Journal of Autonomous Intelligence (2024) Volume 7 Issue 2
doi: 10.32629/jai.v7i2.1322

ORIGINAL RESEARCH ARTICLE

Enhancing data security of cardiac patients in IoMT with Twin-Shield Encryption

Smiley Gandhi[1,*], T. Poongodi[2], K. Sampath Kumar[3]

[1] *Department of Computer Science and Engineering, Galgotias University, Greater Noida 203201, UP, India*
[2] *School of Computing Science & Engineering, Galgotias University, Greater Noida 203201, UP, India*
[3] *AMET University, Chennai 603112, Tamil Nadu, India*
*** Corresponding author:** Smiley Gandhi, smilegandhi@gmail.com

ABSTRACT

Cardiac disease kills most people worldwide. Predicting and monitoring cardiac problems early improves disease treatment and patient outcomes. The Internet of Medical Things (IoMT) can monitor and analyze physiological data in real-time, changing healthcare. Many researchers find data generation problematic. Encryption is needed to secure a massive amount of data. This paper presents a Twin-Shield Encryption (TSE) that combines Elliptic Curve Cryptography (HECC) and Rivest-Shamir-Adleman (RSA) IoMT assistance for heart illness patient monitoring. Cleveland cardiac dataset from the University of California Irvine (UCI) research repository is collected. It has 12 qualities and 303 occurrences. The data is pre-processed using normalization; feature extracted using Principal Component Analysis (PCA), and securely transmitted to the cloud infrastructure for further processing and analysis. TSE encrypts patient data to prevent unauthorized access and maintain data integrity during transmission and storage. The framework could enhance cardiac ailment diagnosis, treatment, and management by giving clinicians and patients individualized care based on physiological profiles.

Keywords: cardiac disease prediction; Internet of Medical Things (IoMT); Principal Component Analysis (PCA); Elliptic Curve Cryptography (ECC); Rivest-Shamir-Adleman (RSA); Twin Shield Encryption

ARTICLE INFO

Received: 9 October 2023
Accepted: 8 November 2023
Available online: 13 December 2023

1. Introduction

The healthcare industry is undergoing rapid changes, characterized by the emergence of advanced technologies and novel approaches that are revolutionizing the processes of diagnosis, treatment, and monitoring of diverse medical diseases. One of the notable progressions in the field involves the incorporation of the Internet of Things (IoT) into the domain of healthcare, resulting in the emergence of the Internet of Medical Things (IoMT). The field of IoMT comprises a whole ecosystem consisting of interconnected medical devices and systems that have been specifically developed to enhance the quality of patient care, optimize healthcare procedures, and ultimately improve overall health outcomes. In this particular scenario, the emphasis on individuals with heart conditions and the monitoring of their health status assumes utmost importance. The IoT stands for the Internet of Things. It describes a network of actual tools, automobiles, household appliances, and other items that are fitted with associations, software, and detectors to allow users to connect and exchange digital information[1]. The idea behind the IoT is to seamlessly integrate both the digital and physical worlds so that

objects may interact with one another together without any human involvement[2]. These gadgets can collect and analyze data by being online, offering insightful information and chances for automation. IoT technology is used in many different fields including production, transport, medical care, farming, and automation in homes[3]. IoMT devices, for instance, can control lighting, thermostats, security systems, and appliances in the home automation industry, enabling customers to manage and monitor their homes from a distance. Smart medical gadgets, wearable health monitors, and remote patient monitoring are all possible uses for IoMT in the healthcare industry. Through connected automotive systems, IoT in transportation can enable real-time tracking of vehicles, optimize routes, and improve safety[4]. IoT sensors in agriculture can gather information on soil moisture, temperature, and other factors to improve crop management and irrigation. IoMT poses serious security and privacy issues since connecting gadgets to the internet can result in security flaws. To safeguard IoMT systems from cyber threats, it is essential to ensure effective security measures, including data encryption, authentication, and regular software updates. IoMT can completely change the way we interact with technology and the real world, allowing for more automation, efficiency, and convenience in several facets of our life.

IoMT has several applications in the healthcare field that can boost the effectiveness of the system, promote patient care, and optimize operations[5]. Remote patient monitoring allows medical practitioners to keep an eye on patients' vital signs like heart rate, blood pressure, levels of glucose, and respiration rate. This is made possible via IoT devices. The ability of these gadgets to transmit real-time data to healthcare professionals enables them to quickly identify any irregularities or changes in a patient's condition. Health characteristics including levels of exercise, sleeping habits, heart rate, and consumed calories can all be tracked via wearable health trackers, which include wearable and fitness bands that are IoT-enabled[6]. Users can use this data to track their health, encourage healthy behaviors, and communicate relevant data to healthcare experts for better-individualized care. Smart medical devices: The IoT can enable remote tracking and autonomous data collecting in medical devices including insulin pumps, pacemakers, and continuous glucose monitors. Healthcare professionals can closely monitor patient health according to this connectivity, change therapies from a distance, and get notifications in case of incidents or life-threatening conditions[7]. IoMT can help with better drug management and adherence. Smart pill dispensers can deliver precisely enough medication at the right time and remind patients when it's time for them to consume their pills. If a medication is missed or if there are any problems, these gadgets can also notify carers or medical professionals. IoT can improve the monitoring and control of medical tools, supplies, and drugs in hospitals[8]. Integrated sensors can keep track of equipment locations, expiration dates, and levels of stock to ensure effective use and prevent waste or stockouts. IoT technology makes it possible to provide remote healthcare services including telehealth. Access to care is improved, particularly in rural places, thanks to the availability of telemedicine platforms, video meetings with doctors, and real-time sharing of vital signs or health data. Ambient assisted living: IoT gadgets can help the elderly or people with chronic diseases live independently and safely. Smart home solutions can keep an eye on activities; spot falls, or sends notifications in case of crises, giving patients and carers peace of mind. While IoT in healthcare has many advantages, it is vital to remember that patient data security and privacy remain serious problems. To guarantee the safety and confidentiality of medical data, strict privacy laws must be followed and effective safety precautions must be put in place.

IoMT is an IoT subgroup focusing on applications related to healthcare and devices. Medical gadgets, smart watches, software programs, and systems that gather, exchange, and analyze health data are called IoMT. Devices collect and send patient data using sensors and connections. These systems use artificial intelligence (AI) and machine learning to find abnormalities, trends, and actionable insights for medical professionals. IoMT allows remote assessments and virtual care. Healthcare experts can advise patients, examine them remotely, and deliver telemedicine services using multimedia communication platforms, surveillance of patients, and safe data transmission[9]. IoMT creates massive volumes of data, which analytics tools help

interpret. Electronic Health Records (EHRs) and health networks maintain and organize patient data, providing complete and centralized accessibility to medical information.

Key contribution

- This paper presents the concept of Twin-Shield Encryption (TSE), which integrates the HECC and the RSA encryption algorithms for securing the IoMT in the context of cardiac patient monitoring.
- The Cleveland cardiac dataset is employed for the purpose of analysis, after undergoing pre-processing, and thereafter transmitted to the cloud in a secure way.
- This approach improves the diagnosis, treatment, and management of cardiac diseases by providing personalized care that is tailored to individual physiological characteristics.
- This study focuses on the reduction of data security risks in the IoMT with the aim of enhancing patient outcomes and optimizing healthcare efficiency.

The following sections are broken down into four parts as follows: the literature review is discussed in section 2; section 3 is the methodology used; section 4 is the result and discussion, and section 5 is the research's conclusion.

2. Related works

Preethi and Priyadharsini[10] intended to establish the safe management of information in the healthcare industry utilizing deep learning and blockchain technologies. Rana et al.[11] intended to enhance the confidentiality of patient health data obtained via remote surveillance using the Constrained Application Protocol (CoAP). Verma[12] examined to launch of a revolutionary blockchain solution for encrypted cloud healthcare records, which helps to ensure identification and provides integrity to medical information. Irshad et al.[13] offers a revolutionary healthcare surveillance system that analyses illness activities and predictions diseases using data from individuals living in remote areas. Kumar et al.[14] examined that security be improved on the IoMT using "rooted ECC with Vigenère cipher (RECC-VC)". The study of Sun et al.[15] offered a general introduction to contemporary techniques while examining the requirements for secrecy and safety, difficulties, risks, and potential research objectives in the IoMT sector. Bikku et al.[16] examined the combined concept for a system of healthcare that uses IoT and ML technologies. Some detectors, such as movable, compact sensor nodes, can be used to monitor the health of patients. The investigation done by Hasan et al.[17] who evaluated the development of a secure image encryption method for the healthcare sector along with an effective, compact encryption algorithm. Bahache et al.[18] introduced a brand-new classification of Wireless Multimedia Sensor Network (WMSN) authentication techniques that is based on its architecture. It also offers a thorough analysis of the performance and security of the current authentication methods[19–22]. The work done by Singh et al.[23] introduced three metaheuristic algorithm-based feature selection methods: "Emperor Penguin (EPO), Bacterial Foraging (BFOA), and a hybrid approach called hBFEPO that combines EPO and BFOA." While the baseline methods have not been studied for breast cancer categorization, they had been studied for feature selection in other ML applications. The study done by Singh et al.[24] introduced a new and efficient methodology that utilizes two modern and advanced soft-computing methods, namely the Grey Wolf Optimizer (GWO) and the Whale Optimization Algorithm (WOA). Singh et al.[25] presented three metaheuristic feature selection methods: "the Emperor Penguin Optimization (EPO), the Gravitational Search Optimization approach (GSOA), and an integrated (hGSEPO)" approach that integrates EPO and GSOA. Singh et al.[26] presented their hybrid approach and applied a metaheuristics-based method for feature selection based on bacterial foraging optimization and emperor penguin optimization.

Problem statement

To improve patient outcomes, the study covers the challenges of initial cardiac ailment prognosis and follow-up. It offers a technique for carrying out that task that makes use of the IoMT to monitor and assess

real-time physiological data. Data security, nevertheless, is a concern given how much information is created. By presenting doctors and patients with individualized treatment regimens based on their distinct physiological profiles; the proposed approach has the potential to enhance the area of cardiac care. "Elephant Herding Optimization with Opposition-based Learning's (EHO-OBL)" drawbacks include its restricted applicability to certain problem domains, sensitivity to parameter adjustment, and probable convergence to poor solutions. The CCRBM-WO algorithm's drawbacks include complexity, computational expense, restricted generalization, and probable overfitting, which limit its usefulness for a range of tasks. Limitations of the "Improved Elman Neural Network (IENN)" include susceptibility to hyperparameter tuning, vanishing gradients, and difficulties simulating long-term dependencies.

3. Proposed methodology

Cardiac datasets are collected. It has 14 qualities and 303 occurrences. The data is pre-processed using normalization; feature extracted using Principal Component Analysis (PCA), and securely transmitted to the cloud infrastructure for further processing and analysis. Twin-Shield Encryption IoMT assistance for heart illness patient monitoring. **Figure 1** represents the methodological design.

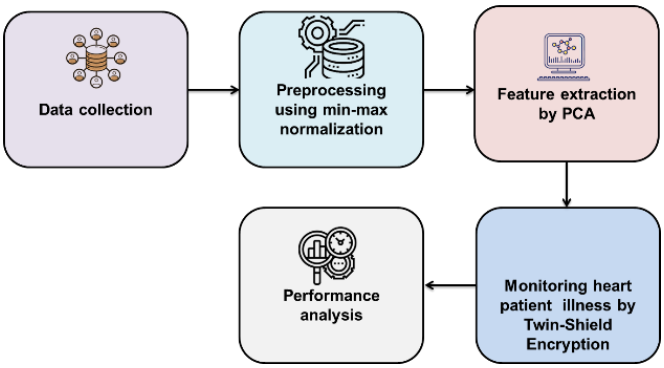

Figure 1. Methodological design.

3.1. Dataset

Cleveland cardiac dataset from the UCI research repository is collected. It has 14 qualities and 303 occurrences.

3.2. Data pre-processing

Min-max normalization can be used to scale the variables within a specific range once the information has been produced. When normalizing each piece of information, choose the lowest and greatest values related to each attribute. This will ensure that all of the features have comparable scales. Scattering normalization, also known as min-max normalization, is a linear alteration of the initial information that produces variables that are mapped between 0 and 1. This transformation is demonstrated in

$$z = \frac{z - \min}{\max - \min} \tag{1}$$

The initial information's average and standard deviation are used to finish the information's standardization. The pre-processed data has a mean of 0 and an average deviation of 1, which is consistent with the traditional typical distribution, as seen in

$$z = \frac{z - s}{r} \tag{2}$$

where, s indicates the sample's overall mean and r denotes its overall standard deviation.

3.3. Feature extraction

Various key factors can be converted into no relevant indexes using PCA to reduce the dimension of the

initial scores in the event of a little amount of information loss, filter redundant information, and gain vast indexes indicating the danger of athletic events.

The following are the PCA steps:

If the research area is, *A* chooses *B* indexes there, and then set the sample matrices of each index to get:

$$C = (C_{sq})A \times B \tag{3}$$

The PCA formulation method is as follows, considering $G_{r\times r}$it represents the index of the correlation coefficient matrix and that its eigenvalue falls within the condition range of $> 1 \geq r \geq 0$:

$$w_r = C_{eq} \tag{4}$$

where, the normalized eigenvector of the correlation coefficient matrix, and eq is the principal component.

Only the initial principal components are chosen if the variation in the contribution rate of the q-th principal component is greater than 86%. At this point, the first indications' data can be reflected, and the percentage of contributions is as follows:

$$m = \sum_{s=1}^{o} mq \tag{5}$$

The following summarises the score I:

$$I = aX_1 + bX_2 + \cdots + xX_X \tag{6}$$

where X represents the normalized information of the starting index, a, b and x is the eigenvector of the eigenvalue. **Table 1** displays the extracted features.

Table 1. Extracted features.

S. No	Feature
1	Age
2	Sex
3	Chest pain type
4	Resting blood pressure
5	Serum cholesterol (mg/dL)
6	Fasting blood sugar > 120 mg/dL
7	Resting electrocardiographic results
8	Maximum heart rate
9	Exercise-induced angina
10	ST depression induced by exercise (relative to rest)
11	Slope of the peak exercise ST segment
12	Number of major vessels

3.4. Twin-Shield Encryption (TSE)

Due to its small key size, high velocity, and low storage utilization, TSE has been picked to develop techniques related to the public key, electronic data encryption, and Bitcoin features, along with other elements. The concurrent problem with the exponential (DLP), a computationally challenging issue, is the foundation for the well-known TSE qualifications. The formula below generates a cloud of points in the FP prime finite field that roughly corresponds to the Elliptic curve.

$$z_2 = w_3 + bw + \text{amodo} \tag{7}$$

When all three of the *w*, *a*, and *b* components of the FP are present. Which points will be on the curve are determined by the *b* and indices. **Algorithm 1** represents the Hybrid Elliptic Curve Cryptography (HECC) algorithm.

Algorithm 1 Hybrid Elliptic Curve Cryptography

Step 1: process 1
Step 2: a, b, c, and m are provided as variables to the HECC.
Step 3: Select plaintext C.
Step 4: C to an integer conversion
Step 5: Using the following formula, find (y, z): $z2 = y3 + axe + c \pmod{p}$
Step 6: Output: C is transformed into the elliptic curve's point (y, z).
Step 7: End process 1
Step 8: Process 2
Step 9: (y, z) as sources
Step 10: Then choose the randomly generated parameter R.
Step 11: The mathematical equation is $(y - 1)/R$.
Step 12: C the initial plaintext result
Step 13: End process 2

TSE can provide a better level of protection based on the measurement of the key used. The TSE encoder transforms the recipient's information up to that stage. Before being converted into the appropriate locations on the elliptic curve, the client data or pure text is first converted into numerals and decimals. This process is handled by the encoder. During the decoding procedure, the TSE decoder is used. The decoder converts the elliptic curve components to integers, which are then converted to simple text.

It is essential to safeguard health data collected by various sensors against unauthorized access. As a result, careful precautions and specialized safety measures should be used while sharing medical data with authorized individuals and organizations. Physical security, achieving transportation, access to data, secure management of IoT data, and other issues with protecting information are difficulties. RSA is one of the most widely used and safe algorithms. **Algorithm 2** represents the RSA algorithm.

Algorithm 2 RSA algorithm

Step 1: Calculate B and C, two prime numbers, where is not equal to c.
Step 2: Calculate mod d i.e., $c = b \times c$.
Step 3: Calculate phi φ where $\varphi = (b - 1) \times (c - 1)$
Step 4: Exponent f should be calculated so that equation $1f\ (d)$ is satisfied.
Step 5: The plaintext message should be represented as a positive integer m using the public key (d, f).
Step 6: Compute the cipher text $p = nf$
(Mod d)
Step 7: Computing $n = pd \times \pmod{d}$ with the use of the private key (e, f).
Step 8: Extract the plaintext from cipher text n.

Due to its lengthy key generation process, TSE is one of the best cryptographic algorithms now in use for ensuring safe communications across networks. Due to the importance of medical information, we benefited from the challenge of factoring in enormous quantities.

4. Result and discussion

The overall performances of the study are analyzed by comparing the actual and predicted values of both encryption and decryption. The existing methods such as Bayesian Belief Network (BBN), Convolutional Neural Network (CNN), and Fuzzy-Based Duo-secure multi-modal framework are compared with the proposed method for assessing the TSE generation execution time, TSE key generation execution time, and PSNR.

While the anticipated encryption time refers to a predicted or planned time for the encryption process determined by certain criteria or computations, the real encryption time is related to the time required to encrypt a piece of information utilizing a certain encryption technique and setup. **Figure 2** represents the actual and predicted encryption time.

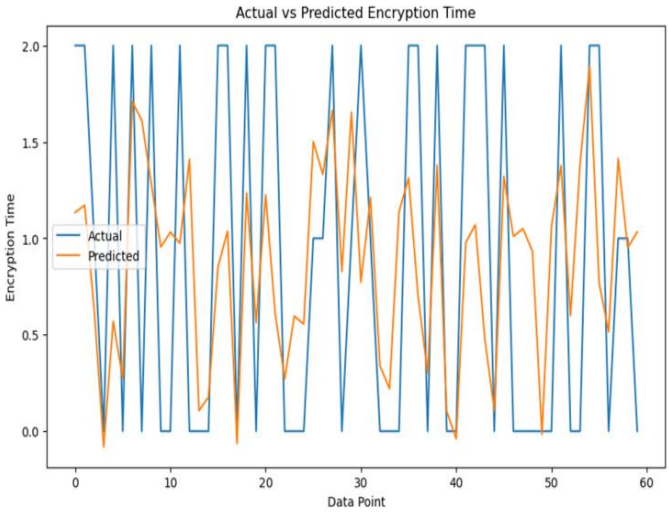

Figure 2. Actual vs. predicted encryption time.

The underlying encryption time may be impacted by the following factors: different encryption techniques may differ in their effectiveness, and they all have different computing requirements. Some algorithms are faster than others. Key length or duration: how quickly data is encrypted may depend on the amount or length of the encryption key used. Longer keys typically lengthen the time needed for encrypting. Technology capacity: the hardware's performance and capabilities can affect how quickly encryption is completed. Technology acceleration, specialized cryptography technology, and a faster processor can all hasten the process. Data size: the amount of data that needs to be encrypted will affect how long it takes to encrypt. Encrypting larger files or larger volumes of data will typically take lengthier. Forecasting the time required for encryption often involves taking into account elements like the hardware requirements, the key size, and the algorithm of encryption in use. One can calculate roughly how long it might take to encrypt data by looking at these characteristics. It's crucial to remember that since projections are based on assumptions and estimates, they are not always accurate. While the anticipated decryption time refers to a projected or planned time for the decryption process according to certain parameters or computations, the actual decryption time relates to how long it takes to decrypt encrypted data using a particular decryption algorithm and setup. **Figure 3** depicts the actual and predicted decryption time.

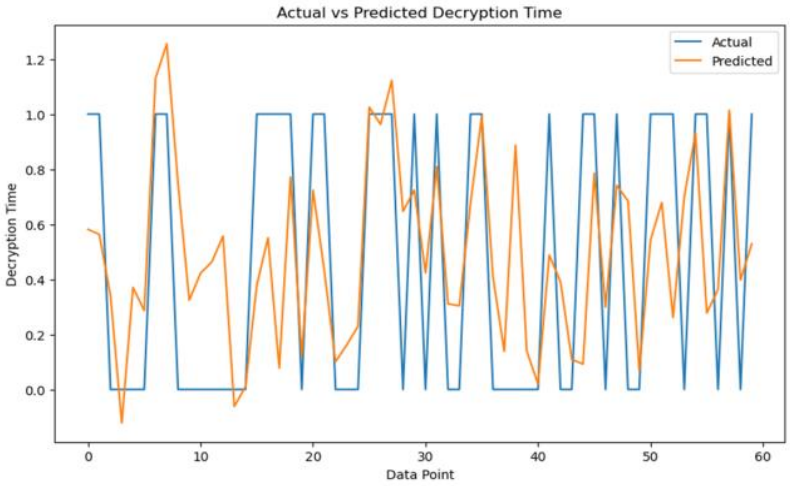

Figure 3. Actual vs. predicted decryption time.

Similar to encryption, various variables can affect how long decryption takes. The decryption algorithm employed can have an impact on how quickly data is decrypted. The processing demands of various algorithms vary, and some might run faster than others. The speed at which data is decrypted may depend on the size of

the decryption key. Since longer keys need more processing power to decrypt, they often take longer. The decryption time may be impacted by the decryption hardware's speed and capacity. The decryption process can be accelerated by using faster CPUs or hardware acceleration. The length of time required to decrypt a given quantity of encrypted data depends on that amount. In overall, decrypting bigger documents or considerable volumes of data will require longer. Considerations for estimating decryption time include the decryption technique, key size, and hardware requirements. One can calculate the approximate time it might take to decrypt the data by looking at these parameters. These forecasts, like encryption, can occasionally not be correct and can change based on the particular situation.

4.1. ECC key generation execution time

The particular elliptic curve utilized, the key size, and the capacity of the processing power can all affect how long it takes to generate a TSE. The amount of elliptic curve scalar additions carried out during key creation is commonly used to gauge the time taken for execution. **Figure 4** and **Table 2** represent the TSE generation execution time of different methods.

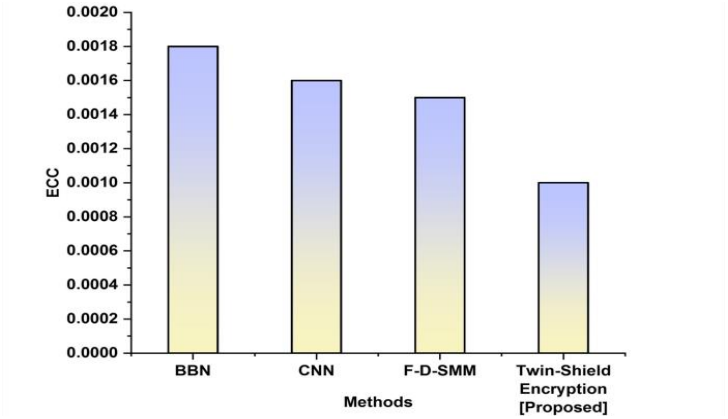

Figure 4. Time required to generate an ECC key.

The time it takes to generate keys depends on the elliptic curve were choose. Various curves have various characteristics and processing needs. An accidental integer is chosen from a range to serve as the password for the private key. The cryptography library or technology being used determines the length of time needed to create an unpredictable number. Elliptic curve scalar division is used to create the public key from the private key.

Table 2. ECC key generation execution time.

Methods	ECC
BBN	0.0018
CNN	0.0016
F-D-SMM	0.0015
TSE	0.001

The dimension of the key and the difficulty of the elliptic curve arithmetic determine how long this phase takes to complete. Based on the aforementioned variables, the completion time for TSE creation can change dramatically. Comparing TSE generation to other uneven cryptographic techniques like TSE, it is generally accepted that TSE generation is more efficient in terms of computation. However, the precise length of execution can change based on the key's size and obtainable computer power. It's important to keep in mind that hardware acceleration, specific cryptography hardware, or specialized elliptic curve installations can all have an impact on how quickly the TSE creation of keys runs.

4.2. RSA key generation execution time

The amount of time required to generate depends on several variables, including the key size, available computing power, and the specific version of hardware or software being used. **Figure 5** and **Table 3** represent the TSE generation execution time of different methods.

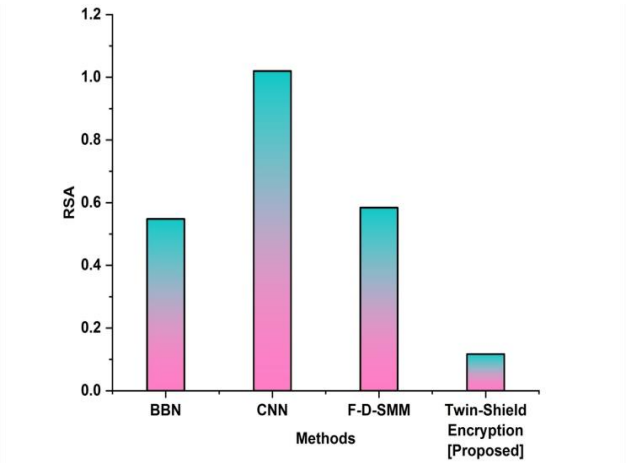

Figure 5. Execution time for generating an RSA key.

To generate aTSE, two large prime numbers, *p*, and *q*, must be chosen. Concerning the procedures and strategies utilized for prime subsequent ones, the amount of time needed to find huge prime numbers can change. *P* and *Q* are multiplied to determine the coefficient of variation (*n*). The quantity of the employed prime numbers will determine how long the procedure takes. The prime values *p* and *q* are used to calculate the toting function, which is represented by the symbol (*n*). Simple computations are used in this stage, which has little effect on the length of execution as a whole.

Table 3. RSA key generation execution time.

Methods	RSA
BBN	0.548
CNN	1.02
F-D-SMM	0.584
TSE	0.1169

The public exponent and the toting function are used to generate the private exponent, which is then determined using the extended Euclidean algorithm or another method. Depending on the algorithm employed, this step's execution duration can change. The size of the key has a major impact on the length of time it takes to generate a TSE. Higher security is provided by larger key sizes, but key generation takes longer and requires more computing power. For instance, it often takes longer to generate a 2048-bit TSE pair than a 1024-bit key pair. It's crucial to remember that hardware acceleration, specialized libraries, or optimized implementations can all affect execution speed. These can considerably quicken the key generation process.

4.3. PSNR

PSNR, or peak signal-to-noise ratio, is the term. It is an essential tool for assessing how well an image or video that has been reduced or rebuilt compares to the distinctive, unprocessed version. The PSNR test compares the strength of the noise to the greatest possible strength of a signal. The PSNR, which is typically reported in decibels (dB), offers a numerical assessment of the integrity or clarity of the compressed/reconstructed image or video. A higher PSNR number suggests less distortion or noise, which means the compacted or rebuilt version, is more faithful to the original. A lower PSNR number, on the other

hand, denotes greater compression or noise and suggests a lesser-quality compressed/reconstructed version. **Table 4** and **Figure 6** show the PSNR for various techniques.

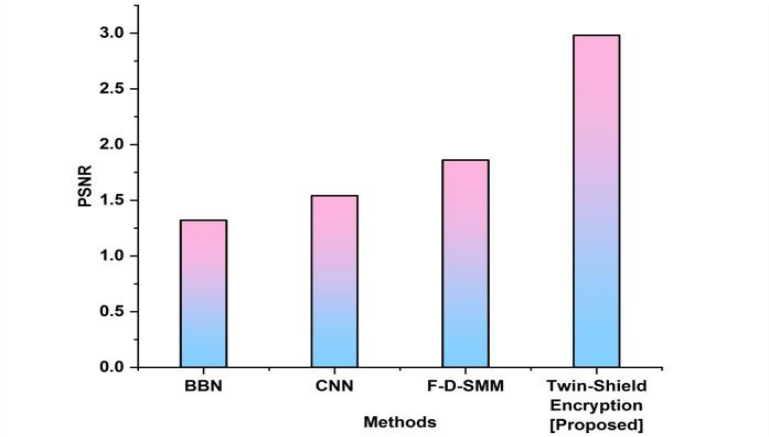

Figure 6. PSNR of different methods.

It's crucial to remember that PSNR has several drawbacks despite being a widely used statistic. It is not always correlated with how well people see or perceive video or image quality.

Table 4. PSNR of different methods.

Methods	**PSNR**
BBN	1.32
CNN	1.54
F-D-SMM	1.86
Twin-Shield Encryption	2.981

For instance, it doesn't take into account perceptual elements like color fidelity or spatial details. Therefore, PSNR should be used in conjunction with other quality indicators and judgments when evaluating the visual appeal of condensed or rebuilt media.

5. Discussion

High-dimensional data processing challenges, the need for expert input for structure, and the possibility of false simplifying independence assumptions are just a few of the drawbacks associated with Bayesian Belief Networks. The applicability of Fuzzy-Based Duo-Secure Multi-Modal systems is limited by their complexity, resource-intensive nature, and susceptibility to external influences, integration issues, and potential for false positives/negatives. Convolutional Neural Networks (CNNs) have several limitations, such as being vulnerable to adversarial attacks, needing huge labeled datasets, having trouble with different dimensions, and having a limited comprehension of the global context in images.

6. Conclusion

IoMT can dramatically improve information safety for heart patients through the adoption of a hybrid cryptographic scheme integrating Twin-Shield Encryption that combines TSE. The IoMT has transformed the field of health care by making it possible to continuously monitor and gather crucial patient data, especially for cardiac patients. There are various advantages to using this hybrid cryptographic system in the IoMT context. It would, most importantly, greatly improve the security of patient data by ensuring that only permitted users and gadgets can view and alter the data. As a result, the confidentiality and security of cardiac patients would be protected from data breaches, theft of identity, and unauthorized manipulation. The IoMT has a very bright future and is predicted to revolutionize medicine in many ways.

Author contributions

Conceptualization, SG and TP; methodology, SG; software, SG; validation, KSK, TP and SG; formal analysis, SG; investigation, SG; resources, TP; data curation, SG; writing—original draft preparation, SG; writing—review and editing, TP; visualization, SG; supervision, TP; project administration, KSK; funding acquisition, SG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Mishra S, Tyagi AK. The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. Artificial Intelligence-based Internet of Things Systems. Published online 2022: 105-135. doi: 10.1007/978-3-030-87059-1_4
2. Guan J, Irizawa J, Morris A. Extended Reality and Internet of Things for Hyper-Connected Metaverse Environments. 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW). Published online March 2022. doi: 10.1109/vrw55335.2022.00043
3. Chanak P, Banerjee I. Internet-of-Things-Enabled SmartVillages: An Overview. IEEE Consumer Electronics Magazine. 2021, 10(3): 12-18. doi: 10.1109/mce.2020.3013244
4. Adhikari M, Hazra A, Menon VG, et al. A Roadmap of Next-Generation Wireless Technology for 6G-Enabled Vehicular Networks. IEEE Internet of Things Magazine. 2021, 4(4): 79-85. doi: 10.1109/iotm.001.2100075
5. Kadhim KT, Alsahlany AM, Wadi SM, et al. An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT). Wireless Personal Communications. 2020, 114(3): 2235-2262. doi: 10.1007/s11277-020-07474-0
6. Karami Z, Hines A, Jahromi HZ. Leveraging IoT Lifelog Data to Analyse Performance of Physical Activities. 2021 32nd Irish Signals and Systems Conference (ISSC). Published online June 10, 2021. doi: 10.1109/issc52156.2021.9467846
7. Mudawi NA. Integration of IoT and Fog Computing in Healthcare Based the Smart Intensive Units. IEEE Access. 2022, 10: 59906-59918. doi: 10.1109/access.2022.3179704
8. Ahmad RW, Salah K, Jayaraman R, et al. Blockchain-Based Forward Supply Chain and Waste Management for COVID-19 Medical Equipment and Supplies. IEEE Access. 2021, 9: 44905-44927. doi: 10.1109/access.2021.3066503
9. Monaghesh E, Hajizadeh A. The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence. BMC Public Health. 2020, 20(1). doi: 10.1186/s12889-020-09301-4
10. Preethi S, Priyadharsini C. Deep Learning with Blockchain Technology for Secure Data Management in Healthcare Sector using Hybrid Elliptic Curve-Rivest–Shamir–Adleman Cryptography. Cybernetics and Systems. Published online December 9, 2022: 1-37. doi: 10.1080/01969722.2022.2151187
11. Rana A, Chakraborty C, Sharma S, et al. Internet of Medical Things-Based Secure and Energy-Efficient Framework for Health Care. Big Data. 2022, 10(1): 18-33. doi: 10.1089/big.2021.0202
12. Verma G. Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence. Published online November 21, 2022: 1-14. doi: 10.1080/0952813x.2022.2135611
13. Irshad RR, Alattab AA, Alsaiari OAS, et al. An Optimization-Linked Intelligent Security Algorithm for Smart Healthcare Organizations. Healthcare. 2023, 11(4): 580. doi: 10.3390/healthcare11040580
14. Kumar M, Kavita, Verma S, et al. ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC. IEEE Transactions on Industrial Informatics. 2022, 18(12): 8936-8943. doi: 10.1109/tii.2022.3181614
15. Sun Y, Lo FPW, Lo B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. IEEE Access. 2019, 7: 183339-183355. doi: 10.1109/access.2019.2960617
16. Bikku T, Sree KPNVS, Jarugula J, et al. A Novel Integrated IoT Framework with Classification Approach for Medical Data Analysis. 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom). Published online March 23, 2022. doi: 10.23919/indiacom54597.2022.9763297
17. Hasan MK, Islam S, Sulaiman R, et al. Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. IEEE Access. 2021, 9: 47731-47742. doi: 10.1109/access.2021.3061710
18. Bahache AN, Chikouche N, Mezrag F. Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. SN Computer Science. 2022, 3(5). doi: 10.1007/s42979-022-01300-z
19. Younas MS. Effective Heart Disease Prediction using Machine Learning and Data Mining Techniques. Int. Res. J. Eng. Technol. 2021, 8: 3539-3546.
20. Verma P, Sood SK. Fog Assisted-IoT Enabled Patient Health Monitoring in Smart Homes. IEEE Internet of

Things Journal. 2018, 5(3): 1789-1796. doi: 10.1109/jiot.2018.2803201
21. Awotunde JB, Folorunso SO, Ajagbe SA, et al. AiIoMT: IoMT-Based System-Enabled Artificial Intelligence for Enhanced Smart Healthcare Systems. Machine Learning for Critical Internet of Medical Things. Published online 2022: 229-254. doi: 10.1007/978-3-030-80928-7_10
22. Wagan SA, Koo J, Siddiqui IF, et al. A Fuzzy-Based Duo-Secure Multi-Modal Framework for IoMT Anomaly Detection. Journal of King Saud University - Computer and Information Sciences. 2023, 35(1): 131-144. doi: 10.1016/j.jksuci.2022.11.007
23. Singh LK, Khanna M, singh R. A novel enhanced hybrid clinical decision support system for accurate breast cancer prediction. Measurement. 2023, 221: 113525. doi: 10.1016/j.measurement.2023.113525
24. Singh LK, Khanna M, Thawkar S, et al. A novel hybridized feature selection strategy for the effective prediction of glaucoma in retinal fundus images. Multimedia Tools and Applications. Published online October 21, 2023. doi: 10.1007/s11042-023-17081-3
25. Singh LK, Khanna M, Singh R. Efficient feature selection for breast cancer classification using soft computing approach: A novel clinical decision support system. Multimedia Tools and Applications. Published online October 16, 2023. doi: 10.1007/s11042-023-17044-8
26. Singh LK, Khanna M, Garg H, et al. Emperor penguin optimization algorithm- and bacterial foraging optimization algorithm-based novel feature selection approach for glaucoma classification from fundus images. Soft Computing. Published online May 27, 2023. doi: 10.1007/s00500-023-08449-6