Towards Secure Internet of Things-Enabled Healthcare: Integrating Elliptic Curve Digital Signatures and Rivest Cipher Encryption

Longyang Du*, Tian Xie
School of Artificial Intelligence, Jiaozuo University, Jiaozuo 454000, Henan, China

***Abstract*—The expansion of Internet of Things (IoT) applications, such as wireless sensor networks, intelligent devices, Internet technologies, and machine-to-machine interaction, has changed current information technology in recent decades. The IoT enables the exchange of information and communication between items via an internal network. Nevertheless, the advancement of technology raises the urgent issue of ensuring data privacy and security, particularly in critical sectors like healthcare. This study aims to address the problem by developing a hybrid security scheme that combines the Secure Hash Algorithm (SHA-256), Rivest Cipher 4 (RC4), and Elliptic Curve Digital Signature Scheme (ECDSS) to ensure the confidentiality and integrity of medical data transmitted by IoT-enabled healthcare systems. This hybrid model employs the Elliptic Curve Digital Signature Scheme (ECDSS) to perform exclusive OR (XOR) operations inside the RC4 encryption algorithm. This enhances the RC4 encryption process by manipulating the encryption key. Moreover, SHA-256 is used to convert incoming data in order to guarantee data security. An empirical investigation validates the superiority of the suggested model. This framework attains a data transfer rate of 11.67 megabytes per millisecond, accompanied by an encryption duration of 846 milliseconds and a decryption duration of 627 milliseconds.**

***Keywords*—IoT-enabled healthcare; data privacy; security; hybrid security framework; SHA-256; RC4; encryption; data integrity**

I. Introduction

A. Background

The conventional healthcare system faces challenges in meeting the demands of an extensive population due to its constraints in terms of cost and accessibility [1, 2]. The emerging concept of smart healthcare empowers individuals regarding their health conditions, enabling them to manage certain medical situations and enhance the quality of care [3]. This technology permits remote patient monitoring, reducing healthcare expenses and allowing medical practitioners to extend their services across geographical boundaries [4]. An operationally intelligent healthcare system corresponds with the development of innovative urban areas, offering inhabitants a better lifestyle [5]. The National Sanitation Foundation (NSF) examined how nanotechnology and Information and Communication Technology (ICT) could enhance human well-being. This convergence enables the interconnection of items via nanotechnology, embedded systems, sensors, and wireless networks, giving each Internet-connected object its own unique identity [6]. The Internet of Things (IoT) covers a broad spectrum of technologies providing connectivity between different objects, and it has been successfully applied in several industries, particularly healthcare facilities [7]. IoT-enabled healthcare is a sophisticated process involving computer science, medical technology, medicine, microelectronics, and other related fields [8].

B. Challenges

According to current projections, the industrial IoT domain is anticipated to have a market worth $110.6 billion by 2025 after a substantial growth trend in recent times [9]. Projections suggest that by 2030, the quantity of IoT objects and devices in operation will exceed 50 billion, forming an extensive interconnected system that encompasses smartphones and household appliances [10]. The widespread adoption of IoT, combined with the declining costs of electronic devices and networking, has significantly facilitated the proliferation of its use in the healthcare industry. The introduction of IoT in the healthcare field holds immense potential. The utilization of IoT for remote health monitoring is expected to have a substantial influence on both healthcare establishments and people's homes [11]. The technology offers considerable potential to augment healthcare quality and save costs by enabling early identification and avoidance of illnesses and other hazardous situations [12]. The potential uses of this technology include managing long-term medical conditions, providing elderly care, facilitating physical fitness endeavors, and several other domains. Using technology to enable remote patient monitoring can significantly decrease hospitalization expenses by communicating up-to-date health information to healthcare professionals and promptly identifying and managing health conditions [13].

The IoT combines health sensors, imaging, and diagnostic devices to provide healthcare services that improve efficiency and prolong patient lives. The IoT allows healthcare professionals to remotely manage equipment, effectively allocate resources, and support cost-efficient interaction through safe, real-time communication among medical facilities and patients [14]. This helps in minimizing equipment downtime and improving overall efficiency in healthcare operations. Moreover, healthcare networks enabled by the IoT are positioned to assist in timely identifying diseases, managing long-term medical conditions, handling medical crises, and providing healthcare services as needed, aided by database systems, entry points, and medical servers [15].

Recent advancements in machine learning, such as the multi-expert large language model architecture for Verilog code

generation, have shown promise in automating complex design tasks, potentially offering new avenues for secure and efficient hardware design in IoT applications [16]. The automatic synthesis of models from communication traces in System-on-Chip (SoC) designs has been shown to streamline the development of secure and efficient systems, which is critical for managing the complex data flows in IoT-enabled healthcare environments [17].

C. Problem Statement

Security is a significant concern in large-scale network configurations, particularly in healthcare IoT deployments that handle sensitive patient information. The wireless nature of most devices and their communications in IoT-enabled healthcare systems raises considerable privacy and security concerns [18, 19]. For example, under a Medical Sensor Network (MSN), an IP-enabled sensor might send health information to distant healthcare services. Nevertheless, patient privacy becomes a significant concern when medical data is transmitted through potentially untrustworthy network infrastructures, such as the Internet [20]. Therefore, it is imperative to guarantee the confidentiality and security of health information in healthcare IoT applications. Ensuring the identity verification and permission granting of distant healthcare facilities or caregivers and safeguarding data during its transmission are crucial requirements in healthcare IoT to avoid unauthorized access to confidential medical information or intentional disruption of particular operations. Given individuals' ongoing engagement with these applications, ensuring secure and reliable data communication across healthcare sensors, patients, caregivers, and actuators is vital. Concerns about misuse or privacy issues might deter people from embracing IoT-based healthcare applications.

D. Contribution

This paper introduces a hybrid model that combines the Secure Hash Algorithm (SHA-256), Rivest Cipher 4 (RC4), and Elliptic Curve Digital Signature Scheme (ECDSS) to enhance the security of patient data collected through IoT and various health devices. SHA-256+RC4+ECDSS employs RC4 encryption using ECDSS and introduces shift-right operation to improve the Pseudo-Random Number Generation Mechanism (PRGM) stage. Through the use of shift-right, the key is modified, and subsequently, the plaintext is encrypted. ECDSS encrypts the resulting ciphertext, which is further processed by SHA-256. This combination of algorithms prevents third-party access to data and ensures complete privacy assurance. The following questions guide the study:

- How can a hybrid security framework improve the confidentiality and integrity of data in IoT-enabled healthcare systems?
- What are the computational trade-offs involved in integrating SHA-256, RC4, and ECDSS in a single security framework?
- How does the proposed framework perform in comparison to existing security solutions?

The paper is formatted in the following fashion. Section II comprehensively analyzes previous research on the same topic. Section III outlines the suggested approach. Section IV presents a comprehensive overview of the simulation parameters and presents the findings. Section V discusses the obtained results in detail. Finally, Section VI concludes and discusses potential future enhancements for this research.

II. Related Work

Research efforts in recent years have shown significant progress in securing IoT-enabled healthcare systems. Security, privacy, and efficient data management have been addressed in numerous studies. Table I compares the methodologies, key contributions, and performance metrics of several research studies on data encryption, attack detection, blockchain integration, energy efficiency, anomaly identification, and medical image security.

Al Shahrani, et al. [21] proposed an efficient hashing technique that utilizes digital certificates to boost safety measures. At first, medical data is collected and filtered through normalization before being saved on the IoT device. In this process, digital certificates play a role in authentication. Their approach, known as the Discrete Decision Tree Hashing Algorithm (DDTHA), incorporates the Ant Colony Optimization (ACO) algorithm to hash the unsigned certificates. Encryption is carried out using the Blowfish algorithm, resulting in signed digital certificates for authentication. The proposed method underwent analysis and comparative evaluation against existing approaches, demonstrating superior performance for crucial factors such as energy consumption, avalanche effect, execution time, decryption time, and encryption time compared to other existing methods.

Aruna Santhi and Vijaya Saradhi [22] proposed a method to identify attacks on healthcare IoT devices by using an improved deep learning framework to support the Bring Your Own Device (BYOD) concept. Their approach involves modeling a simulated hospital environment where numerous IoT devices and medical equipment communicate. The datasets on malware assessment in medical IoT devices are collected from every node and treated as features. The processing of these characteristics is carried out using a Deep Belief Network (DBN), which is a constituent of the deep learning algorithm. To optimize the DBN's performance, they fine-tune the number of hidden neurons by leveraging a hybrid meta-heuristic algorithm, a combination of the Spider Monkey Optimization (SMO) and Grasshopper Optimization Algorithm (GOA), called Local Leader Phase-based GOA (LLP-GOA). The DBN trains the nodes by constructing an extensive data store, including attack specifics, allowing precise detection throughout testing. The analysis shows that the suggested LLP-GOA-based DBN model achieved a higher accuracy of 0.25% compared to Particle Swarm Optimization (PSO)-DBN, 0.15% compared to Grey Wolf Algorithm (GWO)-DBN, 0.26% compared to SMO-DBN, and 0.43% compared to GOA-DBN. In addition, the LLP-GOA-DBN model demonstrated a 13% improvement in accuracy compared to the Support Vector Machine (SVM), a 5.4% improvement over the K-Nearest Neighbor (KNN), an 8.7% improvement over the Neural Network (NN), and a 3.5% improvement over a regular DBN.

TABLE I. IOT-ENABLED HEALTHCARE SYSTEMS

Reference	Methodology/Approach	Key contributions	Comparative performance/results
[21]	Optimized hashing algorithm using digital certificates for security. Encryption via the blowfish algorithm.	Using the discrete decision tree hashing algorithm (DDTHA) with ant colony optimization (ACO) for unsigned digital certificates' hashing.	Superior performance compared to existing methods in encryption/decryption time, execution, avalanche effect, and energy consumption.
[22]	Attack detection in medical IoT devices using a deep learning architecture enhanced with a hybrid meta-heuristic algorithm (LLP-GOA).	Utilization of Deep Belief Network (DBN) with LLP-GOA for attack detection.	Improved accuracy (0.25% - 13%) compared to PSO-DBN, GWO-DBN, SMO-DBN, GOA-DBN, SVM, KNN, NN, and standard DBN.
[23]	Addressing security concerns in exchanging patients' records using blockchain and NuCypher threshold re-encryption mechanism.	Introduction of a secure architecture using blockchain for E-healthcare data security, redesigning medical WSN lifecycle, and employing NuCypher for data encryption. Implementation of customized lightweight blockchain PoW/PoS with digital signatures.	Improved security, reduced storage load, and improved transaction processing for E-healthcare compared to centralized systems.
[24]	Utilizing permissioned blockchain, MEC, and DRL-enabled IoT for secure and energy-efficient healthcare services.	Integration of permissioned blockchain and MEC to enhance security and energy efficiency. The application of DRL is to optimize system security and energy consumption.	Balanced security and energy efficiency to combat COVID-19-related challenges.
[25]	Introduction of PRISM, an edge-centric system for intelligent healthcare tools assessment using IoT trials.	A systematic approach for IoT-based trials in domestic healthcare settings. Achieved high precision in anomaly identification.	High precision in models trained on individual patients, decline in accuracy observed on diverse patients.
[26]	Exploration of medical image security within IoT-based healthcare systems using cryptography-based networks.	Use of ResNet-50 architecture for encryption and decryption of medical images. Implementing reconstructive network for decryption and Return on Investment (ROI) framework.	Strong security outcomes in medical image encryption/decryption and potential for precise therapy assessments.

Khan, et al. [23] have proposed a comprehensive strategy to address security concerns in exchanging patients' records across centralized server-based systems. Their solutions address node connectivity rates, parallel data-sharing failures, and delivery complications. The strategy comprises three main components. Initially, it presents a new and reliable framework for ensuring the security of electronic healthcare data by utilizing blockchain-distributed ledger architecture. Furthermore, it improves how medical Wireless Sensor Networks (WSNs) operate by implementing a distributed tiered structure, improving network capacity, and promoting confidence in the blockchain-enabled Peer-to-Peer (P2P) environment. Also, it utilizes the NuCypher threshold re-encryption process to encrypt data, guaranteeing the security of shared resources stored in blocks inside an immutable blockchain. The system utilizes chain codes to automate the processes of verification, logging, distribution of index information, and transaction traceability to prevent illegal actions in the e-healthcare distributed application. In addition, it implements tailored, efficient blockchain systems that utilize both multi-proof-of-work (PoW) and multi-proof-of-stake (PoS) mechanisms, together with digital signatures. These enhancements optimize resource usage, minimize storage requirements, and streamline the transaction process specifically for e-healthcare.

Liu and Li [24] proposed a novel system that combines a permissioned blockchain with Deep Reinforcement Learning (DRL)-enabled IoT to address privacy and power constraints. The proposed mechanism aims to provide healthcare services in real time, ensuring security and energy efficiency. Its primary focus is on assisting in the management of the COVID-19 pandemic. To deal with issues regarding security, a technique based on permissioned blockchain has been developed to guarantee the system's security. The strategy incorporates mobile edge computing (MEC) to disperse computing tasks to address energy restrictions. This helps decrease the proposed H-IoT system's computational load and energy consumption. Additionally, the system employs energy harvesting techniques to enhance performance. Moreover, using a DRL technique simultaneously improves the system's energy efficiency and security aspects. The simulation findings demonstrate that the suggested method successfully achieves a harmonious equilibrium between security and energy efficiency, providing a solid and effective response to the issues brought about by the COVID-19 pandemic.

Hadjixenophontos, et al. [25] introduced PRISM, an edge-centric system designed to assess innovative healthcare tools within domestic settings. They established a systematic approach rooted in automated IoT trials. Leveraging an extensive real-world dataset from in-home patient surveillance across 44 residences of People Living with Dementia (PLWD) spanning a two-year duration. Findings revealed anomaly identification with precision reaching 99%, alongside an average training duration as brief as 0.88 seconds. Despite the high precision observed in models trained on the same individual, a decline in accuracy occurred when assessed on diverse patients.

In healthcare, preserving the confidentiality, integrity, and availability of medical images is critical for precise diagnoses, treatment planning, and patient well-being. Consequently, Nadhan and Jacob [26] explored medical image security within IoT-based healthcare systems. Their study focused on using cryptography-based networks to encrypt and decrypt medical images, especially in secure image transmission through deep learning. The critical network was built upon the ResNet-50 architecture to establish the correlation between various image representations, enabling the incorporation of these intricate elements into the learning model for fine-tuning the encryption technique in specific domains. A reconstructive network was

then used in the decryption process to convert the encrypted image to its original "plaintext" form. Upon revealing the concealed components, an accessible Return on Investment (ROI) framework was established, streamlining data mining by accessing information directly from the user's local environment. The proposed system presented highly reliable imaging tools for assessing therapy outcomes. The utilization of two distinct publicly available datasets facilitated the accomplishment of their research objectives. The robust empirical setup and security analysis outcomes strongly suggest that the proposed approach can offer unparalleled security and yield powerful outcomes in medical image encryption and decryption.

Researchers have focused on efficient hashing techniques and digital certificates but may overlook the importance of integrating multiple cryptographic methods to enhance both security and efficiency. The work of Aruna Santhi and Vijaya Saradhi on attack detection using deep learning frameworks is innovative but does not specifically address encryption and integrity of medical data transmission. In the same way, Khan et al.'s blockchain-based approach enhances security in centralized systems but may introduce complexities in terms of data management and computational overhead. A hybrid security framework combining RC4, ECDSS, and SHA-256 is proposed in our research to address these gaps, providing a balanced solution to the challenges of encryption, authentication, and data transmission in IoT-enabled healthcare systems.

III. Proposed Approach

Securing the privacy and integrity of healthcare data transmission via networks is an ongoing and dynamic problem in IoT technologies. Conventional approaches to network access control are often ineffective and susceptible to unauthorized access or replication. Novel techniques like encryption algorithms have been developed to provide a highly efficient data invisibility framework. However, encryption algorithms encounter difficulties as a result of the strong relationship between the original message and the encrypted message, which facilitates the extraction of encryption keys and the retrieval of the original message by attackers. This study addresses these concerns, proposing a hybrid algorithm called RC4+ECDSS+SHA-256 to enhance the privacy and security of incoming data originating from healthcare and IoT equipment.

The RC4 technique has two primary stages: the Key Scheduling Process (KSP) and PRGM. The KSP populates the S-Box, a 256-byte table, by distributing the elements based on a key. The PRGM then generates a pseudo-random key, which is then used for XOR encryption to form the ciphertext. For more extensive plaintext data, the encryption time may be longer. Moreover, the ECDSS produces a cryptographic key for the RC4 method. ECDSS relies on the Discrete Logarithmic Problem (DLP) and operates within a group of cycles known as EC(Fp), which has a designated generator (G) and a co-factor (h) of 1. ECDSS utilizes key sets comprising a public key (PuK) and a private key (PrK). The SHA-256 is employed to guarantee data integrity. SHA-256 is a cryptographic hash algorithm used to validate data integrity. The suggested hybrid technique enhances privacy and security for medical data exchanged over IoT networks by integrating the RC4, ECDSS, and SHA-256 algorithms.

In the proposed technique, the efficiency and security of the system are improved by leveraging ECDSS for faster key generation during the PRGM process in RC4. KSP in RC4 modifies the key, which can be 40 to 256 bits depending on specific requirements. The suggested approach enhances security resilience versus various threats and improves storage effectiveness by incorporating modifications of ECDSS into RC4. The XOR operation encrypts the plaintext by combining it with the pseudo-random bits generated via the PRGM procedure. This process occurs after the critical encryption is performed by ECDSS and the permutation operation is performed in the KSP section.

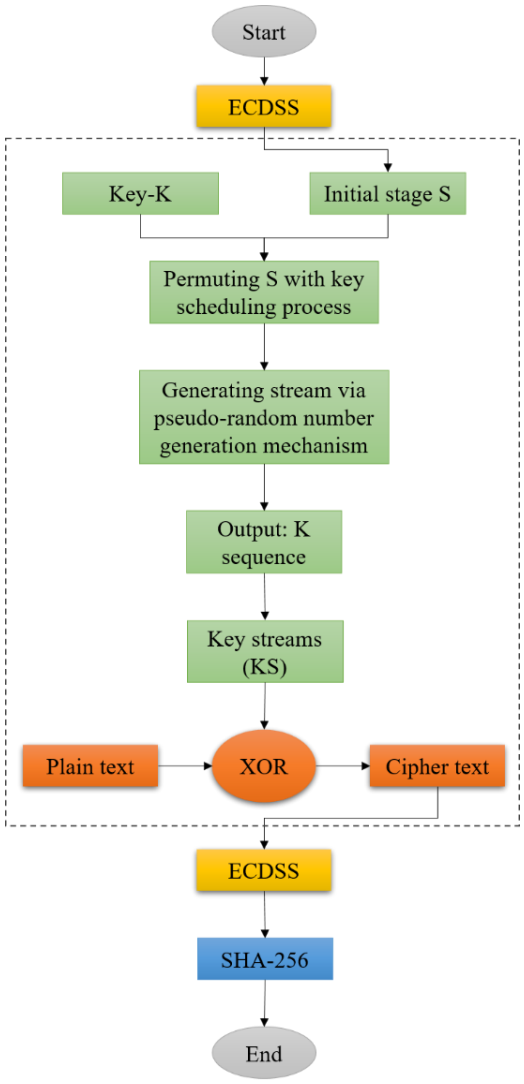

Fig. 1. The workflow of SHA-256+RC4+ECDSS.

To further increase security, a shift-right function is employed to choose a value prior to executing the XOR function. The plaintext is encrypted using the RC4 technique, and the entire process is further encrypted using the ECDSS certification. In addition, to ensure data integrity, the SHA-256 algorithm is used to encrypt the ECDSS signature. This ensures

that only authenticated users with access rights can access the ciphertext. Fig. 1 illustrates the process of the proposed SHA-256+RC4+ECDSS architecture. It provides a comprehensive overview of the various steps of the encryption process, including key generation, encryption with RC4, and data integrity verification with SHA-256. Overall, this hybrid approach combines the strengths of ECDSS, RC4, and SHA-256 to ensure security, efficiency, and data integrity in transmission and improve medical data via IoT networks.

The encryption process involves the following steps. Firstly, an elliptic curve (EC) is selected, and a generator (G) is chosen from its cyclic group. Next, the public-private key pair (*PuK*, *PrK*) is generated using ECDSS. This is achieved by randomly selecting a private key (*PrK*) within a specific range and computing the corresponding public key (*PuK = PrK * G*). The public key is then used as input for the KSP within the RC4 algorithm, modifying the *S* array (the key schedule) and determining its final state. The modified *S* array is employed in the PRGM to generate a pseudo-random key for encryption. Shift-right operations are performed on the *PuK* vector values to create a new key. The plaintext is encrypted using XOR encryption with the generated pseudo-random key. Additionally, a signature is generated for the Encrypted Plaintext (*EP*) using ECDSS with the private key and other parameters. The signature is then hashed using the SHA-256 algorithm. The encrypted message and the signature are the final output of the encryption process.

On the other hand, the decryption process involves the following steps. Given the encrypted message (EM) or ciphertext, the message is decrypted using the SHA-256 decryption process. The signature is verified to determine its acceptance or rejection. Signature verification involves the computation of various values using the ECDSS parameters and the received signature. The *R.y* value is calculated using the square root method. To verify the signature, the computation of *RwPrK + uPuK*EM (FPrK)* is performed. The signature is accepted if *x(R)* is congruent to *k (mod n)*, where *x(R)* represents the x-coordinate of *R*. Finally, the ciphertext is decrypted using the RC4 algorithm, and the resulting plaintext is the output of the decryption process.

Algorithm 1 outlines the pseudocode of the proposed technique, which incorporates the use of ECDSS, RC4, and SHA-256 algorithms in the workflow. In this situation, users transmit medical data from Internet of Things (IoT) devices to cloud storage. At this point, the initial task is to create the procedure for each workflow utilizing the SHA-256, ECDSS, and RC4 algorithms. ECDSS is a public key cryptography algorithm used for generating digital signatures, ensuring the authenticity and integrity of the data. RC4 is a widely used stream cipher algorithm for encryption and decryption, providing confidentiality to the transmitted data. SHA-256 is a cryptographic hash function that generates a unique hash value to ensure data integrity and detect modifications. Subsequently, the S array is altered for the data arriving utilizing the ECDSA public key. This phase guarantees that the received data is thoroughly validated and certified securely. Ultimately, users execute the encryption and decryption processes according to the instructions outlined in Algorithm 1. This allows for the secure transmission and retrieval of medical data, ensuring confidentiality and privacy.

Algorithm 1. Pseudocode of the proposed method

Input: Elliptic Curve Parameters (EC)
Output: Key Pairs (Public Key PuK, Private Key PrK)
Encryption process:
Iterate over each EC(Fp) to choose a point G from order n.
Generate the Elliptic Curve over Fp (GEEC(Fp)).
Select a random integer PrK within the range 2 < PrK < n-2.
Compute PuK = PrK * G.
Apply PuK as input for the KSA function.
Generate the state S = KSA(PuK, S).
Define the key length for S, modify the S array using PuK, and execute the PRGA function for S.
Assign S as PuK, shift-right the PuK vector values, and create a new key based on shift-right operations.
Encrypt the plaintext using the XOR operation, defining the encrypted plaintext as EP, private key PrK, and ECD parameters.
Choose a random integer r within the range 2 < r < n-2.
Calculate R = rG.
Determine k = x(R) (mod n).
Compute $S = r^{-1} * (h(M) + dk) \pmod n$.
Hash(S) using SHA-256.
Generate the Encrypted Message EM.
Decryption Process: Input the Encrypted Message EM or Cipher Text.
Decrypt the message using SHA-256-decryption.
Accept or reject the signature.
Compute $v = S^{-1} \pmod n$ for verification.
Compute w = h(M) * v (mod n).
Calculate u = k * v (mod n).
Calculate R.y value.
Retrieve point R by k value using the square root method.
Calculate $R = wPrK + uPuKeEM(F_{PrK})$.
Accept the signature If x(R) = k (mod n).
Decrypt the cipher text using RC4.
Output: Plaintext

The input submitted for encryption is converted into an array using ECDSS, which is altered using the public key of the ECDSS encryption scheme. To illustrate, the original key “abcd” is converted into array K by the ECDSS process. The strings are then converted into bytes. Encryption and decryption are done using the RC4 algorithm based on the byte arrays. For example, array *A* is obtained as [97, 98, 99, 100] from abcd, and the encrypted RC4 key is generated using ECDSS, resulting in array *K* as [65, 121, 53, 47, 104, 87, 86].

The proposed model aims to improve data security for healthcare infrastructure and applications. In these systems, diverse health information is collected from IoT devices, archived in the cloud, and transmitted to medical facilities, healthcare institutions, and private doctors for assessment. However, the focus is on unauthorized access by third parties, which poses a significant risk to the confidentiality of the data. In the suggested algorithm, the collected IoT data is encoded and decoded by a combined approach of RC4+ECDSS+SHA-256. This ensures that only trusted parties, such as doctors, health centers, and research centers, can access the data, lowering the risk of unauthorized access.

In this proposed hybrid algorithm, RC4, ECDSS, and SHA-256 are individually complex cryptographic components, and their sequential application determines the algorithm's computational complexity. As a stream encryption algorithm, RC4 has a time complexity of *O(n)*, where *n* is the length of the input data. However, KSP and PRGM in RC4 incur some overhead due to their iterative nature. For key generation and signature generation, the ECDSS, which uses elliptic curve cryptography, requires *O(log(n))* and *O(n)*, respectively. SHA-256 is a cryptographic hash function that operates with a fixed complexity of *O(n)*. These algorithms, particularly the repetition of key generation and transformation steps, result in a complexity of *O(n)* for encryption and decryption, but with additional overhead from elliptic curve operations and hash computation, making the hybrid approach computationally intensive but robust against various security threats at the same time.

IV. Simulation Results

We evaluated the presented security framework using various performance metrics, including throughput, decryption time, and encryption time. A summary of the components and parameters considered in the system is outlined in Table II. The CPU is an Intel i5 processor running at 3.2 GHz, while the operating system is Windows 10. The system boasts 4 GB of RAM and operates on a 32-bit architecture. The simulation leverages Python with the Cryptography class for its configuration. Moreover, various cryptographic models and their respective specifications, including key size, block size, and other specific parameters like S-box size for RC4, are outlined in Table II, providing a comprehensive overview of the system used for the study.

A ratio of original data size to encryption time determines encryption throughput. An increase in encryption throughput indicates higher algorithm efficiency. As shown in Table III, we adopted a file size of 10 MB for the test, which resulted in a throughput time of 11.67 ms. Eq. (1) calculates encryption throughput. The analysis of encryption throughput compared to other techniques is shown in Fig. 2.

$$E_t(KB/ms) = \frac{\sum input\ file}{\sum encryption\ time} \quad (1)$$

Likewise, the decryption throughput is calculated by dividing the input file size by the decryption time. For a file size of 10 MB, the analysis resulted in a decryption throughput of 12.79 ms, as shown in Table IV. The calculation of the decryption throughput follows Eq. (2). Fig. 3 illustrates the analysis of the decryption throughput.

$$D_t(KB/ms) = \frac{\sum input\ file}{\sum decryption\ time} \quad (2)$$

TABLE II. Simulation Parameters

Cryptographic model	Block size (bits)	Key size (bits)
RC2	128	128
AES	128	256
RC4	S-box (256 bytes)	256
ECDSS	128	256
3DES	64	256

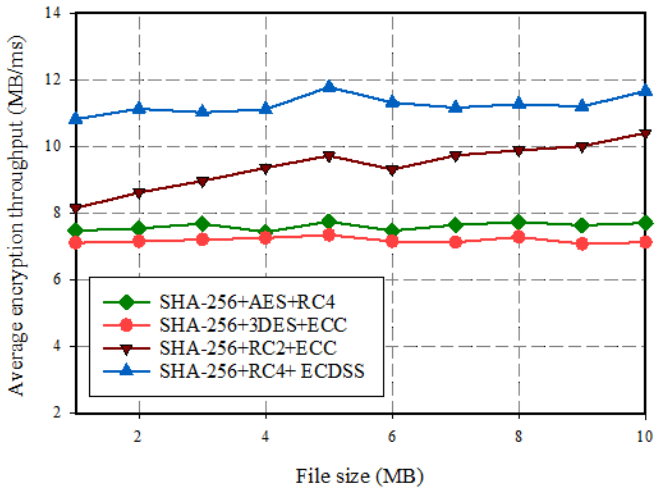

Fig. 2. Encryption throughput comparison.

TABLE III. Encryption Throughput Analysis

Size of the original file (MB)	Average duration taken for encryption throughput			
	SHA-256+AES+RC4	SHA-256+3DES+ECC	SHA-256+RC2+ECC	SHA-256+RC4+ ECDSS
1	7.48	7.11	8.16	10.83
2	7.55	7.16	8.63	11.14
3	7.69	7.21	8.97	11.03
4	7.44	7.26	9.37	11.12
5	7.75	7.35	9.73	11.79
6	7.48	7.16	9.32	11.33
7	7.65	7.13	9.74	11.17
8	7.74	7.29	9.89	11.28
9	7.64	7.08	10.02	11.21
10	7.71	7.13	10.41	11.67
Average time	7.613	7.188	9.424	11.257
Total time	83.743	79.068	103.664	123.827

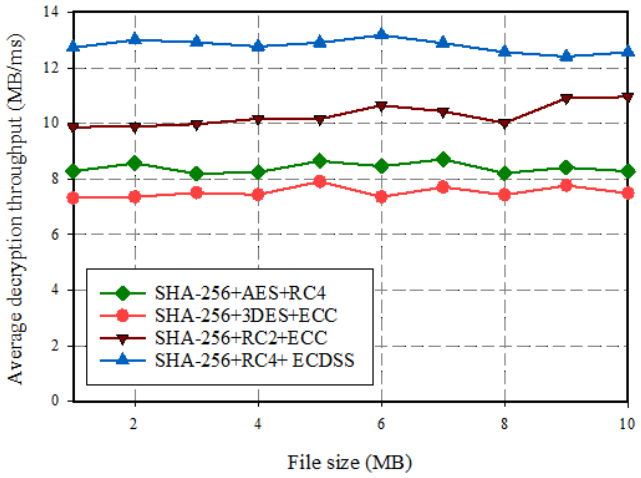

Fig. 3. Decryption throughput comparison.

Table V compares the proposed hybrid algorithm with other algorithms regarding the encryption time. All files with the suggested algorithm were encrypted in 331.5 ms on average, indicating a faster encryption process. Fig. 4 provides a visualization of the encryption time analysis. Furthermore, In Table VI, the developed method and alternatives are compared in terms of decryption times. Our method has a shorter decryption time of 312.1 ms than any other method. Fig. 5 provides a graphical representation of the decryption time analysis and illustrates the performance of the proposed and existing methods.

The results show that the proposed hybrid security framework has superior performance in terms of encryption and decryption efficiency. The observed encryption throughput of 11.67 KB/ms and decryption throughput of 12.79 KB/ms with a file size of 10 MB indicates a highly efficient process that outperforms many existing methods. The average encryption time of 331.5 ms and the decryption time of 312.1 ms further underline the effectiveness of the model, as these times are significantly lower than those of other algorithms. These metrics justify the conclusion that the proposed framework increases both security and efficiency, making it suitable for real-time applications in IoT-enabled healthcare systems. The reduced processing times mean the framework can process large volumes of sensitive data quickly, ensuring robust security without compromising performance, which is critical in healthcare environments where timely data processing is essential.

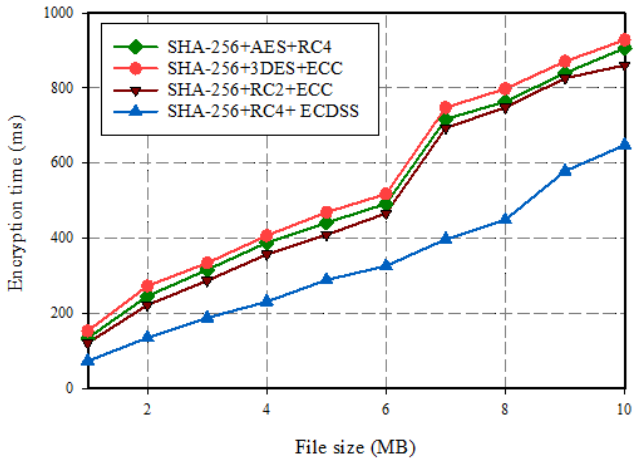

Fig. 4. Encryption time comparison.

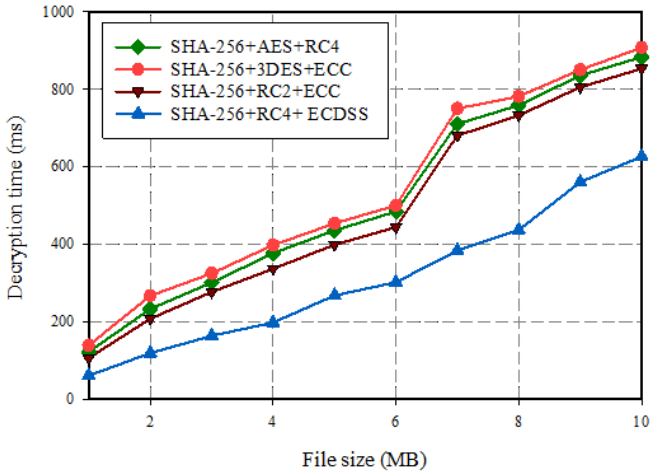

Fig. 5. Decryption time comparison.

TABLE IV. DECRYPTION THROUGHPUT ANALYSIS

Size of the original file (MB)	Average duration taken for decryption throughput			
	SHA-256+AES+RC4	SHA-256+3DES+ECC	SHA-256+RC2+ECC	SHA-256+RC4+ ECDSS
1	8.28	7.32	9.87	12.73
2	8.57	7.36	9.89	13.01
3	8.19	7.51	9.98	12.92
4	8.25	7.44	10.17	12.77
5	8.65	7.91	10.16	12.91
6	8.46	7.36	10.65	13.18
7	8.71	7.71	10.44	12.89
8	8.21	7.43	10.02	12.57
9	8.42	7.77	10.91	12.41
10	8.28	7.49	10.96	12.57
Average time	8.4	7.53	10.3	12.79
Total time	92.42	82.83	113.35	140.75

TABLE V. ENCRYPTION TIME ANALYSIS

Size of the original file (MB)	Required duration for encryption			
	SHA-256+AES+RC4	SHA-256+3DES+ECC	SHA-256+RC2+ECC	SHA-256+RC4+ ECDSS
1	134	153	121	73
2	246	273	222	135
3	316	334	287	188
4	388	407	357	231
5	441	469	409	289
6	492	518	466	326
7	717	748	694	397
8	764	798	748	449
9	840	871	826	579
10	906	928	861	648
Average time	524.4	549.9	499.1	331.5
Total time	5768.4	6048.9	5490.1	3646.5

TABLE VI. DECRYPTION TIME ANALYSIS

Size of the original file (MB)	Required duration for decryption			
	SHA-256+AES+RC4	SHA-256+3DES+ECC	SHA-256+RC2+ECC	SHA-256+RC4+ ECDSS
1	122	139	106	61
2	233	267	208	119
3	301	325	277	164
4	377	398	337	198
5	436	454	399	268
6	485	501	444	302
7	711	751	681	384
8	759	782	733	437
9	836	851	806	561
10	884	908	854	627
Average time	514.4	537.6	484.5	312.1
Total time	5658.4	5913.6	5329.5	3433.1

V. DISCUSSION

The proposed hybrid security framework combining RC4, ECDSS, and SHA-256 has demonstrated significant improvements in healthcare systems' efficiency and security. The encryption and decryption throughput results show that the framework can process large amounts of data quickly, which is critical in real-time healthcare environments where timely access to patient data can be life-saving. Integrating ECDSS with RC4 not only increases key management efficiency but also strengthens encryption against common cryptographic attacks. Using SHA-256 ensures data integrity and provides an additional layer of security that is essential to maintaining patient confidentiality and complying with healthcare regulatory standards.

Furthermore, the empirical analysis confirms that the proposed framework outperforms existing security models in terms of encryption and decryption times, indicating its suitability for resource-constrained IoT devices commonly used in healthcare. This performance improvement is critical for practical use as it minimizes computational overhead while maximizing security. The hybrid approach also addresses the identified gaps in previous research by providing a more comprehensive solution that integrates multiple cryptographic techniques, providing robust protection against unauthorized access and ensuring the integrity and confidentiality of medical data during transmission. This makes the proposed framework a viable option for improving the security of IoT-enabled healthcare systems in an increasingly connected and vulnerable digital landscape.

VI. CONCLUSION

This study addresses the critical challenge of data privacy and security in IoT-based healthcare systems by proposing a hybrid security framework. The framework combined ECDSS, RC4, and SHA-256 to preserve the integrity and confidentiality of data sent. The experimental analysis demonstrated the superiority of the proposed model, particularly when encrypting

data of 10 MB. The framework achieved a high throughput of 11.67 MB per millisecond, with an encryption time of 846 milliseconds and a decryption time of 627 milliseconds. These results highlighted the efficiency and effectiveness of the proposed hybrid security framework. Compared to existing techniques such as SHA-256+3DES+ECC, SHA-256+ AES+RC4, and SHA-256+ RC2+ECC, the proposed model outperformed for encryption time, decryption time, and overall security. It provided a robust solution for protecting sensitive healthcare data transmitted through IoT devices.

Further investigation in healthcare IoT security could concentrate on using advanced cryptographic techniques, such as homomorphic encryption and quantum-resistant algorithms, to enhance data protection. Exploring decentralized identity management and blockchain applications has the potential to improve identity verification in healthcare systems. In addition, creating machine learning models to identify anomalies in healthcare data collected by IoT devices could facilitate proactive security measures. Furthermore, the combination of edge computing with federated learning has the potential to resolve privacy issues by locally processing confidential data. These instructions guarantee the enhancement of the durability of healthcare IoT systems against advancing cyber dangers while promoting innovation in patient data confidentiality and protection.

REFERENCES

[1] S. K. Dezfuli, "Targeted killings and the erosion of international norm against assassination," Defense & Security Analysis, vol. 39, no. 2, pp. 191-206, 2023, doi: https://doi.org/10.1080/14751798.2023.2185947.

[2] S. Abdidizaji, A. K. Yalabadi, M. Yazdani-Jahromi, O. O. Garibay, and I. Garibay, "Agent-Based Modeling of C. Difficile Spread in Hospitals: Assessing Contribution of High-Touch vs. Low-Touch Surfaces and Inoculations' Containment Impact," arXiv preprint arXiv:2401.11656, 2024, doi: https://doi.org/10.48550/arXiv.2401.11656.

[3] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective," Sustainability, vol. 15, no. 4, p. 3317, 2023.

[4] T. Arpitha, D. Chouhan, and J. Shreyas, "Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications," Journal of Engineering and Applied Science, vol. 71, no. 1, pp. 1-23, 2024.

[5] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy - efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, vol. 34, no. 15, p. e6959, 2022.

[6] Z. N. Aghdam, A. M. Rahmani, and M. Hosseinzadeh, "The role of the Internet of Things in healthcare: Future trends and challenges," Computer methods and programs in biomedicine, vol. 199, p. 105903, 2021.

[7] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23-34, 2017.

[8] B. Pourghebleh, V. Hayyolalam, and A. A. Anvigh, "Service discovery in the Internet of Things: review of current trends and research challenges," Wireless Networks, vol. 26, no. 7, pp. 5371-5391, 2020.

[9] D. Hao and C. JianHua, "A Survey of Structural Health Monitoring Advances Based on Internet of Things (IoT) Sensors," International Journal of Advanced Computer Science and Applications, vol. 14, no. 10, 2023.

[10] A. SRHIR, T. MAZRI, and M. BENBRAHIM, "Security in the IoT: State-of-the-art, issues, solutions, and challenges," International Journal of Advanced Computer Science and Applications, vol. 14, no. 5, 2023.

[11] R. Zgheib, S. Kristiansen, E. Conchon, T. Plageman, V. Goebel, and R. Bastide, "A scalable semantic framework for IoT healthcare applications," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 5, pp. 4883-4901, 2023.

[12] S. Vairachilai, A. Bostani, A. Mehbodniya, J. L. Webber, O. Hemakesavulu, and P. Vijayakumar, "Body sensor 5 G networks utilising deep learning architectures for emotion detection based on EEG signal processing," Optik, p. 170469, 2022.

[13] A. Rejeb et al., "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," Internet of Things, p. 100721, 2023.

[14] S. S. Sefati, B. Arasteh, S. Halunga, O. Fratu, and A. Bouyer, "Meet User's Service Requirements in Smart Cities Using Recurrent Neural Networks and Optimization Algorithm," IEEE Internet of Things Journal, 2023.

[15] S. Yazdanpanah, S. S. Chaeikar, and A. Jolfaei, "Monitoring the security of audio biomedical signals communications in wearable IoT healthcare," Digital Communications and Networks, vol. 9, no. 2, pp. 393-399, 2023.

[16] B. Nadimi and H. Zheng, "A Multi-Expert Large Language Model Architecture for Verilog Code Generation," arXiv preprint arXiv:2404.08029, 2024.

[17] M. R. Ahmed, B. Nadimi, and H. Zheng, "AutoModel: Automatic Synthesis of Models from Communication Traces of SoC Designs," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2024.

[18] S. Boopathi, "Securing Healthcare Systems Integrated With IoT: Fundamentals, Applications, and Future Trends," in Dynamics of Swarm Intelligence Health Analysis for the Next Generation: IGI Global, 2023, pp. 186-209.

[19] M. A. Tofighi, B. Ousat, J. Zandi, E. Schafir, and A. Kharraz, "Constructs of Deceit: Exploring Nuances in Modern Social Engineering Attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2024: Springer, pp. 107-127, doi: https://doi.org/10.1007/978-3-031-64171-8_6

[20] H. Verma, N. Chauhan, and L. K. Awasthi, "A Comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns," Computer Science Review, vol. 50, p. 100591, 2023.

[21] 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, 2022.

[22] J. Aruna Santhi and T. Vijaya Saradhi, "Attack detection in medical Internet of things using optimized deep learning: Enhanced security in healthcare sector," Data Technologies and Applications, vol. 55, no. 5, pp. 682-714, 2021.

[23] A. A. Khan et al., "Data Security in Healthcare Industrial Internet of Things with Blockchain," IEEE Sensors Journal, 2023.

[24] L. Liu and Z. Li, "Permissioned blockchain and deep reinforcement learning enabled security and energy efficient Healthcare Internet of Things," Ieee Access, vol. 10, pp. 53640-53651, 2022.

[25] S. Hadjixenophontos, A. M. Mandalari, Y. Zhao, and H. Haddadi, "PRISM: Privacy Preserving Healthcare Internet of Things Security Management," in 2023 IEEE Symposium on Computers and Communications (ISCC), 2023: IEEE, pp. 1-5.

[26] A. S. Nadhan and I. J. Jacob, "Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications," Biomedical Signal Processing and Control, vol. 88, p. 105511, 2024.