriate key assignment process. The patient data are eligible to be shared with the additional conjugated key that depends on the AES-256-bit authentication (Δ) that is denoted as

$$\left.\begin{array}{c} \Delta(M_{pd}) = r_N[p_{ID}||\mathbb{C}_K] \\ for\ all \\ p_{ID} \in M_{pd} \leq \mathbb{C}_K \\ \mathbb{C}_K \in sck_{gt} < dly_t \end{array}\right\} \quad (3)$$

Where, Δ signifies authentication and p_{ID} signifies the patient identification number (register number) is prominent in identifying the patients to a sharing security. In equation (3) the authentication eligibility is verified for the patient-monitored data to meet the sharing security requirements at data transmission. In this authentication assignment, if the condition of $M_{pd_N} < \mathbb{C}_{K_N}$ is satisfied by any p_{ID} then $\mathbb{C}_{K_N}$. Therefore, the remaining conjugated keys are used for the successive sending and receiving of the data in the healthcare center. The assignment of authentication Δ follows track neural network learning. The authentication process is illustrated in Fig. 2.

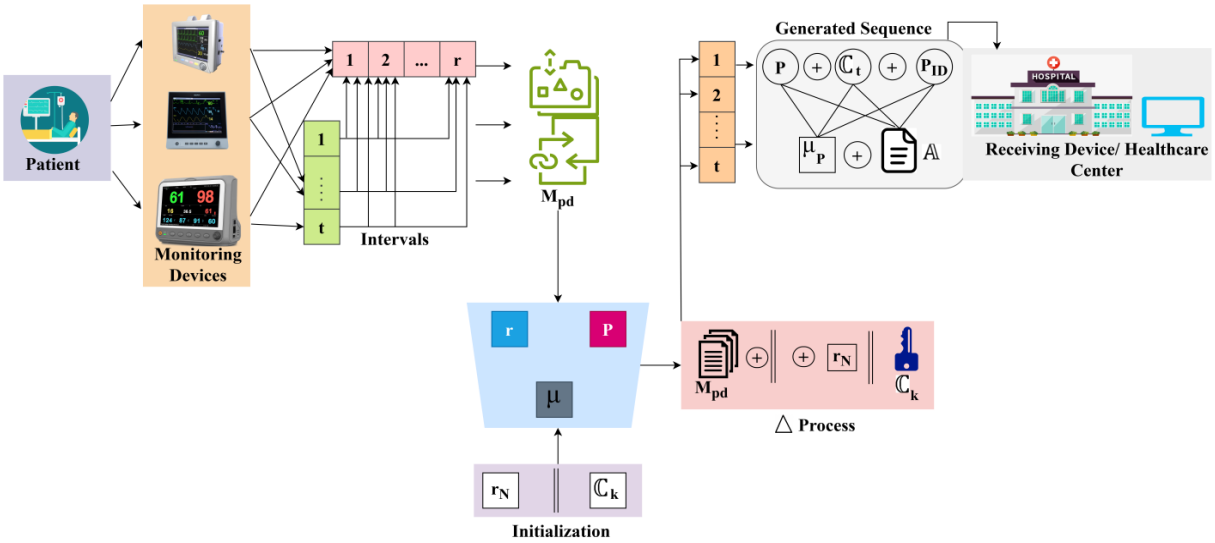


Fig. 2 *Authentication process for patient monitored data*

The μ process is illustrated in Fig. 2 for a dense M_{pd} accumulated in t intervals. In the authentication initialization process, (r, P, μ) are the requisites and validation for communicating through t intervals. The sequence of $[P \oplus \mathbb{C}_t \oplus \mu_p]$ and $[\mathbb{C}_t \oplus \mu_p]$ are used along the A active interval for which Δ the process is active. Depending on the $\mathbb{C}_k$ generation rate, the μ_p is validated across $P(M_{pdN} \oplus r_N)$ for M_{pdN} shared using sck. The conventional AES-256 authentication is pursued as $r_N[p_{ID}||\mathbb{C}_K]$. In this case, the change in Δ process is required for authentication re-verification to categorize $[M_{pd_N} < \mathbb{C}_{K_N}]$ selected by $[p_{ID} \in M_{pd} \leq \mathbb{C}_K]$ condition satisfaction.

Therefore the initialization is revisited by integrating $(\mu \oplus P \oplus r_{gt})$ for different intervals maximizing Δ levels. The authentication time for $\mathbb{C}_{K_N}$ and other variants are analyzed for μ process is given in Fig. 3.

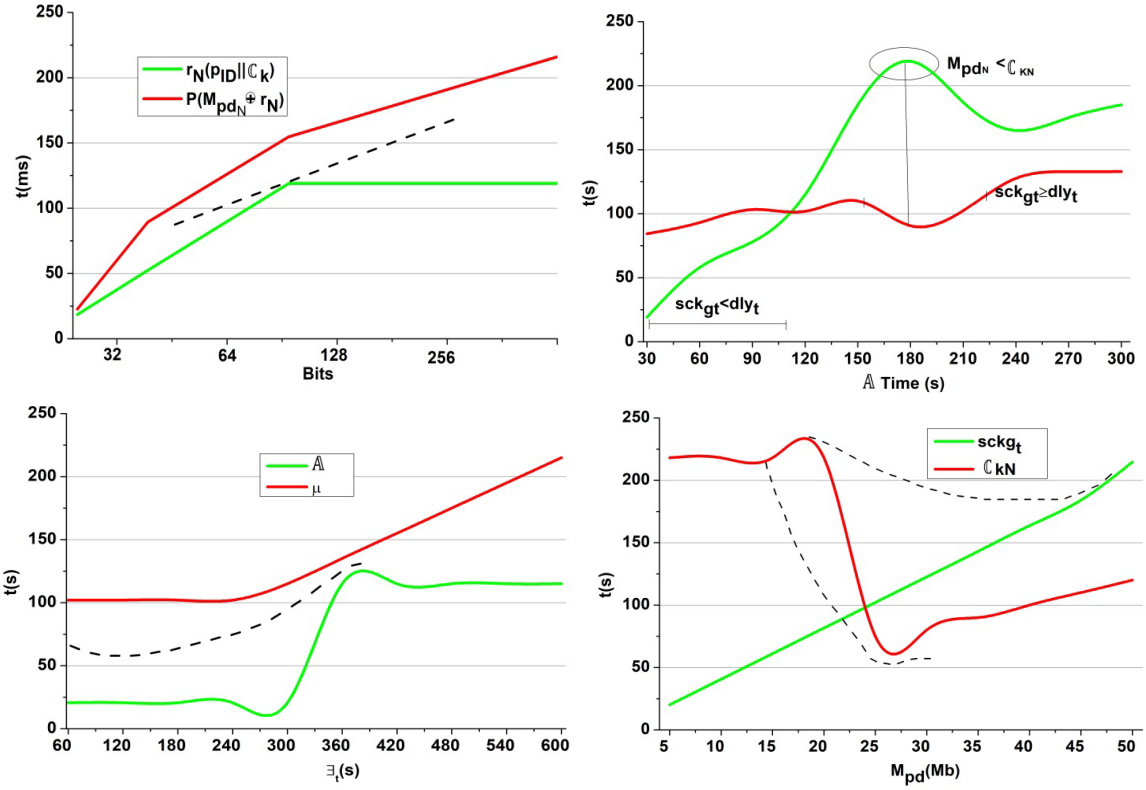


Fig 3 Δ *based* t *analysis for different variants*

The sending and receiving keys are used for integrity verification; this process is performed by disjoining the agreement to improve health record management. In this paper, the conjugation key is valid until anonymous access/ changes are addressed in IoMT. The framework is implemented to augment data authentication signature and their existence with the consensus data. Based on the shared security, the patient-monitored data is authenticated from forgery. This framework provides different authentication based on varying patient data. Using Lightweight authentication and validation, the time for authentication is reduced (Fig. 3). This signcryption key-sharing security is distinct for both $M_{pd_N} = \mathbb{C}_{K_N}$, $M_{pd_N} < \mathbb{C}_{K_N}$ and $M_{pd_N} > \mathbb{C}_{K_N}$ scenarios. From the instance, the first condition of $M_{pd_N} = \mathbb{C}_{K_N}$ is modeled as a conjugated function for authenticating the patients on both ends using the conjugated key and private key. Second condition, $M_{pd_N} < \mathbb{C}_{K_N}$ is modeled as a sequential function for authenticating the patient's data at the receiver end based on dly_tusing the public key. The third condition of $M_{pd_N} > \mathbb{C}_{K_N}$ is modeled as an intermediate function for authenticating the patient-monitored data based on conjugation time and agreement status. For all the above three conditions, the data authentication signature and key management are different in IoMT, and it follows diverse signcryption procedures. The validation process is the same for all the signcryption assignment procedures, regardless of the patient's data and delay time.

3.3 Signing Process

The data authentication signature procedure for the above conditions is discussed in the following.

Step 1: The count of patient-monitored data matches the number of conjugated keys generated.

Solution 1: This is an ideal condition, where the deficiency of conjugated keys is not met, the sharing security requirement is utilized to protect the sensitive patient health data at both the sender and receiver ends. Here, the tracking level $Track_L$ of the neural network is determined based on M_{pd} or $\mathbb{C}_K$.

In the above representation, μ_o represents the data authentication signature employed by the proposed framework that serves as the input for the $Track_L$ identification. The output of $\mu(.)$ is as $\{\mathbb{C}_{K_1}, \mathbb{C}_{K_2}, \ldots \mathbb{C}_{K_N}\}$ that is assigned for the patient-monitored data at both ends using a conjugated key and a private key. This means, the authentication signature μ_p and the monitored data assigned for signcryption is seamless. This authentication is regardless of additional sharing security requirements. In the process of data sharing, $\forall M_{pd} = \mathbb{C}_K$then, the sender and receiver devices process as follows.

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

$$\left.\begin{array}{c}\left[\mathbb{C}_{K_N} \times \mu_o|r_N|\right]\|\left[\Delta(M_{pd}) * G_N * sck_i|r_N\right]\|\left[\Delta(M_{pd}) \times \mu_p|r_N\right] \\ where, \\ sck_i = \left[A_k^o \oplus \left(B_k^o \frac{1}{\mu_N}(Track_{L-1})|r_N|\right)\right]\end{array}\right\} \quad (4)$$

Where, sck_i denotes the shared secret key and G is the generator used in both public and private keys A_k^o and B_k^o. This security sharing makes use of the first conjugated key generation, count up to N. In equation (4), the format of secured patient data is shared from the sender to the receiver devices, and it updates the condition of $\left[\left(\Delta(M_{pd}) \times \frac{1}{\mu_N}\right) \times |r_N| \oplus A_{Nq}B_{Nq}\right]$ to the proposed framework to address that the patient-monitored data is authenticated with its private key and public key. Therefore, the condition of $\left[\Delta(M_{pd}) * G_N|r_N|\right] \oplus \left[A_{Nq} \oplus B_{Nq}\right] \frac{1}{\mu_N}$. It is the sequence of sharing security keys for the sending and receiving of patient data. The sending and receiving ofpatient's data through the cloud makes use of it's A_{Nq} and B_{Nq} sequence for integrity validation and authentication verification. As in equation (4), the monitored patient data is shared through the cloud; it follows the sharing security requirements of the data authentication signature represented. This conjugated factor is different for the two cases below. It follows a sequential and time-based authentication process.

The LWAVF uses one-track neural learning in IoT and medical settings to improve data authentication efficiency and security. It reduces computational complexity and improves real-time performance by simplifying the neural network-based learning model to employ a single, focused tracking path instead of multiple paths or complex layered processing. Traditional neural networks extract information, evaluate input, and predict outcomes using multiple layers or pathways (multi-track). One-Track Neural Learning uses a single processing path to learn authentication and validation signatures in LWAVF. This neural network learns and tracks authentication factors like key generation, data signatures, and secure communication patterns for transferring patient health data between devices and healthcare centers. One-track neural learning plays a key role by

1. The neural network tracks data signatures during encryption or signing to ensure validation at both the sender's and receiver's ends.
2. The one-track approach simplifies the learning process, minimizing computational load for real-time authentication in resource-constrained IoT environments.
3. Simplifies sequence generation and authentication signature sequences based on current and past data states, ensuring data integrity and trust in the source.
4. The model adapts to varying data sizes and security needs, making it effective for dynamic patient data authentication.

Pseudocode: One-Track Neural Learning in LWAVF
Input: M_{pd}, K_{sig}, K_{val}
Output: Authenticated data
Step 1: Initialize OneTrackNeuralModel()
Step 2: encode $M_{pd} \rightarrow E_{pd} \leftarrow encrypt(M_{pd}, K_{sig})$
Step 3: Generate signature $S \leftarrow OneTrackNeuralModel.validate(E_{pd}, K_{val})$
Step 4: transmit (E_{pd}, S)
Step 5: receive (E_{pd}, S)
Step 6: validate S using $OneTrackNeuralModel.validate(E_{pd}, K_{val})$
Step 7: if valid then
Step 8: authenticated data$\leftarrow decrypt(E_{pd}, K_{val})$
Step 9: else
Step 10: reject data

One-Track Neural Learning ensures lightweight, safe, and real-time authentication of sensitive patient health data sent across IoMT systems in the LWAVF architecture. Using a simple linear neural architecture, the method tracks encrypted data sequences and generates unique authentication signatures. The monitored patient data M_{pd} is encrypted using a signing keyK_{sig} to create an encrypted form E_{pd}. The one-track neural model generates a signature S from encrypted data. Signatures are tamper-proof verification tokens. The encrypted data and signature are sent to the receiving end, where a one-track neural model and validation key K_{val} validate the authenticity of the received signature. It is encrypted and accepted if the signature is validated; otherwise, it is refused to prevent breaches. By eliminating costly multi-path neural computations, this architecture reduces

computing overhead and enables the system to adapt to varying data volumes and transmission conditions. The security and efficiency of One-Track Neural Learning make it ideal for resource-constrained healthcare IoT scenarios.

Step 2: The count of patient-monitored data is less than the generated keys (i.e.) $M_{pd} < \mathbb{C}_K$

Analysis 2: In this case, the role of both private keys and public keys makes it flexible for the sender to reduce the chances of anonymous access or changes due to privacy vulnerability. The neural network tracked in this process is again used for the conjugation time-dependent authentication assignment or the sequential authentication of the patient-monitored data without increasing the computation complexity. The representation of neural network tracking follows from the authentication assignment. This secret key assignment is performed with less time and computation complexity. Let $M_{pd_N} < \mathbb{C}_{K_N}$ that follows $\frac{M_{pd}}{\mathbb{C}_K} = even\ or\ odd$ for which the data authentication signature is assigned.

The assignment provides the need for the tracking levels in authenticating the patient-monitored data in the successive transmission interval. In both $odd/even$ cases, the sequence of signcryption relies on the integrity validation (Vld) and authentication μ_o. This sequence is expressed as follows$[Vld - Track_L)/|\mu_o| + 1]$, $|\mu_o|$ is the modulus of a definite authentication signature to the data. Here, $\forall 1 \leq M_{pd} < \mathbb{C}_K$ is the condition for meeting the sharing security requirements using conjugation time and agreement status is as follows

$$\left[\Delta(M_{pd}).\mu_o\right] \times \left[\left|r_{N_{\mathbb{C}_K}}\right| \frac{1}{M_{pd} - \mathbb{C}_K} || \oplus B_{Nq}\right] = \left[(|r_N| \times Track_{L-\mathbb{C}_K}) \oplus A_{Nq}\right] \tag{5}$$

Now, the random number count is reduced to r_q.

Where, $q = \left(\frac{(Vld - Track_L)}{|\mu_o|+1}\right)$

Therefore,

$$\left[Track_{L_{M_{pd}-\mathbb{C}_K}}.\mu_o\right]\left[\left|r_{M_{pd}-\mathbb{C}_K}\right| \frac{1}{M_{pd} - \mathbb{C}_K} \oplus B_{M_{pd}-\mathbb{C}_K}\right] = \left[\left|r_{M_{pd}-\mathbb{C}_K}\right| * Track_{L_q} \bigoplus A_{M_{pd}-\mathbb{C}_K q}\right] \tag{6}$$

As per the equation (5) and (6) the sequence of $G = \{1\ to\ M_{pd} - \mathbb{C}_K\}$ is processed to protect the patient's health data. The above validation helps to compute the sequence of sharing data without assigning keys. Therefore, the additional computation of the patient data $(M_{pd} - \mathbb{C}_K)$ is not required. Based on the instance, the sequence is to be preserved at the time of odd is observed in any case. In this condition, the authentication sequence output follows $sck(1, \mathbb{C}_K - M_{pd})$ such that several iterations and conjugations are addressed. Contrarily, the authentication signature is different for the even condition; it is represented as $q - 2(\mathbb{C}_K - M_{pd})$ is the authentication sequence considered. This authentication signature sequence is given as in equation (7)

$$\left.\begin{aligned}\left[\Delta(M_{pd}).\mu_o\right] \times [r_q \frac{1}{Track_{L-q}} || \oplus B_{Nq}] &= \left[|r_N| Track_{L-q} \oplus A_{Nq} \oplus B_{Nq}\right] \\ \left[Track_{L-q}.\mu_o\right] \times [r_q \frac{1}{Track_{L-q}} || A_{Nq} \oplus B_{Nq}] &= \left[|r_q| Track_{L-q} \oplus A_{Nq} \oplus B_{Nq}\right]\end{aligned}\right\} \tag{7}$$

The above equation follows the nearest possible authentication and integrity validation is required for assigning the appropriate key to the data. Therefore, the validation need not be complete for two mappings $\mu = \{0\ to\ Track_L - M_{pd}\}$ and $\mu = \{0\ to\ M_{pd}\}$. From the above condition, $M_{pd_N} < \mathbb{C}_{K_N}$ is considered to improve the sequential authentication rate with less complexity.

Step 3: The generated keys are not sufficient to meet the sharing security requirements of all thepatients' data (i.e.) $M_{pd_N} > \mathbb{C}_{K_N}$.

Analysis 3: In this condition, the preference of authentication process to patient-monitored data signature is initiated with mappings and integrity (i.e.) $(\mathbb{C}_K - M_{pd})$ or from $\mu = \{0\ to\ Track_L - M_{pd}\}$ and $\mu = \{0\ to\ M_{pd}\}$. The mapping condition of $\mu = \{0\ to\ Track_L - M_{pd}\}$ and $\mu = \{0\ to\ M_{pd}\}$ are similar to above step 1. This authentication signature is used for the successive data sharing from the sender to receiver devices.

This authentication sequence based on conjugation and sequence is required to proceed with the consensus mechanisms to monitor the mapping of time, agreement status,sender's data count, andreceiver's data count for better integrity. Therefore, the sequence of authentication signatures is provided for all the patients. Here, the mapping m_n and integrity $intg_n$ are the considerable factors. If conjugated time $\mathbb{C}_t$ is computed for the first authentication sequence, then the time for generating the secret key sck_{gt} is used for serving the conditions $\mu =$

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

$\{0\ to\ Track_L - M_{pd}\}$ and $\mu = \{0\ to\ M_{pd}\}$. The authentication sequence is initiated from the time of $(\mathbb{C}_t - sck_{gt})$. Hence, the consensus mechanisms are represented from$(\mathbb{C}_t - sck_{gt})$ and Vld is as follows

$$\left.\begin{gathered}\left[\Delta(\mathbb{C}_K - M_{pd}) \times \mu_o |r_{q-p}|\right] || \left[m_n.intg_n \times \mathbb{A}_o G_{M_{pd}-\mathbb{C}_K-1} \middle| r_{q-p}\right] \\ \forall\ \mathbb{C}_t \geq sck_{gt}\ and\ q-p \neq 0 \\ \left[|r_{q-p}| \frac{1}{m_n.intg_n} \oplus B_{Nq}\right] = \left[|r_{q-p}| \oplus A_{Nq} \frac{1}{M_{pd} - \mathbb{C}_K - 1}\right]\end{gathered}\right\} \tag{8}$$

Similarly,

$$\left.\begin{gathered}\left[\mathbb{C}_{K_1} \times \mu_o \left|r_{q-M_{pd}}\right|\right] \left\| \left[Track_{L_{q-M_{pd}}}.\mathbb{A}_o G_{q-M_{pd}}\right] = \left[A_{Nq} \oplus B_{Nq}\right] \right\| Track_{L_{q-M_{pd}}}.G_{q-M_{pd}-1}|r_{q-p}| \\ \vdots \\ \left[\mathbb{C}_{K_N} \times \mu_o |r_p|\right] \left\| \left[Track_{L_q} \mathbb{A}_o G_q\right] = \left[\left[A_{Nq} \oplus B_{Nq}\right] \right\| Track_{L_q} G_q |r_{\mathbb{C}_K}|\right]\end{gathered}\right\} \tag{9}$$

As per the above equations, the sequence of authentication based on conjugation time and agreement status is used to match the consensus data for differentiation. The mapping time between the sequences is addressed by assigning sequential data authentication signatures such that the consensus mechanism is deployed to reduce the anonymous access/ changes. The mapping process constraints are described below.

Discussion 1 Constraint Description for Mapping

The mapping of the parameters is satisfied when $\mathbb{C}_K \rightarrow M_{pd}$ if $M_{pd} = P\left(M_{pd_N} \oplus r_N\right)$ where $\mathbb{C}_t = 0$ and $\mathbb{A} = \varepsilon_{min}$,

$$M_{pd} = r_N \times (\alpha(Vld) + \beta(Vld) + \gamma(Vld)) \times \left(\frac{1}{Track_L}\right) \times \left[\left(\left|M_{pd} - \mathbb{C}_K\right|^2\right) + \left|A_{Nq}\right|^2 + \left|B_{Nq}\right|^2\right] \Longrightarrow r_N \geq r_{N,min}$$

$$= r_N$$

$$\mathbb{C}_t = sck_{gt,min} \times \left(1 - \frac{dly_t}{t_{max}}\right) = 0 \Longrightarrow t_{max} = sck_{gt,min} \times (t_{max} - \exists_t)$$

Combining $dly_t = 0$ and $\varepsilon = \varepsilon_{min}$ with $r_N = \left(\frac{sck_{gt}}{\exists_t \times p_{ID}}\right) + \mathbb{C}_K \times (\alpha(Vld) + \beta(Vld) + \gamma(Vld)) \times \left(\frac{1}{t_{max}}\right) \times [(|\mathbb{C}_t - \mathbb{A}|^2) + |\mathbb{C}_t|^2 + |\mathbb{A}|^2]$

Substitute $\mathbb{C}_K = \varepsilon$ if $\mathbb{C}_K = 0$, where ε is the mapping of $\mathbb{C}_t + \mathbb{A} = \Delta\left(M_{pd}\right)$

$\alpha(Vld) = \mathbb{C}_t \times log(1 + \varepsilon) + \mathbb{A} \times \left(\Delta\left(M_{pd}\right) \times dly_t\right) \Longrightarrow \Delta\left(M_{pd}\right) = m_n(Track_L) - m_n(\mathbb{C}_t - \Delta t)$

The mapping process will affect the condition $\varepsilon \geq \varepsilon_{max} = m_n$ along with $\Delta\left(M_{pd}\right) > r_N$, therefore,

$$\left[\varepsilon = \frac{\varepsilon - \varepsilon_{min}}{\varepsilon_{max} - \varepsilon_{min}} \Longrightarrow \varepsilon = \varepsilon_{min}\right] = \max_{r_N} m_n \Longrightarrow \mathbb{C}_t \times log(1 + \varepsilon) + \mathbb{A} \times \left(\Delta\left(M_{pd}\right) \times dly_t\right)$$

The actual mapping is performed as $m_n = \frac{m_n - m_n^{min}}{m_n^{max} - m_n^{min}} \rightarrow m_n^{min} \geq m_n = \mathbb{C}_t$ when $\mathbb{C}_t \rightarrow sck_{gt}$ that maintains mapping even in varying patient data.

After the authentication, data integrity validation is performed by disjoining the agreement after differentiating the consensus data at the receiver end. This performance ensures the non-altering of sensitive patient health data between the sender and receiver ends through the cloud without complexity. The secure sharing process between the sending device and the healthcare center is illustrated in Fig. 4.

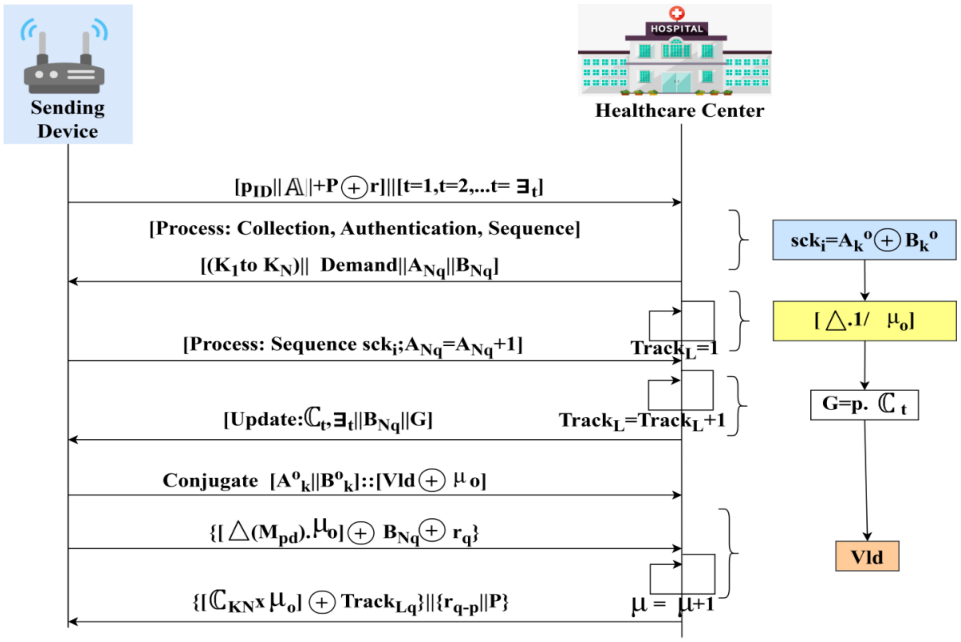


Fig. 4 *Secure sharing process between the sending device and the healthcare center*

The secure sharing process is initiated using $p_{ID} \forall\, t = 1$ to $\exists_t$ for which the processes of collection, authentication, and sequence are pursued. In this step, M_{pd} is collected to meet the demands of $\exists_t$ such that $\left[sck_i = A_k^{\circ} \oplus B_k^{\circ}\right]$ is the initial authentication key for sharing. If this authentication is valid, then $\left(\Delta . \frac{1}{\mu_o} = 1\right)$ is the satisfying condition. If this condition is not satisfied, then $(G = P.\mathbb{C}_t)$ Is the new generator equivalent to performing a conjugation operation? Besides the $\left(B_{Nq} \oplus rq\right)$ equivalent to $\left(A_{Nq} \oplus Track_{L_q}\right)$ is the validation condition to increment μ by 1. Therefore the Vld process is performed from $Track_L = 1$ to $Track_L = Track_{Lq}$. This update reduces overhead by relying on $Track_L$ or B_{Nq} and the analysis is given in Fig. 5.

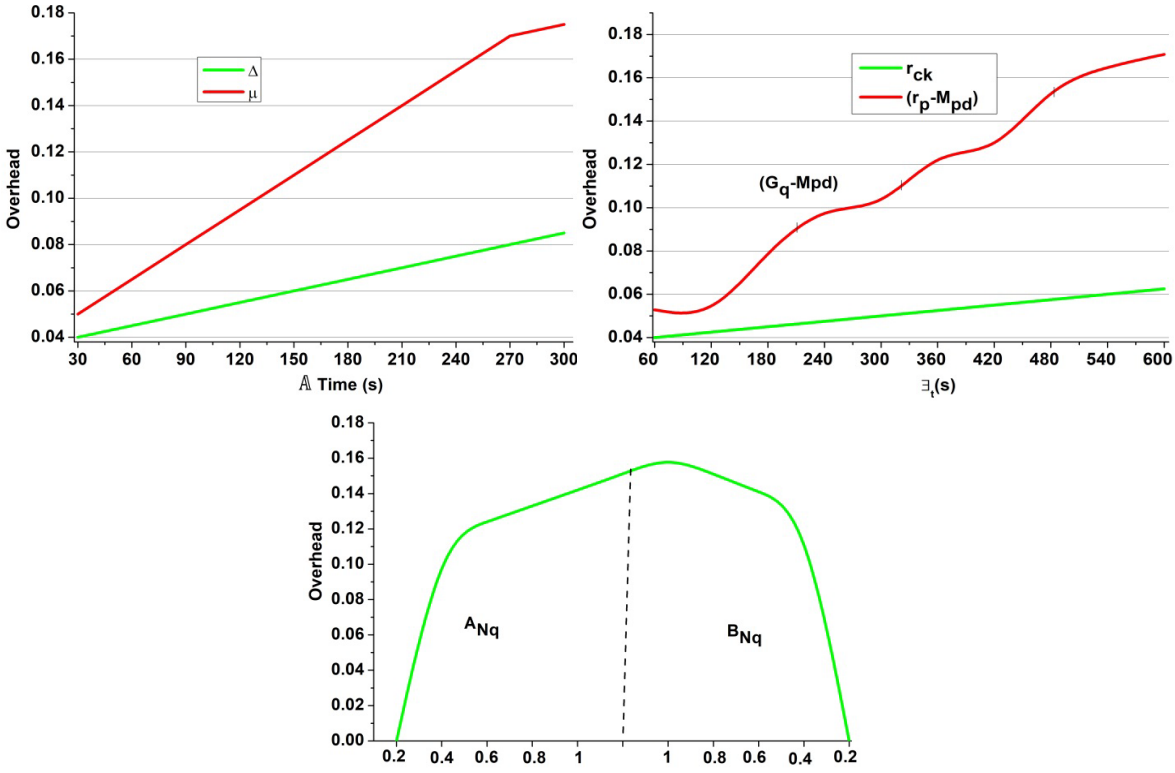


Fig. 5 *Overhead analysis for different variants*

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

The additional authentication is provided for the data when the joining key is identified using one-track neural learning. This authentication overhead is suppressed through consensus mechanisms. The sending key and receiving are matched to identify the disjoin key accurately. The validation of mapping is performed to identify authentication overhead in this data transmission. The tack level of the shared patient health data is obtained through encryption. In this framework, the protection of sensitive health data is pursued based on tacking level, which reduces authentication overhead (Fig. 5). Following the above analysis, the consensus functions for mapping conjugated keys and M_{pd}, are presented in Fig. 6.

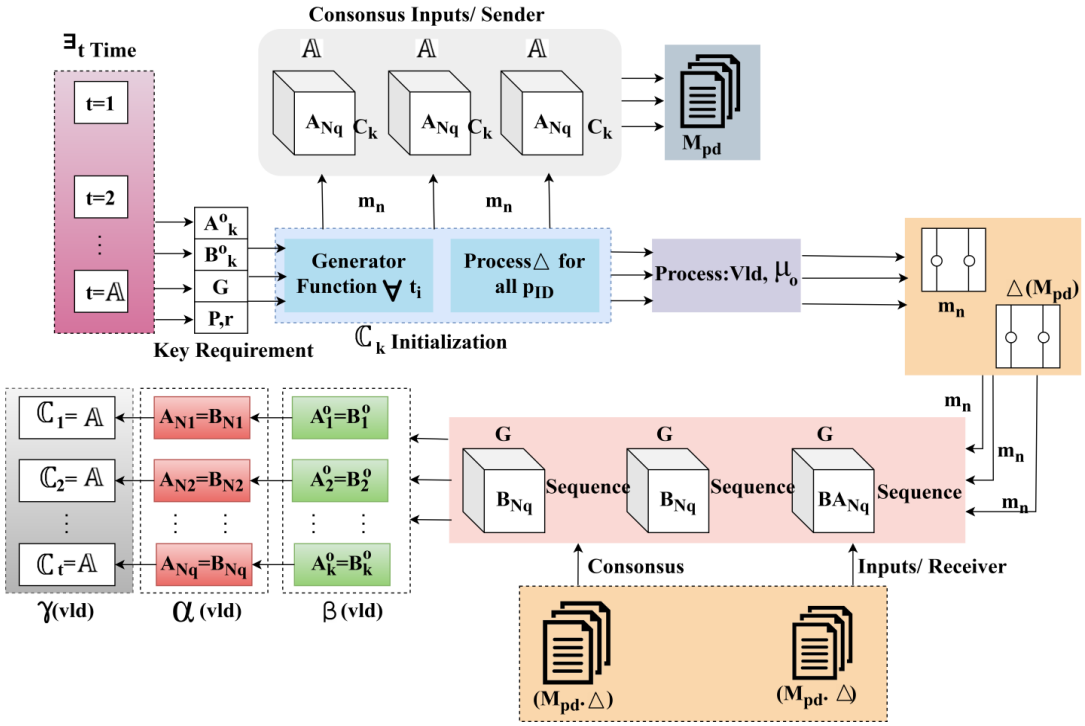
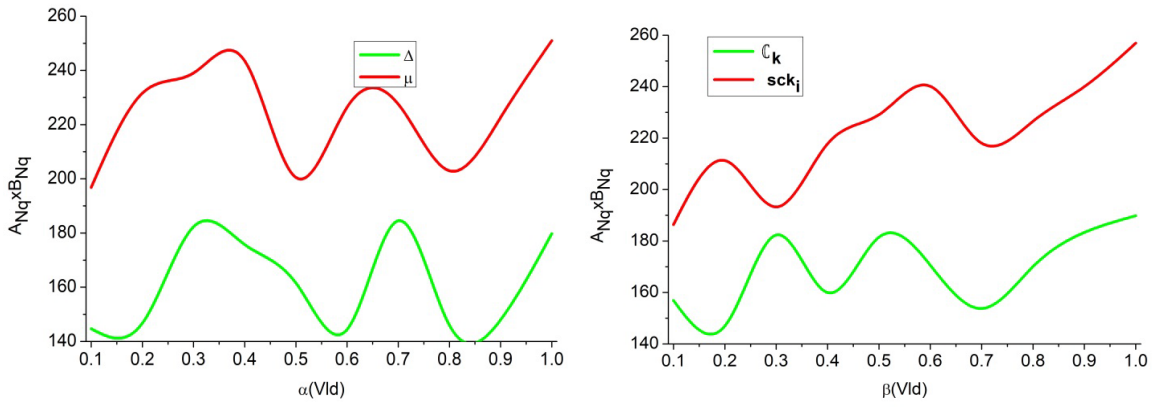


Fig. 6 *Consensus functions for mapping conjugated keys and* M_{pd}

The consensus functions for mapping using $\mathbb{C}_k$ and M_{pd} is described using Fig. 6 above. The $t = \mathbb{A}$ is the increasing time interval for initial key requirements $(A_k^{\circ}, B_k^{\circ})$ and $[G = (P, r)]$. Based on this key requirement, the generator function creates the maximum possible t_i bound $\mathbb{C}_k$. In this case the initialization for Δ conceding P_{ID} is utilized (enclosed) for authentication. The m_n the process is performed for $(A, A_{Nq}, \mathbb{C}_k) \forall M_{pd}$ such that (Vld, μ_a) are the mapping process. This is proceeded using $\Delta(M_{pd})$ such that the consecutive (receiver end) m_n is used to map $G(B_{Nq}, and\ Sequence)$. The verification phase requires $\alpha(Vld), \beta(Vld)$ and $\gamma(Vld)$ obtained from $(A_k^{\circ}, B_k^{\circ}), (A_{Nq} = B_{Nq})$, and $(\mathbb{C}_t = \mathbb{A}) \forall m_n$. Therefore, the authentication and integrity verification rely on mutual $\mathbb{C}_k$ initialization. Hence the m_n variants are validation for nearly $(A_{Nq} \times B_{NQ})$ sequences from which the following assessment is presented.



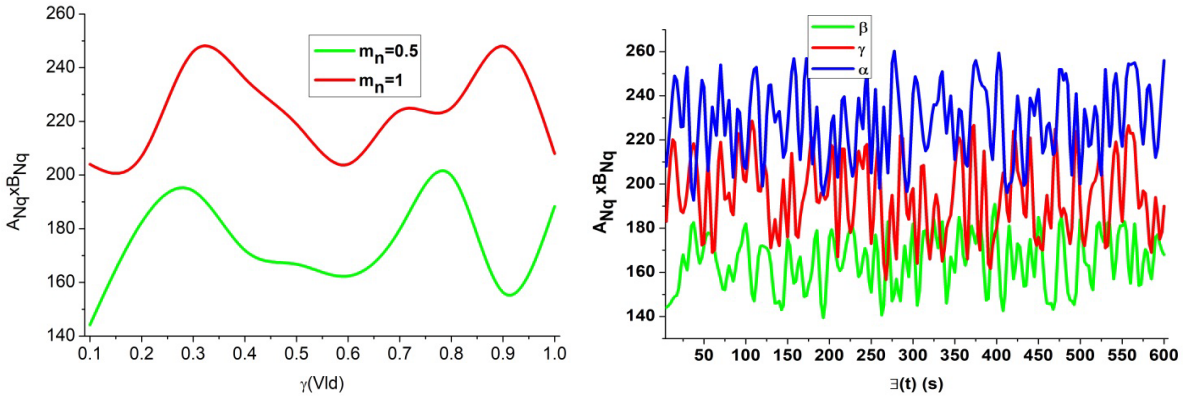


Fig. 7 $A_{Nq} \times B_{Nq}$ *analysis of different mapping variants*

This model is primarily used for enhancing health record management and diagnosis support through secure one-track neural learning with feasible authentication. Integrity verification is conducted at the receiver end to deploy a consensus mechanism that monitors mapping time, agreement status, sender's data count, and receiver's data count. This verification process decreases the need for authentication checks. Additionally, it mitigates generator complexity in data sharing by utilizing track levels and modifying the key at the receiver end through learning. Less consensus mapping occurs due to anonymous modifications/access to patient data. Compared to other factors, consensus mapping is more pronounced in this model (Fig. 7).

3.4 Integrity Validation

For the different conditions, the data integrity validation is performed by disjointing the agreement unanimously through one-track neural learning. In this process, the factors of $\Delta(M_{pd})$ and μ are served input to the one-track learning makes use of the private and public keys at the receiving device. Let $\alpha(Vld)$, $\beta(Vld)$ and $\gamma(Vld)$ are the matching, validation, and agreement status validation are modeled based on conjugation time is expressed as

$$\alpha(Vld) = \{0,1\}^{M_{pd}} = \{0,1\}^{\mathbb{C}_K + log|q|-1} \forall M_{pd_N} \leq \mathbb{C}_{K_N} \tag{10}$$

$$\beta(Vld) = \{0,1\}^{q-M_{pd}} \oplus \{0,1\}^{q} \tag{11}$$

And,

$$\gamma(Vld) = \{0,1\}^{q-M_{pd}+loh|q|-1} \oplus \{0,1\}^{q+log|q-\mathbb{C}_K-1|} \forall\, M_{pd_N} > \mathbb{C}_{K_N} \tag{12}$$

In the above equations, the validation is performed based on time, and the delay for the receiving data is defined. If ε is the sequence of receiving data, then the mapping is processed as

$$\left.\begin{matrix} if\ \{M_{pd_1}, M_{pd_2}, \dots M_{pd_N}\} = \{\varepsilon_1, \varepsilon_2, \dots \varepsilon_N\} \forall M_{pd} \leq \mathbb{C}_K \\ else \\ \{M_{pd_1}, M_{pd_2}, \dots M_{pd_{p-N+1}}\} \oplus \{M_{pd_{p-N+1}}, M_{pd_{p-N+2}}, \dots, M_{pd_p}\} = \{\varepsilon_1, \varepsilon_2, \dots \varepsilon_{p-N}\} \oplus \{\varepsilon_1, \varepsilon_2, \dots \varepsilon_N\} \end{matrix}\right\} \tag{13}$$

Now, the validation is modeled as in equation (14)

$$\left.\begin{matrix} r_N \leftarrow \varepsilon \in \alpha(Vld) \\ such\ that \\ [\Delta(\mathbb{C}_K) \times \mu_o |r_N|] \left|\left| [\Delta(M_{pd}) \mathbb{A}_o |r_N|] \right|\right| \left[\Delta(M_{pd}) Track_{L_p} |r_N|\right] = \left[M_{pd_1}(p, r_N), \dots, M_{pd_{log|q|}}(p, r_N)\right] \end{matrix}\right\} \tag{14}$$

The verification is pursued following the matching and agreement status validation for the sequence $\varepsilon_N \leq M_{pd}$. If this validation exceeds the conjugated time, then the mapping is validated such that

$$\left.\begin{matrix} \left[\Delta(\mathbb{C}_K - M_{pd}) \times \mu_o |r_q - p|\right] \left\| \left[Track_{L_{\mathbb{C}_K - M_{pd}-1}} \mathbb{A}_o |r_{q-p}|\right] \oplus \left[\Delta(\mathbb{C}_K) \mu_o |r_q|\right] \right\| \left[Track_{L_{q-p-1}} \mathbb{A}_o G_S\right] = \\ \left[G_1(M_{pd}, \varepsilon), \dots, G_{log|M_{pd}-\mathbb{C}_K|}(q-1, \varepsilon)\right] \oplus \left[G_{log(M_{pd}-\mathbb{C}_K+1)}(q-1, \varepsilon), \dots, G_{log|p|}(q-1, \varepsilon)\right] \end{matrix}\right\} \tag{15}$$

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

The validation process for the sequence of authentication is performed to ensure that the conjugation is valid. Here, matching the consensus data for mapping the parameters to verify the integrity, ensuring the modifications over the data do not influence the authentication sequence and conjugation. For any order of sending and receiving the data, the validation is performed under its track neural network without additional time. The integrity validation constraints are discussed below.

Discussion 2: Integrity Validation Constraints

The integrity validation is mandatory to avoid changes in $\varepsilon_{max}\ and\ \varepsilon_{min}$ that provides $\mathbb{C}_t \neq dly_t$ where $intg \propto \frac{\mathbb{C}_K}{M_{pd}}$

$intg(t) = \mathbb{C}_t + intg + (\mathbb{C}_t - \mathbb{A}) - (\varepsilon \times \exists_t)$ is substituted in $\mathbb{C}_t = \left|m_n - \Delta(M_{pd})\right|^2$

Then $intg(t) \Longrightarrow intg(t) = \left|m_n - \Delta(M_{pd})\right|^2 + intg + (\mathbb{C}_t - \mathbb{A}) - (\varepsilon \times \exists_t)$ and

Substitute $intg = \left[(r_N \times \mathbb{C}_t) + \min\left((\mathbb{A} \times m_n)\right) - \left(1 - (\varepsilon \times \mathbb{C}_t)\right)\right]$

Then $intg(t)$ becomes $intg(t) = \left|m_n - \Delta(M_{pd})\right|^2 + \min\left((\mathbb{A} \times m_n)\right) - \left(1 - (\varepsilon \times \mathbb{C}_t)\right)$

Based on the previous m_n substitute $\mathbb{A} = 0$ and $\varepsilon = \varepsilon_{min}$ to obtain $M_{pd} = r_N \rightarrow intg(t)$

If $intg(t) = 1$ in any case, then

$$(\mathbb{C}_K = r_N) \Longrightarrow \mathbb{C}_t \times \log(1+\varepsilon) + m_n \times \left(\Delta(M_{pd}) \times \exists_t\right) = r_N \times (\mathbb{C}_t + m_n) \times \left(\frac{1}{Track_L}\right) = 1$$

If $intg(t) > 1$ in any case, then

$$(\mathbb{C}_K > r_N) \Longrightarrow \mathbb{C}_t \times \log(1+\varepsilon) + m_n \times \left(\Delta(M_{pd}) \times \exists_t\right) > r_N \times (\mathbb{C}_t + m_n) \times \left(\frac{1}{Track_L}\right) \times \min\left((\exists_t \times m_n)\right) > 1$$

If $intg(t) < 1$ in any case, then

$$(\mathbb{C}_K < r_N) \Longrightarrow \mathbb{C}_t \times \log(1+\varepsilon) + m_n \times \left(\Delta(M_{pd}) \times \exists_t\right) < r_N \times (\mathbb{C}_t + m_n) \times \left(\frac{1}{Track_L}\right) < 1$$

The above derivation verifies the data integrity using the constraints of $\mathbb{C}_K = r_N \rightarrow intg(t)$ to meet the sharing security requirements. In this validation, disjoining the agreement after matching the sending and receiving key with the consensus data for providing accurate and appropriate authentication.

The validations for integrity and authentication verifications are presented in Figs. 8 and 9 accounting for the different factors related to security.

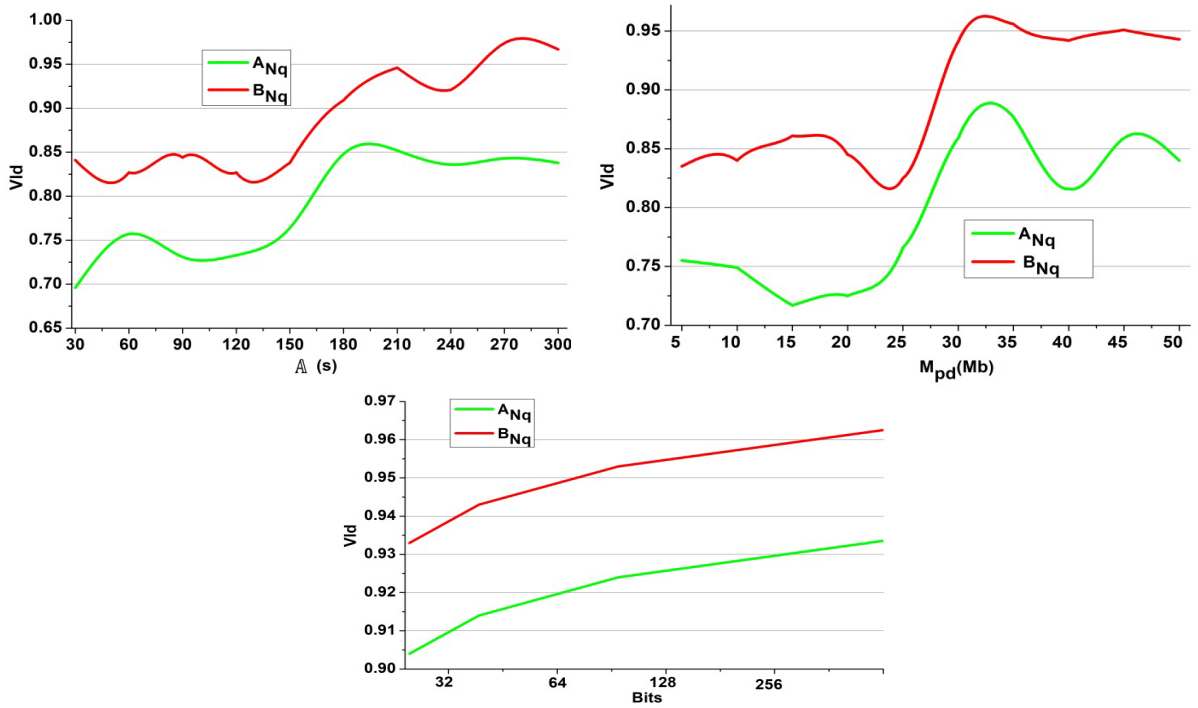


Fig. 8 *Integrity verification analysis*

In this verification, patient-monitored data shared through the cloud platform is managed to identify anonymous access and changes in IoMT. In this framework, the consensus mechanism is applied to reduce the additional authentication and joining conditions by validating the support integrity. The data integrity is validated for shared data in the cloud to ensure better authentication. During patient data sharing between the clouds, if any security vulnerability occurs, then the appropriate authentication is provided to prevent anonymous changes to the data. The tack levels are modified based on mapping and agreement status, which increases integrity verification (Fig. 8).

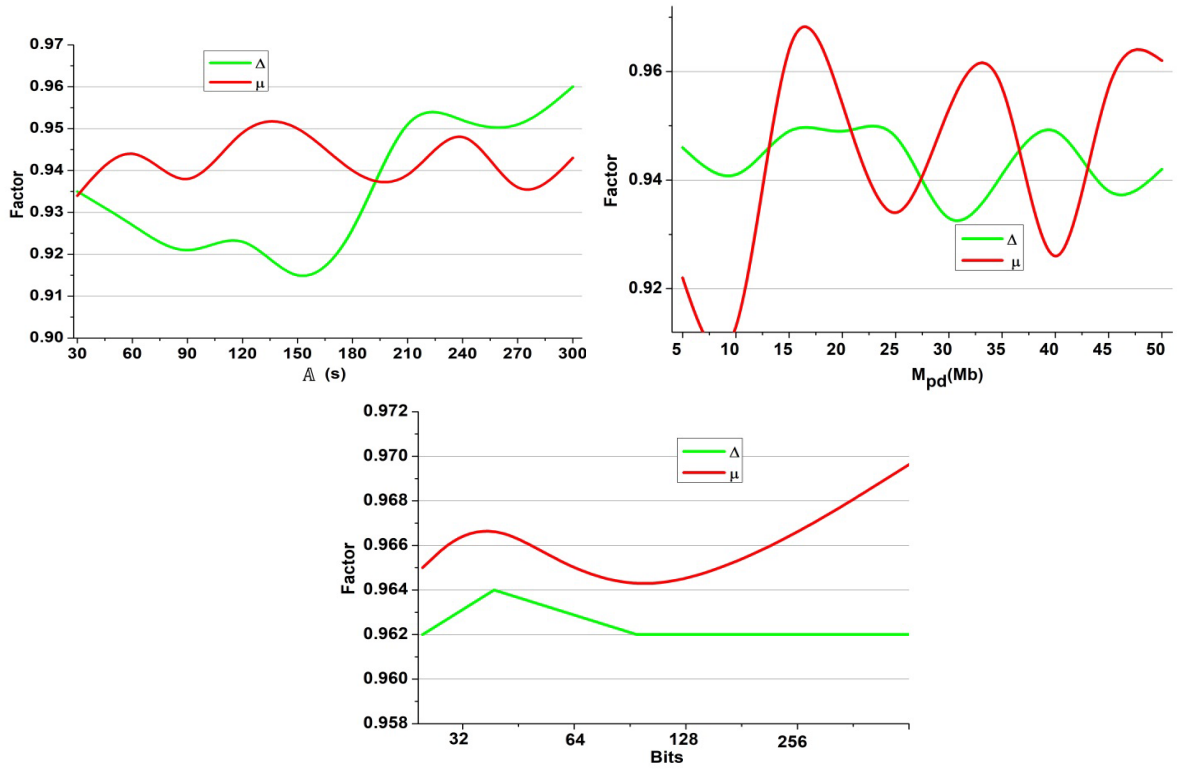


Fig. 9 *Authentication verification analysis*

The Δ time requirements are validated for t requirement using the bits, $\mathbb{A}$ time, $\exists_t$ and M_{pd} variants. The $r_N[P_{ID}\|\mathbb{C}_K]$, and $P\left(M_{pd_N} \oplus r_N\right)$ are the variants for the bits. The $\left(M_{sd_N} = \mathbb{C}_{K_N}\right), \left(sch_{gt} \geq dly_t\right), (\mu, \mathbb{A})$, and $\left(sck_{gt}, \mathbb{C}_{k_N}\right)$ variants are used to analyze the authentication time. These authentication time variants are analyzed for $p_{ID} \in M_{pd} \leq \mathbb{C}_K$ provided the time constraints are utilized for $\mu(.)$ and $Track_L$. Therefore the μ_p is the Δ influencing factor to ensure (r, p) based on outputs across conjugated processes. The conjugated process assimilates $\left(sck_{gt}, \mathbb{C}_{K_N}\right)$ inputs for validating the authentication process. In this process, the assignment of authentication follows tack levels to meet the shared security requirements. The signcryption process is distinct for three conditions (i.e.) $M_{pd_N} = \mathbb{C}_{K_N}$, $M_{pd_N} < \mathbb{C}_{K_N}$ and $M_{pd_N} > \mathbb{C}_{K_N}$ to perform authentication verification. The track level of the shared key is analyzed for monitoring the mapping of time and agreement status through lightweight authentication for the sequence, and the best level is updated and stored from the previous record for future use (Fig. 9).

4. Analysis and Discussion

The discussion is presented using an experiment involving two individual wireless devices connected through a 2.4 GHz wireless channel. The operating bandwidth is 100 Mbps to facilitate raw data sharing for analysis. The health monitoring system dataset from [38] is utilized to enable communication between the devices. This dataset offers monitored information on heart rate, pulse, temperature, oxygen levels, blood pressure, respiratory rates, pH levels, and more. To simulate low-power IoMT edge nodes, Raspberry Pi 4 Model B devices with 4GB RAM and quad-core Cortex-A72 processors were employed. The ultra-lightweight performance of ESP32 microcontrollers and Python 3.10 has been harnessed to construct the software environment. AES-256 encryption and digital signature verification were implemented using PyCryptodome, while neural learning components were developed using TensorFlow Lite for edge-optimized execution. The MQTT protocol simulated a real-time sensor-to-gateway connection with lightweight data transport. Hyperledger Fabric was used to replicate a cloud and

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

decentralized storage architecture to test consensus and integrity. This combined hardware-software environment evaluated LWAVF under realistic network, processor, and latency constraints, demonstrating its suitability for scalable and secure IoMT deployments. Table 2 lists the hyperparameter settings employed in this research.

Table 2 *Hyperparameter settings tabulation*

Hyperparameter Variable	Value	Description
Learning Rate	0.001	Step size for updating model weights during training.
Epochs	100	Total number of training iterations.
Batch Size	32	Number of samples processed before the model is updated.
Early Stopping Patience	10	Number of epochs without improvement before training is halted.
Dropout Rate	0.5	A fraction of neurons is set to zero during training to prevent overfitting.
Input Dimensions	Varies (dependent on data)	Number of features in input data (e.g., patient attributes).
Consensus Time Window, $\exists_t$	600 seconds	Time frame for tracking data consensus.
Log Validity Duration $\mathbb{A}$	300 seconds	Duration for which logs are maintained before invalidation.
Maximum Patient Data M_{pd}	50 MB	The maximum size of patient data shared in a single instance.
Key Size Variation	32 – 256 bits	Range of key sizes used for AES-256 encryption in data validation.
Wireless Channel Frequency	2.4 GHz	Frequency used for wireless communication between devices.
Operating Bandwidth	100 Mbps	Bandwidth available for data sharing between devices.
Total Raw Data Entries	4,286	Number of entries in the health monitoring dataset.
Health Monitoring Parameters	Heart rate, pulse, temperature, oxygen levels, blood pressure, respiratory rates, and pH levels	Patient health indicators are monitored through IoMT.

In this experiment, two wireless devices operating on a 2.4 GHz channel share data efficiently, utilizing a 100 Mbps capacity. The 4,286-entry health monitoring dataset encompasses essential characteristics, including heart rate and blood pressure. Device 1 captures patient data M_{pd} and communicates it with Device 2 using AES-256 for data validation, assuring data integrity and authentication. Logging is essential for the experiment, with logs kept for $\exists_t$ (600 seconds) and $\mathbb{A}$ (300 seconds) to track actions and handle data. This architecture enables rigorous comparison analyses using current frameworks, maintaining the integrity of experimental results through systematic data gathering, sharing, and validation. The total raw information set available is 4286, and the same information is queried using a PHP-designed interface. The data communication/ sharing, experimental method, and data are represented in Fig. 10.

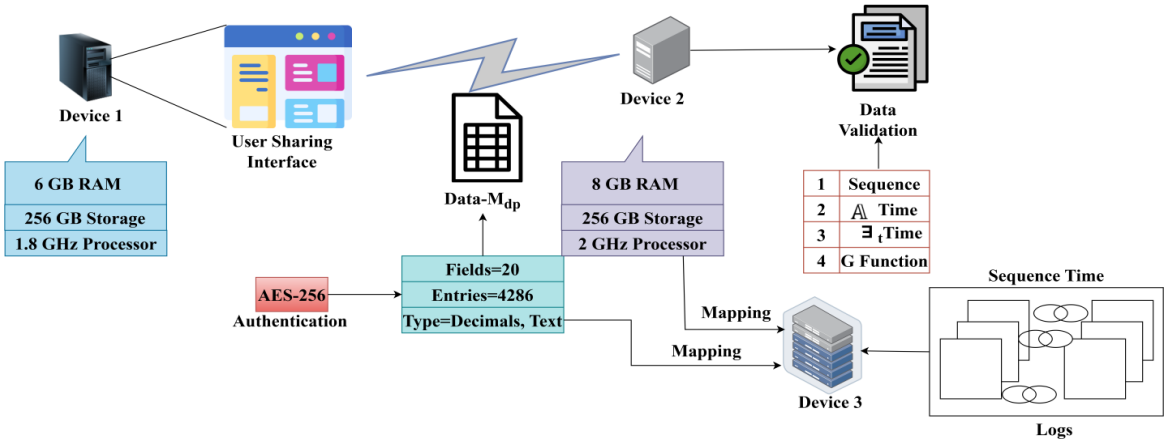


Fig. 10 *Data sharing and representation*

The user-sharing interface accumulates M_{pd} from Device 1 and shares it with Device 2 for validation. Device 1 performs Δ using AES-256 Authentication, and the same is used for data validation (integrity & Authentication check). A separate device is used for sequence and time mapping for different Device 1 and Device 2 entries as logs. The logs are saved throughout $\exists_t$ or until $\mathbb{A}$ is valid. In this experimental setup, $\exists_t$ is set as 600s and $\mathbb{A}$ as 300s, for which the key size is varied from 32 bits to 256 bits on M_{pd}. The maximum M_{pd} is 50 Mb for a maximum of 256 sharing instances. Based on this experimental setup, two parameters, the sequences and time, are comparatively analyzed using Tables 3 and 4. This comparative analysis is performed with the scalable and lightweight group authentication framework [reference 26] and blockchain-integrated security framework [reference 36], which are discussed in the related works section.

Table 4 *Consensus sequence tabulation*

$\exists_t$ (s)	Methods					
	[26]			Proposed		
	Sequences (Max)	Sequences (Min)	Complexity(ms)	Sequences (Max)	Sequences (Min)	Complexity
60	189	62	25.47	198	139	19.25
120	191	55	28.69	201	121	21.36
180	193	51	32.64	205	115	20.59
240	195	45	45.25	215	112	22.96
300	201	32	52.3	219	102	25.36
360	205	25	55.69	225	96	28.74
420	212	19	49.87	214	82	32.58
480	215	7	58.36	225	84	36.98
540	217	5	62.87	236	75	42.47
600	225	4	64.30	256	58	48.21

In this framework, patient-monitored data is secured based on integrity, authentication, validation, and verification to improve the consensus sequence. A tack level is identified to differentiate the sending and receiving keys with consensus data, thereby disjoining the agreement at the receiver end. The learning is processed to verify the mapping parameters, thereby enhancing the security of sensitive health information. In this scenario, the patient-monitored data is indirectly proportional to meet the shared security requirements, resulting in a high consensus sequence.

J. of Soft Computing and Data Mining Vol. 6 No. 1 (2025) p. 35-57

Table 4 *Latency and complexity tabulation*

Methods	Data Size (Mb)	Data Sharing(ms)	Authentication(ms)	Integrity Verification (ms)	Latency (ms)	Complexity (ms)
[36]	10	452.21	12.36	18.65	492.22	20.36
Proposed		416.35	3.22	5.98	455.55	20.15
[36]	20	545.98	86.96	92.6	735.54	25.36
Proposed		426.87	41.21	46.3	524.38	22.15
[36]	30	563.21	90.36	131.6	795.17	28.78
Proposed		431.56	36.58	55.78	533.92	25.41
[36]	40	658.36	112.71	184.36	965.43	32.47
Proposed		453.65	105.96	121.3	690.91	30.74
[36]	50	741.69	212.98	218.36	1183.03	46.17
Proposed		547.69	210.69	215.98	984.36	42.37

The data authentication signature is used to identify the privacy level of the sending and receiving devices under different conditions and verify their integrity. In the proposed framework, the validation of matching and agreement status is performed for conjugation time to ensure data integrity at the receiver end. The lightweight authentication and validation separately provide keys for all the devices in IoMT. In the first shared key, the public and private keys are generated and applied to all the patient-monitored data without complexity. Contrarily, the conditions of $M_{pd_N} = \mathbb{C}_{K_N}$ and $M_{pd_N} < \mathbb{C}_{K_N}$ used to verify the integrity of their existence to reduce latency and complexity (Table 4). In addition, the system's excellence is compared with existing methods, such as the lightweight group authentication framework (LWGA) [26], lightweight blockchain and fog-enabled security systems (LWBC) [36], and Group blind signature (GBS) [37]. The obtained system efficiency is shown in Table 5.

Table 5 *Comparative analysis of system efficiency*

Metric	LWGA [26]	LWBC [36]	GBS [37]	LWAVF (Proposed)
Authentication Time (ms)	M	H	L	VL
Data Sharing Time (ms)	M	H	M	L
Integrity Verification (ms)	M	H	M	L
Latency (ms)	M	H	L	VL
Computation Overhead (ms)	H	VH	M	L
Communication Overhead (Kb)	M	H	M	L
Scalability	M	H	M	H
Energy Consumption (mJ)	M	H	M	L

** Note: M- Moderate, H-High, L-Low, VL-Very Low, VH-Very High*

The LWAVF can be trusted to perform well because it is well-suited for IoMT integrations, as described in Table 5. In contrast to LWGA, due to its non-dependence on moderate computer resources, as it uses cryptographic algorithms which are incomparably lightweight, as well as low. As a result, both the data-sharing time and the authentication time are significantly reduced. Furthermore, it outperforms both the low-light blockchain and fog-enabled systems by optimizing resource utilization, which enables it to eliminate lag and ensure real-time data sharing. When comparing it to a group blind signature, LWAVF proves to be more efficient due to the fact that the streamlined algorithms it uses have an uncompromising degree of security, yet are sufficiently fast. Lastly, LWAVF is energy-efficient because it scales accordingly and utilizes resources efficiently, thereby guaranteeing low-latency communication while maintaining a secure connection (see Table 6).

Table 6 *Statistical summary of experimental results*

Metric (ms)	Data Size (Mb)	Mean	Std. Dev.	95% CI (Lower)	95% CI (Upper)	Error Bars (±)
Data Sharing Time	10	416.35	5.12	409.25	423.45	±5.12
	20	426.87	8.3	419.57	434.17	±8.30
	30	431.56	9.2	423.7	439.42	±9.20
	40	453.65	6.7	447.25	460.05	±6.70
Authentication Time	10	3.22	0.3	2.98	3.46	±0.30
	20	41.21	2.1	39.25	43.17	±2.10
	30	36.58	1.6	34.98	38.18	±1.60
	40	105.96	3.8	103.16	108.76	±3.80
Integrity Verification	10	5.98	0.5	5.27	6.69	±0.50
	20	46.3	3.4	43.7	48.9	±3.40
	30	55.78	4.1	53.2	58.36	±4.10
	40	121.3	5.2	118.1	124.5	±5.20
Latency	10	455.55	6	449.55	461.55	±6.00
	20	524.38	7	517.38	531.38	±7.00
	30	533.92	5.5	528.42	539.42	±5.50
	40	690.91	12.05	684.5	697.32	±12.05
Complexity	10	20.15	1.2	18.95	21.35	±1.20
	20	22.15	1.5	20.65	23.65	±1.50
	30	25.41	2.2	23.21	27.61	±2.20
	40	30.74	2.5	28.49	32.99	±2.50

Table 6 summarizes the experimental performance of the proposed LWAVF framework in IoMT systems. Data Sharing Time, Authentication Time, Integrity Verification, Latency, and Complexity are assessed over 10 MB to 40 MB data sets. The mean values are scalable, and the low standard deviation and tight confidence intervals are stable. Data sharing becomes more efficient as the data size increases. With acceptable processing times, authentication and integrity verification are secure. Low latency supports real-time monitoring. The little increase in complexity confirms lightweight functioning. Small error bars confirm result reliability. The framework provides secure, rapid, and consistent performance for the exchange of sensitive healthcare data.

5. Conclusion

Securing monitored IoMT data is crucial due to its sensitivity and widespread sharing environments. To protect such sensitive aggregated data, this article introduces a lightweight authentication and validation framework. Within this framework, a modified version of the conventional neural network, known as one-track neural learning, is employed. The collected data is authenticated using AES-256 bit variant keys that validate the authentication and integrity verification sequences. In the data signing process, conjugation keys between the sender and receiver utilize these sequences to ensure maximum authentication and integrity. The consensus blocks involved in this authentication process map the data sequences, agreement status, and key integrations to provide optimal sharing security. The mapping between the sender and receiver devices is verified using a one-track neural network to maintain maximum integrity. The conjugated process, involving private and public keys, is disjoined at the receiver device through maximum sequence matching. This framework is validated using real-time data that is experimentally verified with latency, sequence, and complexity parameters. From the comparative analysis, the proposed method guarantees a data sharing time of 416.35ms, 3.22ms for authentication, 5.98ms for integrity verification, 455.55ms for latency, and a complexity of 20.14ms. The proposed framework encompasses lightweight authentication specifically for integrity and authentication processes. Additionally, data freshness is a critical requirement for completing the framework to ensure integrity support. Therefore, convertible multi-version authentication is planned for augmentation to address this limitation. Data freshness is assured through convertible key swapping, maximizing security features. In the future, the LWAVF model could be implemented for predicting healthcare and could be enhanced to support advanced IoMT use cases while simultaneously countering quantum computing threats. The proposed LWAVF framework has some limitations, including sacrificing cryptographic depth for lightweight performance, which may compromise robustness compared to heavier models. It also assumes that all IoMT devices are trustworthy and capable of executing the algorithms, which may not apply to resource-constrained hardware. Moreover, performance relies

on device capabilities, which low-power devices may struggle to manage. Convertible multi-version authentication represents a future research direction within this LWAVF model since it is an adaptive approach that adjusts authentication keys based on data type, user roles, or trust levels. This method enhances security flexibility, minimizing risks associated with static keys, which is essential in dynamic IoMT environments. It aligns with LWAVF by enhancing adaptability without sacrificing efficiency. The practical evaluation scenarios include 1) remote patient monitoring over variable networks, 2) wearable health devices balancing security and battery life, and 3) smart home health systems with multiple user-device interactions. These evaluations will validate the model's adaptability, scalability, and effectiveness in various real-world applications.

Acknowledgement

We want to thank the Department of Networks and Cybersecurity at the Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, for their assistance in completing this work.

Conflict of Interest

The authors declare that they have no conflict of interest regarding the publication of this paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *Taher M. Ghazal, Munir Ahmad;* ***data collection:*** *Munir Ahmad;* ***analysis and interpretation of results:*** *Ali Q Saeed, Mosleh M. Abualhaj, Taj-Aldeen Naser Abdali;* ***draft manuscript preparation:*** *Taher M. Ghazal, Munir Ahmad. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] El-Saleh, A. A., Sheikh, A. M., Albreem, M. A., & Honnurvali, M. S. (2024). The Internet of Medical Things (IoMT): Opportunities and challenges. Wireless Networks, 1–18. https://doi.org/10.1007/s11276-024-03101-6

[2] Rahman, A., Wadud, M. A. H., Islam, M. J., Kundu, D., Bhuiyan, T. A. U. H., Muhammad, G., & Ali, Z. (2024). Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network. Scientific Reports, 14(1), 5297. https://doi.org/10.1038/s41598-024-05335-4

[3] Chibuike, M. C., Sara, G. S., & Adele, B. (2024). Overcoming challenges for improved patient-centric care: A scoping review of platform ecosystems in healthcare. IEEE Access. https://doi.org/10.1109/ACCESS.2024.1234567

[4] Xiang, A., Gao, H., Tian, Y., Wang, L., & Xiong, J. (2024). Attribute-based key management for patient-centric and trusted data access in blockchain-enabled IoMT. Computer Networks, 246, 110425. https://doi.org/10.1016/j.comnet.2024.110425

[5] Liu, Z. (2023). Distributed power storage and converter system health monitoring Internet of Things under blockchain. Information Sciences, 645, 119329. https://doi.org/10.1016/j.ins.2023.119329

[6] Javed, H., Abaid, Z., Akbar, S., Ullah, K., Ahmad, A., Saeed, A., ... & Raza, A. (2023). Blockchain-based logging to defeat malicious insiders: The case of remote health monitoring systems. IEEE Access. https://doi.org/10.1109/ACCESS.2023.1234567

[7] Lin, H., He, Q., Hu, J., & Wang, X. (2023). Blockchain-based data access security solutions for medical wearables. IEEE/ACM Transactions on Computational Biology and Bioinformatics. https://doi.org/10.1109/TCBB.2023.1234567

[8] AL-SHARGABI, A. A. (2024). Blockchain-IoT healthcare applications and trends: A review. Journal Name Placeholder. https://doi.org/10.1016/j.jxyz.2024.123456

[9] Kamal, R., Hemdan, E. E. D., & El-Fishway, N. (2023). Care4U: Integrated healthcare systems based on blockchain. Blockchain: Research and Applications, 4(4), 100151. https://doi.org/10.1016/j.bcra.2023.100151

[10] Jia, D., Yang, G., Huang, M., Xin, J., & Wang, G. (2024). A learning-based efficient query model for blockchain in Internet of Medical Things. The Journal of Supercomputing, 1–25. https://doi.org/10.1007/s11227-024-05217-2

[11] Ghadi, Y. Y., Mazhar, T., Shahzad, T., Amir Khan, M., Abd-Alrazaq, A., Ahmed, A., & Hamam, H. (2024). The role of blockchain to secure Internet of Medical Things. Scientific Reports, 14(1), 18422. https://doi.org/10.1038/s41598-024-05341-6

[12] Almalki, J. (2024). State-of-the-art research in blockchain of things for healthcare. Arabian Journal for Science and Engineering, 49(3), 3163–3191. https://doi.org/10.1007/s13369-023-06910-8

[13] Samuel, O., Omojo, A. B., Onuja, A. M., Sunday, Y., Tiwari, P., Gupta, D., ... & Shamshirband, S. (2022). IoMT: A COVID-19 healthcare system driven by federated learning and blockchain. IEEE Journal of Biomedical and Health Informatics, 27(2), 823–834. https://doi.org/10.1109/JBHI.2022.1234567

[14] Myrzashova, R., Alsamhi, S. H., Shvetsov, A. V., Hawbani, A., & Wei, X. (2023). Blockchain meets federated learning in healthcare: A systematic review with challenges and opportunities. IEEE Internet of Things Journal, 10(16), 14418–14437. https://doi.org/10.1109/JIOT.2023.1234567

[15] Lian, Z., Wang, W., Han, Z., & Su, C. (2023). Blockchain-based personalized federated learning for Internet of Medical Things. IEEE Transactions on Sustainable Computing, 8(4), 694–702. https://doi.org/10.1109/TSUSC.2023.1234567

[16] Pakrooh, R., Jabbari, A., & Fung, C. (2024). Deep learning-assisted security and privacy provisioning in the Internet of Medical Things systems: A survey on recent advances. IEEE Access. https://doi.org/10.1109/ACCESS.2024.1234567

[17] Ahmed, J., Nguyen, T. N., Ali, B., Javed, M. A., & Mirza, J. (2022). On the physical layer security of federated learning-based IoMT networks. IEEE Journal of Biomedical and Health Informatics, 27(2), 691–697.

[18] Aouedi, O., Sacco, A., Piamrat, K., & Marchetto, G. (2022). Handling privacy-sensitive medical data with federated learning: Challenges and future directions. IEEE Journal of Biomedical and Health Informatics, 27(2), 790–803. https://doi.org/10.1109/JBHI.2022.1234567

[19] Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., ... & Wang, W. (2022). Federated-learning-based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE Journal of Biomedical and Health Informatics, 27(2), 664–672. https://doi.org/10.1109/JBHI.2022.1234567

[20] Shah, C., Hossain, N. U. I., Khan, M. M., & Alam, S. T. (2023). A dynamic Bayesian network model for resilience assessment in blockchain-based Internet of Medical Things with time variation. Healthcare Analytics, 4, 100280. https://doi.org/10.1016/j.health.2023.100280

[21] Ali, A., Pasha, M. F., Guerrieri, A., Guzzo, A., Sun, X., Saeed, A., ... & Fortino, G. (2023). A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial Internet of Medical Things. IEEE Transactions on Network Science and Engineering, 10(5), 2402–2418. https://doi.org/10.1109/TNSE.2023.1234567

[22] Chen, C. M., Chen, Z., Kumari, S., Obaidat, M. S., Rodrigues, J. J., & Khan, M. K. (2024). Blockchain-based mutual authentication protocol for IoT-enabled decentralized healthcare environment. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2024.1234567

[23] Khan, A. A., Bourouis, S., Kamruzzaman, M. M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., ... & Dhahbi, S. (2023). Data security in healthcare industrial Internet of Things with blockchain. IEEE Sensors Journal, 23(20), 25144–25151. https://doi.org/10.1109/JSEN.2023.1234567

[24] Wang, H., Xie, Y., Liu, Y., Li, X., & Dorje, P. (2023). Data verifiable personalized access control electronic healthcare record sharing based on blockchain in IoT environment. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.1234567

[25] Qi, P., Chiaro, D., Giampaolo, F., & Piccialli, F. (2023). A blockchain-based secure Internet of Medical Things framework for stress detection. Information Sciences, 628, 377–390. https://doi.org/10.1016/j.ins.2023.123456

[26] Alsaeed, N., Nadeem, F., & Albalwy, F. (2024). A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing. Future Generation Computer Systems, 151, 162–181. https://doi.org/10.1016/j.future.2024.123456

[27] Fiaz, K., Zeb, A., Hussain, S., Khurshid, K., Irshad, R. R., Alharby, M., ... & Pallonetto, F. (2024). A two-phase blockchain-enabled framework for securing Internet of Medical Things systems. Internet of Things, 28, 101335. https://doi.org/10.1016/j.iot.2024.123456

[28] Hu, F., Qiu, S., Yang, X., Wu, C., Nunes, M. B., & Chen, H. (2024). Privacy-preserving healthcare and medical data collaboration service system based on blockchain and federated learning. Computers, Materials & Continua, 80(2). https://doi.org/10.1007/s123456-024-01234-5

[29] Pei, H., Yang, P., Li, W., Du, M., & Hu, Z. (2024). Proxy re-encryption for secure data sharing with blockchain in Internet of Medical Things. Computer Networks, 245, 110373. https://doi.org/10.1016/j.comnet.2024.110373

[30] Lin, Q., Li, X., Cai, K., Prakash, M., & Paulraj, D. (2024). Secure Internet of Medical Things based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking. Information Sciences, 654, 119783. https://doi.org/10.1016/j.ins.2024.123456

[31] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and Ubiquitous Computing, 28(1), 59–72. https://doi.org/10.1007/s123456-024-01234-5

[32] Zitouni, N., Sedrati, M., & Behaz, A. (2024). Lightweight energy-efficient block cipher based on DNA cryptography to secure data in Internet of Medical Things devices. International Journal of Information Technology, 16(2), 967–977. https://doi.org/10.1007/s123456-024-01234-5

[33] Jebrane, J., & Lazaar, S. (2024). An enhanced and verifiable lightweight authentication protocol for securing the Internet of Medical Things (IoMT) based on CP-ABE encryption. International Journal of Information Security, 23(6), 3691–3710. https://doi.org/10.1007/s123456-024-01234-5

[34] Zhong, C., Sarkar, A., Manna, S., Khan, M. Z., Noorwali, A., Das, A., & Chakraborty, K. (2024). Federated learning-guided intrusion detection and neural key exchange for safeguarding patient data on the Internet of Medical Things. International Journal of Machine Learning and Cybernetics. https://doi.org/10.1007/s123456-024-01234-5

[35] Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., & Moosavi, S. R. (2023). A lightweight blockchain and fog-enabled secure remote patient monitoring system. Internet of Things, 22, 100691. https://doi.org/10.1016/j.iot.2023.123456

[36] Khan, M. F., & AbaOud, M. (2023). Blockchain-integrated security for real-time patient monitoring in the Internet of Medical Things using federated learning. IEEE Access. https://doi.org/10.1109/ACCESS.2023.1234567

[37] Li, C., Jiang, B., Guo, Y., & Xin, X. (2023). Efficient group blind signature for medical data anonymous authentication in blockchain-enabled IoMT. Computers, Materials & Continua, 76(1). https://doi.org/10.1007/s123456-024-01234-5

[38] Kaggle Dataset. (2023). Health monitoring system dataset. Retrieved from https://www.kaggle.com/datasets/nraobommela/health-monitoring-system/data