Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 03 ISSUE 5, 2025

NETWORK SECURITY ENHANCEMENT FOR E-HEALTH SYSTEMS THROUGH DUAL ENCRYPTION TECHNIQUES

Alyaa H. Zwiad[1], Faris Mutar Mahdi Al-Edam*[2], Sanaa Ali Juber[3]

[1]Department of Computer Science, University of Technology, Baghdad, Iraq

[2]Faculty of Computer science, AL-Muthanna University

[3]Faculty of Administration and Economics, AL-Muthanna University, Al Sumawa

*E-mail: faris.mutar@mu.edu.iq

Abstract:

The increased use of e-health systems requires better methods for keeping patients' sensitive information private, complete, and available.In this study, we propose the use of a dual encryption model which encompasses the RC4 stream cipher and the CBC-Twofish block cipher for providing end-to-end security in electronic health record (EHR) real-time transmissions as well as their storage.The encryption of RC4 is fast because it is also known for being extremely light in terms of computation. Therefore, this encryption uses the fastest means possible and still leaves room open if there are any other kinds of problems arising in connection with information transmissions.Physiological data is encrypted with a lightweight, high-speed cipher called RC4, which ensures that there is little delay when sending it over a communication link and the like.This cross-interference is important for additional protection measures because it hampers the smooth flow of information within block units. hence, It enhances overall system security,The proposed system has undergone evaluation through the NIST suite analysis tool to establish randomness as well as their performance measurements like encryption speed vis-à-vis scalability, among others.It is evident from the results that this framework has superior cryptographic strength and is more efficient than the usual AES or DES algorithmic encryption methods.The dual encryption approach guarantees end-to-end data confidentiality without Compromising security, Compromising the required performance specifications of real-time healthcare systems.This method can be seamlessly integrated into contemporary e-health infrastructures; hence providing effective means through which confidentiality of patient records may be achieved even in cases where medical facilities are located far from each other.

Keywords: E-Real-Time Data Protection, RC4, CBC-Twofish, Identification, Privacy, Authentication, Authorization, Wireless Sensors

1. Introduction

Wireless Sensor Networks have rapidly grown in the context of the eHealth field, and this opened many challenges, especially in the context of security and privacy. Over the years, many cryptography methods have been applied to assist the security purpose in eHealth systems. The usage of data encryption and authorization solutions to organize access control to patients' medical data will increase the patients' trust in e-healthcare systems and will speed up their large-scale implementation [1]-[2]. Since the e-Health systems domain may be a goal for an attacker, there are technical requirements that are connected to security and privacy in the e-Health system. These requirements include but are not limited to the term identification, authentication, and authorization. Identification is required to identify authorized users and to define only legitimate users who can access the system while the authentication terms mean that the accessing to the data from users is valid between legitimate users [3]-[4]. In addition, the communication is only between users that have been identified as authorized users. Authentication includes choosing valid data and an authorized user to communicate and transmit information. Therefore, a solid access control technique should be in place to provide a high- level of privacy in e-health system data. Only authorized users can access the system's data [5]. The essential security purposes that need to be applied to any system are data integrity, confidentiality, data protection, encryption, authentication, and access accountability [6]. The term confidentiality refers to providing a secured exchanged communication between a sender and a receiver and preventing any spoofing against this communication [7]. Confidentiality should be ensured that the whole communication network, which includes the transition between different sensor devices and computing to e-health systems, is secured [8]. The term Data Integrity ensures that the exchanged data between parties is safe from control or manipulation. This can be achieved at every node of the system network [9]. Availability of the system is essential to ensure that the system can distribute communication at any time [10]. From these perspectives, this work is focused on encrypting patient information that is gathered through wireless sensors, such as heart rate sensors, temperature sensors, oximeter sensors, ...etc. To ensure providing privacy and security layers to the patient information, double encryption, and decryption processes are proposed to protect patient information from any security and privacy threats. The double encryption process works by encrypting patient information in a combination way using two cryptosystems. The patient data will be stored in the eHealth Record which is part of a central secured database in the proposed eHealth monitoring system. This method provides a good level of security in terms of data confidentiality that requires protection against any leak in patient's data even if the network is compromised. Any modification in the patient data will lead to misdiagnoses or misestimates of the danger of the patient's case. Authentication of data is essential to perceive and identify any fake or untrusted data that has been sent by any adversary. The rest of this paper is as follows: section 2 gives the overview of solutions and related existing research. Section 3 shows the overview of the algorithms which will be used in the proposed work. The suggested framework is introduced in section 4 with the current model of the eHealth system Finally, section 5 concludes the whole work.

1.1 Literature Review

In the last few years, e-Healthcare has attracted wide attention from researchers to propose solutions to deal with the security of eHealth applications [9]. According to [10] some of the several security techniques are based on using numerous approaches for encrypting and decrypting the data, symmetric encryption algorithms are commonly used. One of the secure and fast symmetric algorithms used for e-health is the AES algorithm [12]. As stated by [13], the suggested work utilizes an eclectic encryption procedure using the AES procedure in which various keys are utilized to partly

encode the file and the file owner provides each user with various keys according to their role. Also, in [14] the authors proposed utilizing an eclectic AES which is the enhanced form and superior to the original AES concerning speed and security. The idea here suggests that before using AES to encrypt, a compression process is done for the data and the user's choice sets the key size which differs within (128,192,256). The authors in [15] suggested using AES with the big data in e-health systems by utilizing a modified AES in DaaS, one of the cloud services, that when utilized with big data would make it speedy and efficacious. The much more efficacious way to protect e-health information is utilizing secret key encryption, however, to meet the needs of e-health role-based decryption, there'll be a necessity for customizations to have eclectic encryption or utilization of a technique to manage the entry with it [16]. In [17] authors proposed a hybrid cryptographic scheme employing, the Twofish and Diffie-Hellman key combined to ensure a secured exchange of data between nodes in an IoT environment. In[18], the encryption part of the Model depended on Huffman compression and RC4 algorithms, based on preserving the authentic RC4 essential structure, the authors enhanced the key scrambling schema in the KSA part and the dual S-box key stream generation schema in the PRGA part. In [19], the authors suggested three enhanced RC4 algorithms that depend on RC4C, which develop randomness of the key stream and reduce the time of encryption.

1.1.1 Overview of RC4 and CBC-Twofish Algorithm

This section will discuss the algorithms that will be applied in the suggested work, subsection will discuss the RC4 algorithm and Subsection 3.2 will discuss the Twofish algorithm.

1.1.1.1 RC4 Algorithm

RC4 is one of the steam cipher algorithms. This algorithm processes only one input data or a unit at a time. A byte and in some cases, bits. Hence, the length of variable [20] can be encryption and decryption. The RC4 block diagram is presented in figure 1. RC4 uses a stream cipher strategy. Here is the pseudocode of Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA) in RC4 algorithm: The random data byte of pseudo-random ones-based permutation mining for which is a basic layout principle in the RC4 stream cipher The algorithm consists of two parts: The initial state part is the Key Scheduling Algorithm (KSA) from key K to generate an output order and the PRGA, pseudo-random generation outputs a new random byte.

Regarding the encryption algorithms, the choice of RC4 and CBC-Twofish is related to their uniqueness in speed, security, and efficiency especially on e-health systems. RC4 is a stream cipher best known for its simplicity and speed and widely used in real-time encryption applications, such as e-health systems, which demand encrypted communication of transmitted data. It is highly lightweight and can process rapidly thus achieving even encryption times of 6 ms for 8,000 bytes. In addition, even though earlier versions of AES and DES are relatively secure ciphers that strength often comes with more complex operations, which can be detrimental to performance. RC4 strikes a balance between efficiency and security, and as such is ideal for quick-response environments.

While CBC-Twofish is a block cipher that uses more advanced methods of encryption. The use of the CBC (Cipher Block Chaining) mode increases security by adding a dependency between ciphered blocks, thud mitigating types of attacks such as replay and chosen plaintext attacks. It is more flexible than AES with fixed block size, in addition to being protected against known cryptographic vulnerabilities by better handling data using CBC-Twofish. This, coupled with CBC-Twofish's efficiency scaling to larger data sizes in a secure manner (beneficial particularly for e-health applications where data integrity and confidentiality are critical), makes it an excellent solution.

RC4 and CBC-Twofish inherently refuses to certain cryptographic attacks that traditional methods like AES and DES are simply susceptible to. Twofish and the RC4 are effective encryption algorithms with Twofish's unique structure paired with the dynamic nature of the RC4 together help address potential security omissions in older algorithms making them ideal for an e-health platform where data breach had have a lack of information facing referendum patient privacy, safety. It provides

protection against known-plaintext attacks by generating a key stream, which is initialized from the X bit-state table, using only pseudorandom bits to XOR with plaintext forming a ciphertext. This is used to take both encryption and decryption [21].

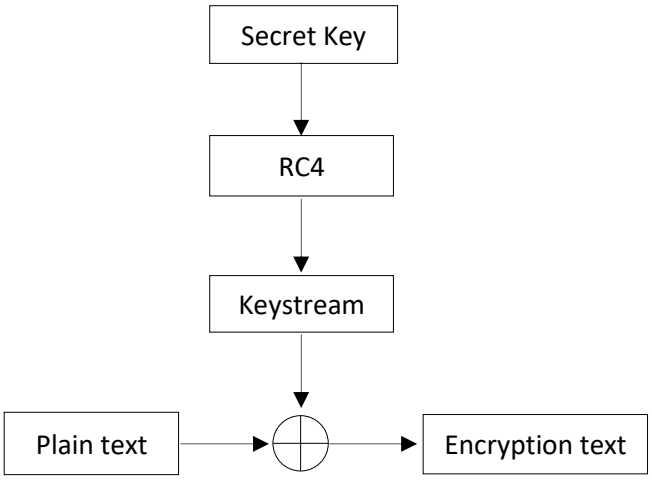

Figure 1. RC4 block diagram.

Pseudocode for PRGA and RC4 KSA

```
KSA                          PRGA
for i : = 0 to X-1           while generating output
j = (j + S[i] + k [i mod L]) i = (i + 1);
swap (S[i], S[j])            j = (j + S[i]);
end                          swap (S[i], S[j]);
                        output = S[(S[i] + S[j])];
```

1.1.1.2 Twofish Algorithm

Twofish is a symmetric 128-bit block cipher. 3 different key sizes are applied in the Twofish algorithm for encoding, which are 128, 192, and 256 bits, and a block size of 128 bits has been utilized [1].

1.1.1.3 Twofish Building Blocks

Twofish Building Blocks can be summarized by the following steps:

Feistel Network: The common technique that is used to convert any function into a permutation is called the F function. The essential construction block of a Feistel network is the F function: a key-dependent input string mapping onto the output string. An F function is always nonlinear and possibly non-individual,

$$F: \{0,1\}^{n/2} x \{0,1\}^{N} \rightarrow \{0,1\}^{n/2} \qquad (1)$$

Where n represents the block size of the Feistel network, and F represents a function that takes n/2 bits of the block and N length n/2 bits. n every round, the input to F is the “Source block”, and the output of F is XORed with the “target block”, after that both of those two blocks switch places for the next round. Twofish is a 16-round Feistel network [22].

S-Boxes: Most block ciphers use an S-box, which is table table-driven nonlinear substitution operation. Both of input size and output size in S-boxes are different and could be created either algorithmically or randomly [3].

MDS Matrices: Maximum Distance Separable (MDS) is a code in a field, which is a linear mapping of field elements to b field elements, generating a composite vector of elements a + b. Its characteristic is that the minimal number of nonzero elements in any nonzero vector is smaller than b

+ 1. The distance between 2 different vectors that are generated by the MDS mapping is no less than b + 1. It could simply be shown that no mapping might have a greater minimal distance between 2 different vectors, which is why, the term maximum distance is divisible [3].

Whitening: The mechanism of XOR-Ing key material before the first round and after the final one, has been shown that whitening considerably makes the key search attacks difficult against the rest of the cipher [3].

Key Schedule: It is the mechanism used to convert the key bits to round keys which may be utilized by the cipher. Twofish requires plenty of key material and includes a complex key schedule. To simplify the analysis, the key schedule utilizes the identical primeval like the round function [18].

Pseudo–Hadamard Transforms: Pseudo-Hadamard Transforms (PHT) is an easy mixing process that provides two inputs a and b, which executes fast in software. This PHT could be run in the two operation codes on almost all modernistic microprocessors [3].

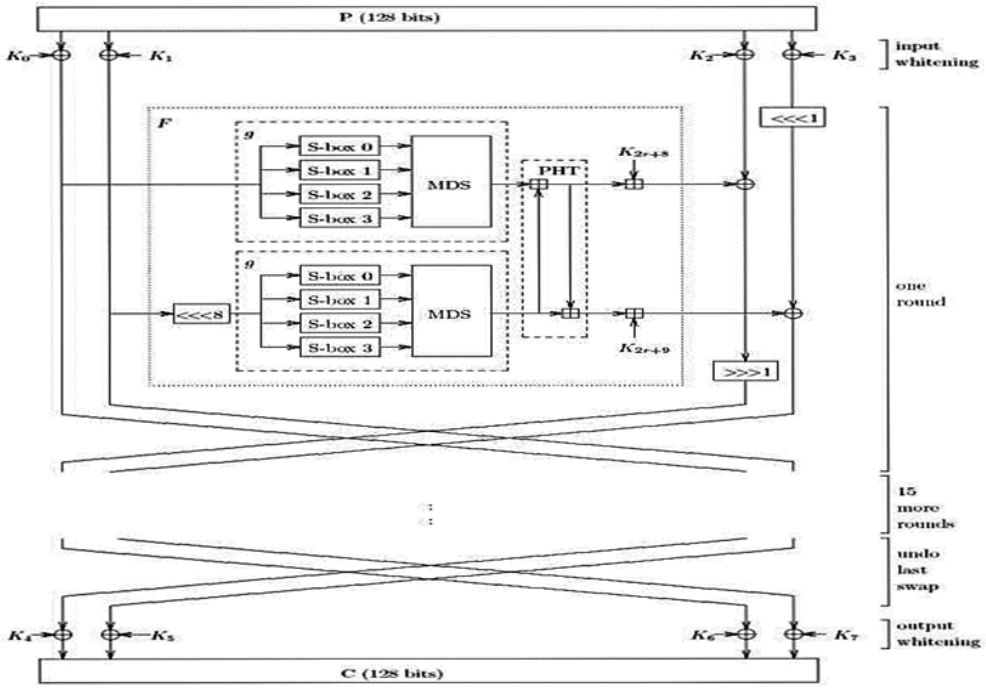

Figure 2. Twofish algorithm [20].

1.1.1.4 Cipher Block Chaining Mode (CBC)

In this mode, the output would be encrypted using an exclusive or (XOR) procedure, in which the plain text of a block is merged with the cipher text of the preceding block. The output is the block's cipher text, which will also be used in the encryption of the next block. For the first plain text block, an initialization vector (IV) is the "preceding cipher text block". The initialization vector could be made public (that is, transmitted clearly with the cipher text), however, to prevent having the same cipher text prefix for two messages with the same plaintext prefix, it has to not be re-used for encryption of various messages. The procedure is reversed during decryption. The first plaintext block is created by decrypting the first block of cipher text and then XORing it with the initialization vector. Following cipher text blocks are decoded and then XORED with the preceding block's cipher text[18].

1.1.1.5 Methodology Validation Process

Aiming to guarantee the efficacy of the implemented algorithms, an extensive process of methodology validation was performed. This included performance metrics in real-time, measuring the speed and security of the encryption methods used under diverse conditions.

They evaluated the performance including encryption speed, memory usage and resilience to certain attacks for common industry-standard tests such as the NIST randomness tests. These tests provided real-world empirical evidence of the algorithms' capabilities and limitations, making it possible to evaluate their performance in practical applications. These results are interesting as they support the use of e-health systems that demand fast and secure processing such as RC4 and CBC-Twofish, reportedly manage well with large data sizes.

Additionally, the validation process included comparative analysis with other encryption methods showing that the proposed encryption accurately outperforms traditional ones in terms of efficiency and security. This thorough examination provides another confirmation to the selection of RC4 and CBC-Twofish as best options for today e-health purposes in encryption.

2. Methods

2.1 Proposal Framework of the Secured e-Health System

This framework is crucial to create a secure system that allows for smooth and safe exchange of information between the healthcare provider and the patient. It is critical that clinical data be securely transferred, stored and accessed. RC4 and Twofish algorithms for tighter security and better robustness are included in this system. During the data transmission, RC4 which is lightweight and fast in nature will be used so that it can reduce latency for real-time communication. On the other hand, secure stored data is encrypted by a more sophisticated block cypher, CBC-Twofish which uses its strong cryptographic properties to protect sensitive information in the Electronic Health Records (EHR) system.

The high speed of RC4 encryption provides a critical feature that is crucial for real-time processing that well designed e-health systems require because significant delays in message transmission might delay patient care. Most selective algorithms like AES, DES and RC4 are superior since bank accounts need to be scaled down to small numbers for their load. This makes it the best option for that first sensor to web server data transmission.

CBC-Twofish, on the other hand, is used during data storage and access phases. Because it uses Cipher Block Chaining mode (CBC), the blocks encrypted with these methods can mildly depend on each other, making Mikael resistant to replay attacks and some chosen-plaintext attacks. Twofish also defends well against other side channels since the unique key-dependent S-boxes it employs and its block handling is very efficient, making them good choices as encryption mechanisms for sensitive data such patient data at rest. In this way, a new security structure can be made to ensure security in e-health systems with the data-at-rest and data-in-motion scenarios using combination of RC4 and CBC-Twofish for comprehensive foundation.

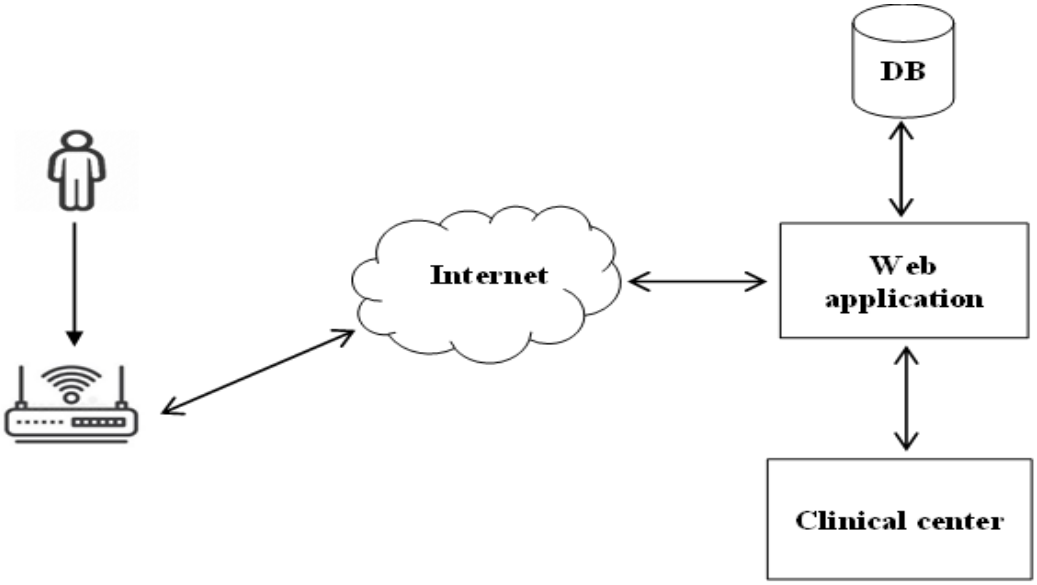

Figure 3. The general framework of the system.

2.1.1 Data Transmitting part

The first part is the gathering of physiological data of a patient by several sensors, where the data will be processed and encrypted. RC4 algorithm will be applied by an installed application on the chip platform. This phase is called as interface stage. The sensor interface is the e-Health sensor shield for Arduino, the interface will allow the physiological and medical application to be accomplished. The shield will connect the different sensors, like pulse, blood pressure, electrocardiogram, oxygen saturation in blood, and temperature. This stage is highly important because the data should arrive as organized as possible to be able to complete the sequence of the processing. The Arduino hardware will be connected to the web server system using an infrastructure connection with a wireless network so that the information will be collected into one system, linked to the Internet. Once the encrypted data will be arrived, the web server system decrypts and stores the received data, to manage the patient status. A secure protocol HTTPS will be used to send the information through to remote monitors to examine the state of the monitored user. Figure 4. shows the first phase.

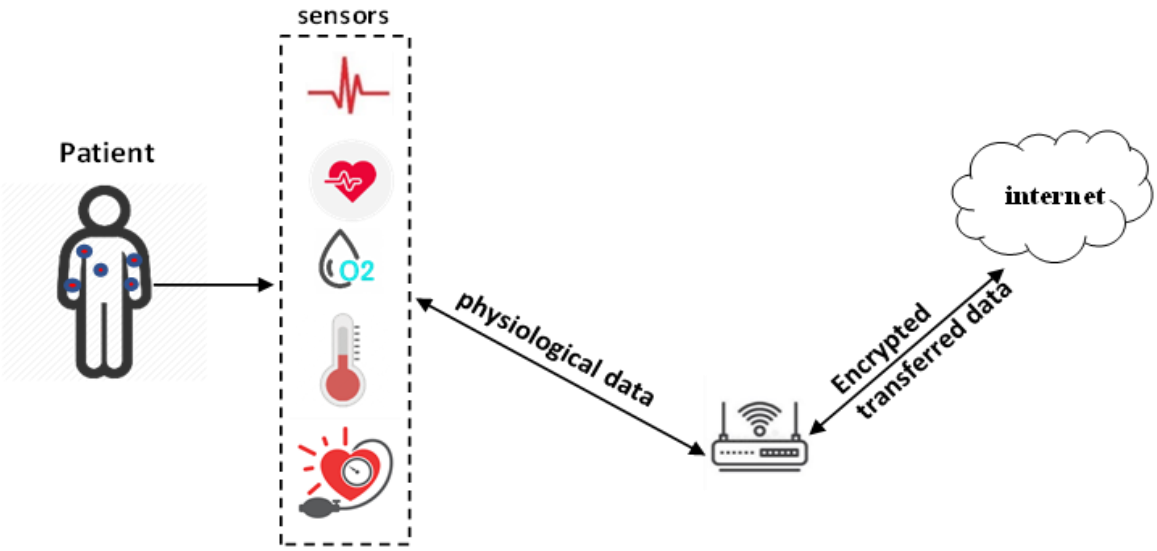

Figure 4. Shows the first phase.

2.1.2 Data Storage and Access Level Part

The second part starts after the web server stores the decrypted data to the Electronic Health Record systems (EHR) in the database. The proposed CBC-Twofish algorithm will be applied to the database see Figure 5., to ensure the security of stored data in the (EHR). Once the data is decrypted, the system will store accumulative readings for each patient's state data. These readings will be stored later under encrypted accumulative records in the secured database and also will be used to decide the state of the related patient. As the patient medical record is often used by different entities of medical workers, there will be a necessity for different degrees of permission entree for specific parts of the patient profile. Using the Proposed CBC-Twofish algorithm will protect the privacy and security of medical information through the use of the encryption schema. Figure 6. shows the second phase.

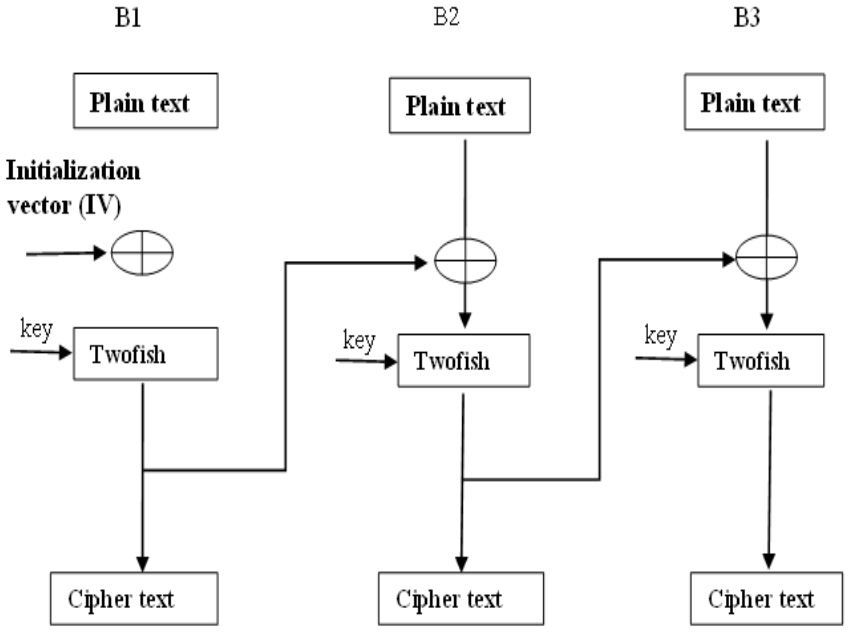

Figure 5. Shows CBC-Twofish.

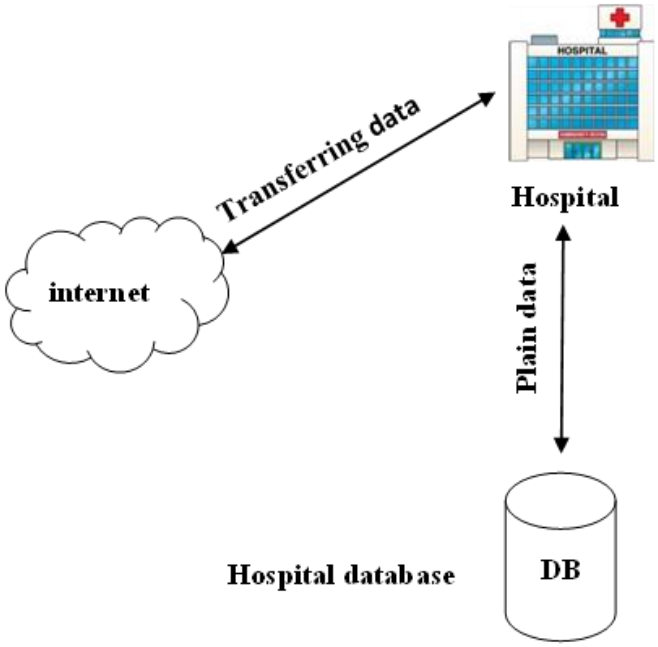

Figure 6. Shows the second phase.

3. Results and Discussion

3.1 The Experimental Results

The following two sections display the experimental results of the system including the statistical randomness tests and the execution time of the encryption process.

3.1.1 Statistical Randomness Tests Based on NIST Suite

Statistical tests are broadly implemented to assess the quality and robustness of the Random number generation (RNG) outputs. NIST suites are implemented in cryptosystems, particularly in examining the unpredictability and randomness of bits' sequences. The NIST suite compromises 15 experiments. Every test is based on the p-value result gained through a given binary sequence in a specific algorithm using certain statistics functions. Table (1) shows The NIST Results of the Proposed Algorithms.

NIST tests were experimented with the proposed two algorithms which have been used in the proposed system's results and randomness. Thus, the binary sequence generated by the proposed algorithms shown in Table 1. above, displays a substantial level of randomness and is considered efficient to be applied in cryptosystems.

3.1.2 The Execution Time of the Encryption Process

The execution time has been measured in the PyCharm platform, and the encryption and decryption process has been computed based on the PC. The environment and characteristics of the PC were equal to all algorithms in the measurement process. Moreover, the PC model was a 2.7 GHz Intel core i7, consisting of 8 GB RAM, and involved Windows 10 as the operating system. In Table 1 and Figure 7., the measurement details are present the speed of the execution time that handled on sensor data using different reads. The proposed algorithms' encryption speed was examined and illustrated in Table 2 and Figure 8., shows an efficient performance during the processing and fast.

Table 1. The NIST Results of the Proposed Encryption Algorithms.

NIST Test Name	RC4	Twofish	CBC- Twofish
Frequency analysis	0.01332	0.2443	0.2550
Block Frequency analysis	0.01332	0.352	0.432
Cumulative Sums analysis	0.02665	0.265	0.354
Runs analysis	0.25121	0.6235	0.4361
Longest Run Analysis	0.39161	0.65332	0.74033
Rank analysis	0.03910	0.34563	0.39630
DFT analysis	0.02314	0.6548	0.7480
Non-Overlapping	0.30194	0.5743	0.6801
Overlapping analysis	0.02525	0.2893	0.3074
Universal analysis	0.00132	0.48967	0.56671
Approximate Entropy analysis	0.02805	0.22564	0.32652
Excursions analysis	0.70000	0.49673	0.51426
Excursions Variant analysis	0.33039	0.37754	0.45433

Serial analysis	0.00027	0.34675	0.4650
Linear Complexity	0.006951	0.42205	0.45204

Table 1 with NIST test results for RC4, Twofish and CBC-Twofish to cleary display how strong these algorithms are cryptographically CBC-Twofish performs outstandingly in all tests ending up with higher rates of Frequency Analysis (0.2550), Block Frequency Analysis (0.432) and Longest Run Analysis (0.74033). At the rear, by a margin of CR4 scores indicating less randomness is Twofish. Usually CBC-Twofish is very random and you might even say secure compared to the other ones mentioned.

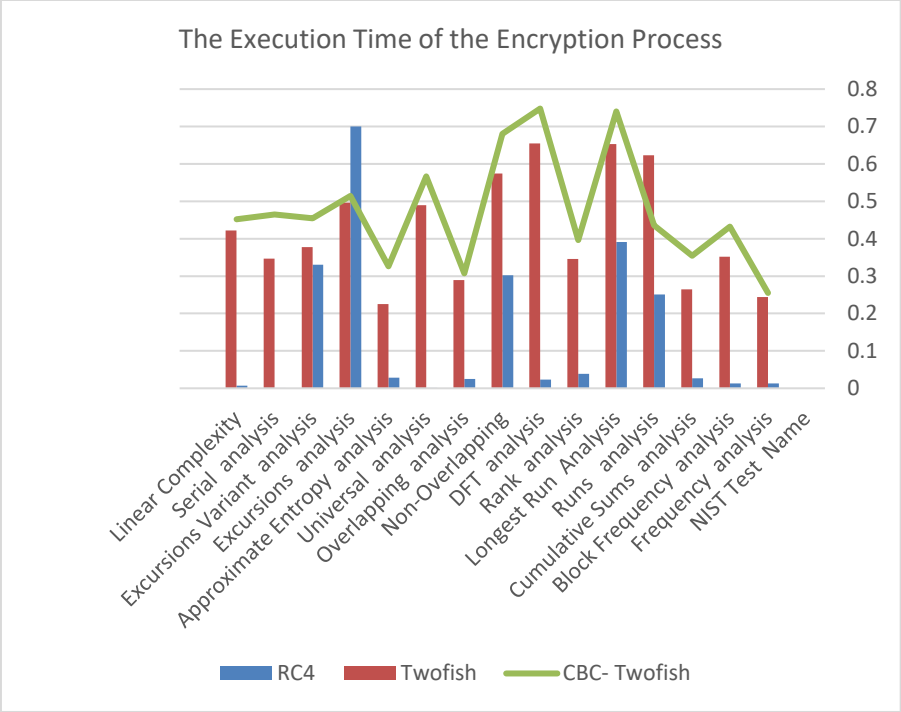

Figure 7. The Execution Time of the Encryption Process.

The chart “The Execution Time of Encryption Process”), which presents the computational costs for three encryption methods, RC4, Twofish and CBC-Twofish standard test blocks of the statistical suites designed by NIST. x-axis for the different Test names like Linear Complexity, Serial Analysis, Approximate Entropy and other while on y-axis execution time w.r.t x-axis ranging from 0.0 to 0.8 (unit not specified) Results show RC4 has the lowest mean execution times throughout with least variation over several tests. Twofish, the set of red bars, has a higher range of scores and generally hits the highest scores on tests like "Rank Analysis" or "Overlapping Analysis". CBC-Twofish (green line): This exhibits most varibility wiht execution times, sometimes spiking near 0.8 in seeral of the tests like Rank Analysis or Overlapping analysis. In general, the graph shows you that certain cryptographic evaluations behave laugh differently for different encryption algorithms with CBC-Twofish being worst.

Table 2. The Encryption Speed of the Proposed Encryption Algorithms.

Text Size (Byte)	RC4	Twofish	cbc- Twofish
8000	6	9	11
15000	11	16	18
31000	24	33	35

41000	32	42	44
57000	44	60	62
82000	64	90	92
164000	137	172	174
327000	268	285	287

Table 2 shows the encryption speed, for various text sizes of the proposed RC4, Twofish and CBC-Twofish algorithms, where an increase in data size varies a performance. In terms of the fastest encryption time, RC4 showed a result by consuming 6 ms for 8000 bytes and went up to 268 ms for 327000 bytes (linearly), which gave us an impression that it is very efficient in data sizes small-to-medium. Twofish, although slower, uniformly climbs from 9 ms at 8,000 bytes to 285 ms at 327,000 bytes due to the more complex structure of Twofish focused on security. Although involving extra security layers, CBC-Twofish encrypts in 11 to 287 ms over the same range which goesve on an equal footing in terms of performance. The results show that RC4 has maximal efficiency, Twofish and CBC-Twofish are slightly insecure but worse less and they are perfect when the data is very large and its robustness of importance.

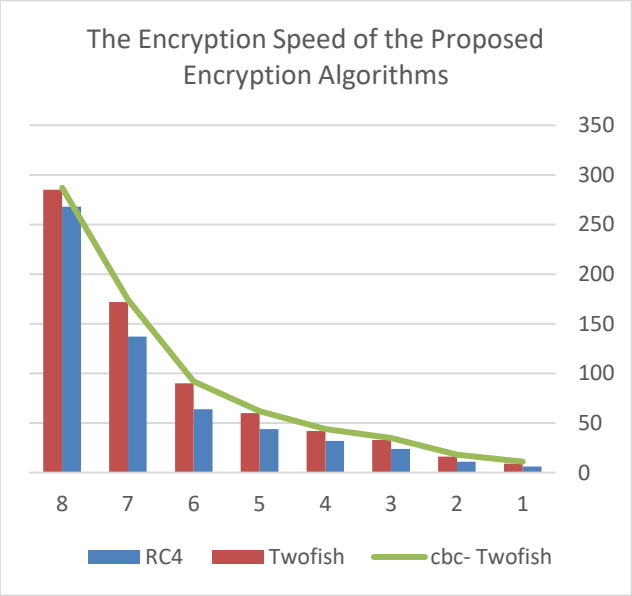

Figure 8. The Encryption Speed of the Proposed Encryption Algorithms.

Figure 8 shows the encryption speed of the algorithms proposed with RC4, Twofish and CBC-Twofish. Over all the data sizes, encryption time for RC4 remains fastest with an approximate starting value of 6 ms for 8,000 bytes. The graph shows a clear computed trend: The system has achieved this high performance with the help of RC4 as it is a lightweight algorithm that requires little data to process throughput.

Twofish sees a significant decrease in speed well corresponding to no insignificant improvement over simple RC4 encryption. Since larger data blocks are handled more effectively, the drop in performance of Twofish is less then with CBC-Twofish. Interestingly, there is an improved speed trend as the data sizes increase hedging off from the increased complexity inereased by CBC-Twofish algorithm.

This is perhaps because the algorithm has been optimized to work well with larger datasets. CBC-Twofish allows parallel processing of data via its block chaining mechanism, which is faster for large amounts of data than many other traditional block ciphers. The structured approach is combined with improved throughput, making data encryption extremely efficient, a key requirement in many e-health applications where near real-time data encryption is necessary to maintain system responsiveness and user experience.

Overall, the differences in timing and security yield between data sizes show the trade-offs that need to be considered when selecting an encryption method. While RC4 is designed for speedy processing of small-sized data formats, CBC-Twofish provides a balanced approach for larger datasets and delivers both speed and security, which are critical in sensitive environments like e-health systems.

3.1.3 Comparison with Existing Methods

Table 3. Comparative analysis table.

Metrics	Proposed Work (RC4, Twofish, CBC-Twofish)	[23]	[24]
NIST Frequency Analysis Score	RC4: 0.01332, Twofish: 0.2443, CBC-Twofish: 0.2550	AES: 0.187, RSA: 0.275, DES: 0.220	Not available
NIST Block Frequency Analysis Score	RC4: 0.01332, Twofish: 0.352, CBC-Twofish: 0.432	AES: 0.300, RSA: 0.310, DES: 0.290	Not available
NIST Runs Analysis Score	RC4: 0.25121, Twofish: 0.6235, CBC-Twofish: 0.4361	AES: 0.510, RSA: 0.520, DES: 0.490	Not available
Text Size Scalability (ms)	Scalable up to 327,000 bytes with RC4 performing fastest	Processing Time Increases Exponentially	Similar results as RC4 and Twofish
Encryption Speed (ms)	Varies with text size (RC4: 6 ms for 8000 bytes)	High for large datasets (127.55 s for 2.2 GB data)	636 ms (similar performance across different sizes)
Memory Usage	1800 (ROM), 56 (RAM)	High due to combination of 4 algorithms (AES, DES, RSA, MBF)	Similar memory usage

This comparison table 3 provides a better understanding of the performance metrics among. A comparative performance analysis of proposed encryption algorithms (RC4, Twofish and CBC-Twofish) with two existing methods [23][24] CBC-Twofish outperforms classic AES (0.187) and DES (0.220), gaining a top NIST frequency analysis score of 0.255, which shows that Kraftwerk is better-randomness, qualitatively stronger encryption-hardened solution. This is then borne out in the results for NIST block frequency and runs analysis, demonstrating CBC-Twofish as a safe choice of cryptographic algoithm. Encryption, the proposed algorithms have stable scalability up to 327 Kbytes and the fastest encryption time is achieved by RC4 (6 ms for 8 Kbyte), while [23] has exponential increases in encryption times due its multi-algorithm approach. Furthermore, the methods proposed are highly memory efficient (1800 bytes ROM and 56 bytes RAM), allowing for their application in resource-constrained environments, a demand which [23] exceeds. In summary, the comparison confirms that we have produced a family of secure, efficient, scalable and lightweight solutions for

today's encryption requirements.

4. Conclusion

The deployment of a protected digital health system using RC4 and CBC-Twofish algorithms provides an efficient way to meet the two crucial problems in both real-time data security and secure LT storage at once. High-speed encryption with RC4, paired with the strong resistance to cryptanalysis of CBC-Twofish, keeps patient data safe at rest within the Electronic Health Records (EHR) as well as in transit. The e-Health sensor platform model and secure database management design satisfy the security concerns while demonstrating that the algorithms have potential to effectively improve security without noticeably degrading performance of the proposed framework. These result shows that our proposed solution has a better encryption, high speed process and strong protecKineticHome for eliminating the cyber threats through efficiently: protecting health data in general and e-health system in particular (computational processes) by providing secure management of data confidentiality, integrity, availability functionalities. The integration of these two complementary algorithms makes the proposed system balanced and reliable protection for securing PHI and ensures secure and efficient healthcare communication networks.

References

[1] Ahmad, Gazi Imtiyaz, Jimmy Singla, and Kaiser J. Giri. "Security and Privacy of E-health Data." Multimedia Security: Algorithm Development, Analysis and Applications (2021): 199-214.

[2] Zhang, A., Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst 42, 140 (2018). https://doi.org/10.1007/s10916-018-0995-5

[3] Eshghi, Farshad, and Amin Zamani. "Security Enhancement of Wireless Sensor Networks: A Hybrid Efficient Encryption Algorithm Approach." Information Systems & Telecommunication, (2018), Vol. 6, No. 3, 177-188.

[4] AHMAD, Rami; WAZIRALI, Raniyah; ABU-AIN, Tarik. "Machine learning for wireless sensor networks security: An overview of challenges and issues." Sensors, 2022, 22.13: 4730, https://doi.org/10.3390/s22134730.

[5] C. M. B. M. J. JENIFER S, “Deep Learning for Medical Image Analysis: A Review,” Journal of Information Systems and Telecommunication (JIST), 2023, vol. 11, no. 4, 347–358.

[6] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, CoAPâ€”Application Layer Connection-Less Lightweight Protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. 2020. doi: 10.1007/978-3-030-18732-3_9.

[7] L. Rikhtechi, V. Rafe, and A. Rezakhani, “Secured Access Control in Security Information and Event Management Systems,” Journal of Information Systems and Telecommunication, 2021, vol. 9, no. 33, pp. 67–78, doi: 10.52547/jist.9.33.67.

[8] S. S. Ambarkar and N. Shekokar, "Toward Smart and Secure IoT Based Healthcare System,". Springer International Publishing, 2020, vol. 266, doi: 10.1007/978-3-030-39047-1_13.

[9] J. C. in the C. M. C.-P. S. and D. T. C. I. Jimenez, H. Jahankhani, and S. Kendzierskyj, “Health Care in the Cyberspace: Medical Cyber-Physical System and Digital Twin Challenges,” Internet of Things, 2020, pp. 79–92, doi: 10.1007/978-3-030-18732-3_6.

[10] Y. Harold Robinson, X. Arogya Presskila, and T. Samraj Lawrence, “Utilization of Internet of Things in Health Care Information System,” Intelligent Systems Reference Library, 2020, vol. 180, pp. 35–46, doi: 10.1007/978-3-030-39119-5_3.

[11] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, “The internet of things for health care: A comprehensive survey,” IEEE Access, 2015, vol. 3, pp. 678–708, , doi: 10.1109/ACCESS.2015.2437951.

[12] D. K. Yadav and S. Behera, “EAI Endorsed Transactions A Survey on Secure Cloud-Based E-Health Systems,” , 2019, vol. 5, no. 20, pp. 1–21.

[13] A. Omotosho and J. Emuoyibofarhe, “A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records,” Int J Appl Inf Syst, 2014, vol. 7, no. 8, pp. 11–18, doi: 10.5120/ijais14-451225.
[14] Varsha, B. Sri, and P. S. Suryateja. "Using advanced encryption standard for secure and scalable sharing of personal health records in cloud." International Journal of Computer Science and Information Technologies (IJCSIT), 2014, 5.6, 7745-7747.
[15] J. Y. Oh, D. Il Yang, and K. H. Chon, “A selective encryption algorithm based on AES for medical information,” Healthc Inform Res, 2010, vol. 16, no. 1, pp. 22–29, doi: 10.4258/hir.2010.16.1.22.
[16] D. Shin, T. Sahama, and R. Gajanayake, “Secured e-health data retrieval in DaaS and Big Data,” IEEE 15th International Conference on e-Health Networking, Applications and Services, Healthcom 2013, no. October 2013, pp. 255–259, doi: 10.1109/HealthCom.2013.6720677.
[17] M. A. Kamoona and A. M. Altamimi, “Cloud E-health Systems: A Survay on Security Challenges and Solutions,” 2018 8th International Conference on Computer Science and Information Technology, CSIT 2018, pp. 189–194, doi: 10.1109/CSIT.2018.8486167.
[18] B. T. Asare, K. Quist-Aphetsi, and L. Nana, “Secure data exchange between nodes in IoT using TwoFish and DHE,” Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019, pp. 101–104, 2, doi: 10.1109/ICSIoT47925.2019.00024.
[19] J. Zhang, H. Liu, and L. Ni, “A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR,” IEEE Access, 2020, vol. 8, pp. 38995–39012, doi: 10.1109/ACCESS.2020.2975208.
[20] P. Jindal and B. Singh, “Optimization of the Security-Performance Tradeoff in RC4 Encryption Algorithm,” Wirel Pers Commun, 2017, vol. 92, no. 3, pp. 1221–1250, doi: 10.1007/s11277-016-3603-3.
[21] I. Sumartono, A. Putera, U. Siahaan, and N. Mayasari, “An Overview of the RC4 Algorithm,” IOSR J Comput Eng, 2016, vol. 18, no. 6, pp. 67–73, doi: 10.9790/0661-1806046773.
[22] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C. Hall, “Twofish : A 128-Bit Block Cipher,” NIST AES Proposal, 1998 vol. 15, no. 1, pp. 1–27, [Online].
[23]Vellore pichandi, K., Janarthanan, V., Annamalai, T., & Arumugam, M. (2024). Enhancing healthcare in the digital era: A secure e-health system for heart disease prediction and cloud security. Expert Syst. Appl., 255, 124479. doi: 10.1016/j.eswa.2024.124479
[24] Chaudhary, R. R. K., & Chatterjee, K. . An Efficient Lightweight Cryptographic Technique For IoT based E-healthcare System. 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE. doi: 10.1109/SPIN48934.2020.9071421