International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Medical Data Privacy Representation with Improved Encryption Algorithm

Zaheer Sultana [1], Deepak Kumar [2]

Submitted: 02/10/2023 **Revised**: 23/11/2023 **Accepted**: 06/12/2023

Abstract: For research projects involving health care, it might be necessary to collect patient health records from several locations, with various rules governing the release of personal health data. Due to the sensitive nature of health information; privacy is a major concern when patients' health care records are used for dissertation. Data preservation is a technique for defending the integrity and confidentiality of data. Huge databases may contain metadata—uncertain, unstable elements—in their data that may include sensitive information, user profiles, and other information that is subject to intrusion from outside parties like hackers or attackers. They may abuse the information, which would compromise its privacy and confidentiality. The data must be stored safely and made accessible for future use. In order to preserve and safeguard people's data privacy in terms of secrecy and dependability, an effective approach is required. In this paper, for encryption a new Advanced Twofish Encryption standard (ATFES) algorithm is proposed that helps to encrypt the collected raw data. Then, in order to generate the optimal key for encryption and decryption Optimized Radial Basis Function Networks (RBFNs) leveraged with Mayfly-Levy optimization algorithm (MLOA). This encrypted data will be stored in the cloud, and it will be transmitted via the blocks of the blockchain. The same ideal code that was used for encryption will be utilised to recover the encrypted data at the receiving end. The receiver is unable to get the data if the same key is not utilised. The research shows that the suggested techniques are more effective at encrypting and decrypting data over the other state-of-the-art methods. The Matlab platform is used to carry out the implementation.

Keywords: *medical records, privacy, Data preservation, integrity, confidentiality, encryption, decryption, cloud, optimal key*

1. Introduction

In Medical records, saving securely and transmission of health records including preservation of patient confidentiality have all helped to precisely document the ailments of individuals [1]. It is challenging to adapt traditional data access control technology to the dispersed network environment of the present day because it designs and applies a secure access plan with a totally trustworthy server. Data protection becoming more and more important in astute hospitals and patient privacy protection is increasingly a top priority [2]. These hospitals are currently concentrating on how to employ practical online medical services to guard against attacks on the medical information system and data theft [3]. As blockchain and cloud computing have matured, related technologies such as medical informatics, online healthcare, healthcare commercial transactions conducted electronically on the internet, smart technology, and virtual health services have evolved swiftly.

The participants are linked one to another through the blockchain [4]. To create a more dynamic manner of collaboration, the candidates combined manage a structure anddefine the collaboration norms using accord mechanisms including astute contracts. The idea of a smart contract first surfaced in 1994, laying the groundwork for bitcoin [5]. A collection of digitally specified pledges known as a "smart contract" also includes agreements for how parties in the contract can carry out their obligations [6]. A collection of digitally specified pledges known as a "smart contract" also includes agreements for how parties in the contract can carry out their obligations [7]. A point-to-point network must be established, encryption must be used, distributed methods must be used, and data storage technology must be used. These four components make up blockchain technology in its broadest meaning. Others could entail large data, distributed storage, artificial intelligence, virtual reality, the internet of things, etc. In a strict sense, blockchain only has to do with database or file operations, data storage technologies, etc. [8]. Proxy re encryption and attribute-based encryption (ABE), in addition to traditional encryption techniques, can be employed for patient privacy protection and medical data exchange [9].

The user installs and decodes data locally protected material through conventional encryption techniques [10]. Afterwards the user secures the information with the specified user's open code before sending it to that user [11]. This allows the specified user to decode the record, but it incurs significant gateway

[1] *PhD Student, Department of computer science Banasthali Vidyapith University, India. zaheersultana71@yahoo.com Orchid ID: 0009-0008-5513-9006*
[2] *Assistant professor, Department of computer science Banasthali Vidyapith University, India. deepakkumar@banasthali.in Orcid id: 0000-0001-5141-2919*

latency, running expenses, more over uses up the user's limited memory, which increases the expense to the user. Proxy re encryption transforms the ciphertext secured by A's public key into the ciphertext that B's private key will use to decode it in order to facilitate password sharing. Proxy re encryption, which is mostly end-to-end, is the ability of one client to decode the ciphertext of other linked client without disclosing the consumer's individual keys or plaintext [12]. One-to-many data sharing and individual privacy preservation are made possible in ABE by the ability of a data holder to define a usage tactics lead in record encryption [13]. Only consumer who meets this lead may decode the code.

The issue of sharing private data can be resolved with an appropriate configuration and sharing strategy contains attribute-based encryption (ABE). ABE may be classified into KP-ABE (Key-Policy ABE) and CP-ABE, based on the embedded objects (Ciphertext-Policy ABE). As intelligent healthcare gains popularity, medical facilities may hold patient data on the cloud to preserve money on apparatus and other expenses [14]. Some medical facilities must secure the data in advance to create ciphertexts in order to preserve information protection and patient security. Additionally, they require other healthcare organisations to often exchange certain ciphertexts in order to hinder everyone (even cloud service providers) from deciphering these data ciphertexts [15]. The decentralisation and tamper-proofing of blockchain in combination with the distributed cloud computing nodes can help health institutions secure patient data's confidentiality and privacy at a lower cost and facilitate data exchange across medical organisations. The future growth of the healthcare business will be significantly impacted by these.

The main aspect of the research is

- Recent Advanced Twofish Encryption Standard (ATFES) algorithm is proposed for encryption, which aids in the encryption of the collected raw data.
- To generate optimal key for encryption and decryption, Radial Basis Function Networks (RBFNs) that have been optimised using the Mayfly-Levy optimization algorithm (MLOA).
- This encrypted data will be stored in the cloud and transmitted using blockchain blocks.

The remaining part of the research is structured as continues. In section 2, the literature review is carried out. Then, in section 3, proposed methodology is explained. Next, in section 4, The outcomes of the experiments demonstrate the effectiveness and efficiency of the suggested method. At last, in section 5, the research is concluded by the conclusion.

2. Literature Review

In 2020, Li *et al.* [16] have outlined a modern homomorphic encoding scheme for non-abelian rings and defined the homomorphism operations in ciphertexts space. On the basis of the Conjugacy Search Problem, the approach can establish directional security. Following that, homomorphic encryption over a matrix-ring was suggested. It enables quick homomorphic comparison of ciphertexts without requiring the intermediate results of any ciphertext operations to be decrypted and provides Based on the homomorphism of the 2-order displacement matrix coding function, real values are encrypted. Additionally, they employed the method to accomplish privacy protection for data ciphertext-based machine learning training and classification. The investigation demonstrates the effectiveness of the encryption/decryption and homomorphic operations of our suggested systems.

In 2019, Wang *et al.* [17] have suggested a privacy-preserving outsourced computing layout for the medical system, which is a successful scheme that can safeguard patients' sensitive information when the e-health platform wants to perform some analysis on this data. The decryption rights were divided between the two servers, which increased the security of our system. In this study, they have done two basic operations, and their future methods might be designing more advanced calculations with exponential and high-dimensional functions. Their techniques were applied to logistic regression and machine learning models, including Support Vector Machine (SVM).

In 2020, Huang *et al.* [18] have suggested a blockchain-based privacy-preserving strategy that enables safe medical data exchange across a number of parties, including patients, research organisations and semi-trusted cloud services. Additionally, data availability and consistency across patients and research organisations are attained. In order to accomplish this without revealing the patient's name, minimum knowledge proof is employed to ensure that the patient's health records comply with the standards set out by the research organisations. The intermediary ciphertext is then encrypted once again using proxy re-encryption technology, which guarantees that only the research institutes can decode it. This proposal can also carry out disbursed statement consist PBFT algorithm for interactions involving research institutes and patients in accordance with the predetermined terms. A theoretical study suggests that the suggested system may fulfil security and privacy criteria including secrecy, integrity, and availability, and performance assessment shows it is practical and effective in comparison to other usual schemes.

In 2021, Hossein *et al.* [19] have presented an architecture

(named BCHealth) to address the trade-off between openness and access control by letting data owners choose their preferred access restrictions over their healthcare data's highly sensitive personal information. For the purposes of preserving data transfers and access rules, BCHealth is made up of two distinct chains. By using a clustering strategy, they were able to overcome the progress in the actual world difficulties of BC, such as adaptability, latency, and expenditure. Our detailed experimental investigation demonstrates BCHealth's effectiveness (in basis of calculation and required time) and its fortitude in the face of numerous security intrusions.

In 2021, Sathya*et al*. [20] have developed an efficient strategy of measuring secrecy in the healthcare Cloud called the Euclidean L3P-based Multi-Objective Successive Approximation (EMSA) algorithm. The fundamental basis for the preserving of critical information in cloud settings is described in this, and it is role-based encryption keys. The hypothesised EMSA method combines the successful Consecutive Approximation, Iterative Proximate, Multi-objective Optimization, and Euclidean L3P Distance algorithms. A comparison of the proposed EMSA's performance against the Bat, PUBAT, TPNGS, WOA, and CIC-WOA algorithms was also made using performance measures including wellness, secrecy, and convenience. According to the prototype, the suggested EMSA model obtains greater privacy values of 0.34, 0.42, 0.42, 0.35, and 0.30 when compared with the current state-of-the-art techniques.

In 2020, Domadiya*et al*. [21] have suggested a unique method for gathering and analysing health data, and this research uses source anonymity as a method for protecting privacy. Their plan gathers information from every EHR system without any information being lost and keeps it in one centralised information gathering gateway, guaranteeing secrecy is protected. Without utilising EHR systems, a central info gathering gateway facilitates the observation of the gathered infoutilising numerous information collecting methods (Association actextracting, Classification, grouping, etc.). The central info extracting server and EHR systems are not vulnerable to collusion under our method. The effectiveness of their plan in terms of computing and communication costs may be seen through theoretical and experimental study. In terms of illness prediction accuracy, the experimental findings utilising a dataset on heart disease demonstrate the benefit of EHR systems employing the suggested technique.

In 2021, Yue *et al.* [22] have developed a convolutional LSTM network called HE-CLSTM for analysing time-series medical pictures that have been encrypted using a fully homomorphic encryption method. In particular, a number of convolutional blocks are built to extrapolate spatially discriminating features, and LSTM-based sequence analysis layers (HE-LSTM) are used to encrypt temporal information derived from the protected picture sequences. Additionally, to enhance performance and lower the incidence of missed diagnoses, a weighted unit and a sequence voting layer are created to add both spatial and temporal variables with distinct weights. Strong proof which our approach can encrypt virtual models and sequential dynamics from encrypted medical photo sequences, as demonstrated by observational data on two difficult definitions(the Cervigram dataset and the BreaK His public dataset); Their approach outperformed multiple other approaches statistically, with AUCs above 0.94 on both the Cervigram and BreaKHis datasets.

In 2020, Liang *et al.* [23] have suggested a multi-source order-preserving encryption (MSOPE) method for cloud-based eHealth systems to allow range queries across secured EHRs from several patients. Three vulnerabilities, including secrecy divulging, frequency analysis, and same information assumption, were found at actual cloud-based eHealth systems. They developed the safety term of indiscernibility under multi-source ordered selected plaintext assault to encapsulate the security characteristics that fend off these attacks (IND-MSOCPA). According to the security study, the MSOPE scheme is IND-MSOCPA secure. Additionally, they carry out thorough performance reviews that show how effective the MSOPE plan is.

In 2018, Ramya Devi *et al*. [24] have explained ways to secure and protect privacy while using big data in the healthcare sector to combat security risks with current methods. The incorporation focuses mostly on anonymization and Triple DES security mechanisms. Without the requirement, create a brand-new block cypher algorithm, Triple DES provides a very easy procedure of boosting the key size of DES to defend towards these attacks. With goal of protecting data privacy, data anonymization functions as an information sanitizer. For the people the data sets identify to remain anonymous, it encrypts or removes their personally identifiable information from the data sets. This study employs the A3DES method, which stands for anonymization and Triple DES combined. The experimental result shows that the strategy worked effectively when compared to all other relevant techniques.

In 2021, Kanwal*et al*. [25] has examined the demand for a hybrid cloud access control architecture that protects privacy. This article offers a detailed and exploratory investigation of secrecy-storing methods for cloud-based EHRs using taxonomy. They were explicitly acknowledged as existing in the outsourcing system design for hybrid cloud, together with internal access restrictions and privacy disclosures to the public. Then they suggested a secrecy-saving XACML-based access control model

(PPX-AC), which provides fine-grained access control with the multifunctional use of EHRs combined with cutting-edge privacy mechanisms. The security and privacy attacks they have uncovered are invalidated by their suggested strategy. Using High-Level Petri Nets, they have officially validated the suggested XACML-based access control mechanism with privacy protection (PPX-AC) by invalidating known privacy threats (HLPN). Additionally, the model's implementation and property checks in SMT lib and Z3 solver demonstrate its usefulness for several purposes, including privacy-aware EHR access.

2.1. Problem Statements

Researchers have developed a number of privacy-preservation strategies for use in healthcare solutions. The implementation of these methodologies and the properties of the supporting infrastructure, i.e., the advantages and disadvantages of the IoT and cloud computing settings, will ultimately determine their success. IoT requires cloud services and similar services because IoT devices' calculation capability is inferior to cloud computing infrastructure. The cloud server receives long-distance data in transit that is exposed to a variety of cyber-attacks that can compromise user and data privacy and confidentiality. Due to its high sensitivity and the fact that it puts patients' and caregivers' lives at greater risk, the data that falls under the HIoT (Healthcare Internet of Things) or IoMT (Internet of Medical Things) umbrella is vulnerable to such assaults.

In this situation the IoT paradigm, cloud computing platforms have substantial opportunities for tackling excessive latency and privacy challenges. Cloud computing enables computation to happen on nearby IoT devices, display the information in real time and lowering the possible danger of data leakage during transmission. The cloud may nevertheless offer non-dynamic analytics and AI capabilities for the massive amounts of data collected to deliver significant services for IoT and cloud end-devices, even while the cloud infrastructure handles the latency issue. However, a unique set of security and privacy-preserving methods are necessary given the nature of cloud services. These need to be in line with its features, which include being spread across numerous data sources and being lightweight, efficient, and resource-constrained.

Cloud computing and the Internet of Things (IoT) both provide cutting-edge services that can reshape and increase the contemporary medical sector; To maintain the privacy of user data, including user habits, identity, and location, their dispersed nature must be controlled. The risk of data exposure is not limited to data loss via broken equipment or hacker assaults. The security of your data may also be greatly endangered by service and infrastructure providers. The employees of the provider's own company might pose an insider threat by using the data for personal advantage, selling it to other parties, or selling it to other third parties.

3. Proposed methodology

In the proposed methodology, an advanced design for preserving the privacy of massive amounts of data is developed based on three stages such as data encryption, optimal key generation, and blockchain based data transmission and data decryption. The work flow of the proposed methodology is shown below,

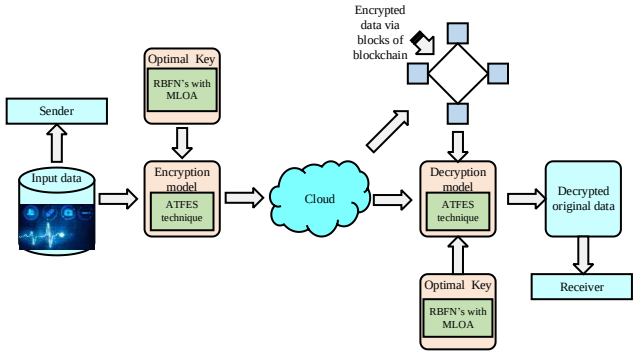

Fig 1: Proposed method's workflow

3.1. Advanced Twofish Encryption Standards (ATFES) Algorithm

3.1.1. Advanced Encryption standards (AES)

Utilising the symmetric block cypher, AES generates a key length of 128 bits. The AES algorithm is presently the strongest due to it is fast and secure for both encryption and decryption. Below are a few AES encryption procedures.

- The key is determined.
- For the turn's arrangement, the initial value is provided and initial rotations key is also provided.
- Rotation=1 to 13, with add round, shift rows, sub bytes, mix columns
- The final rounds key without mix-columns
- The encryptions output resides in rotation 14.

In each rotation four steps are considered:

- Mix-columns: Data in every state array column generated randomly.
- Sub-Bytes: as a hexadecimal substitution transformation.
- Add-Round Key: a round key operation is XOR among states. Its method generates Round-Key, one of that makes use of a substitution table.

In this, never use the "Mix-column" step until the 13th round and the final or 14th round for encryption. The

flowchart depicts the procedures of the Encryption and Decryption Algorithms described above as shown in Figure 2 and 3.

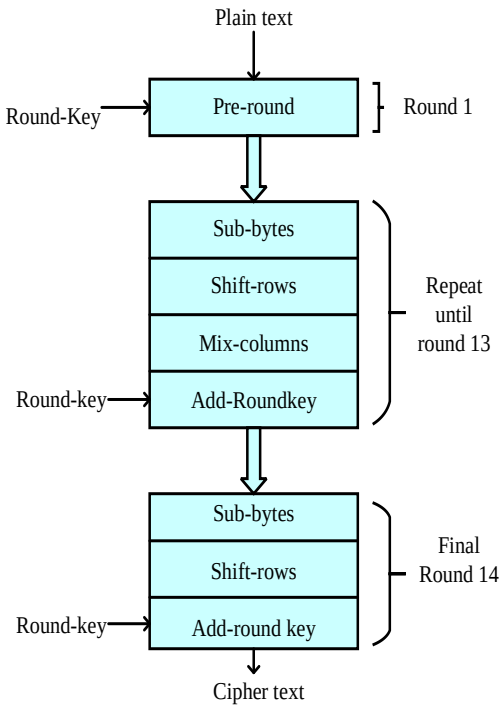

Fig 2: AES Encryption

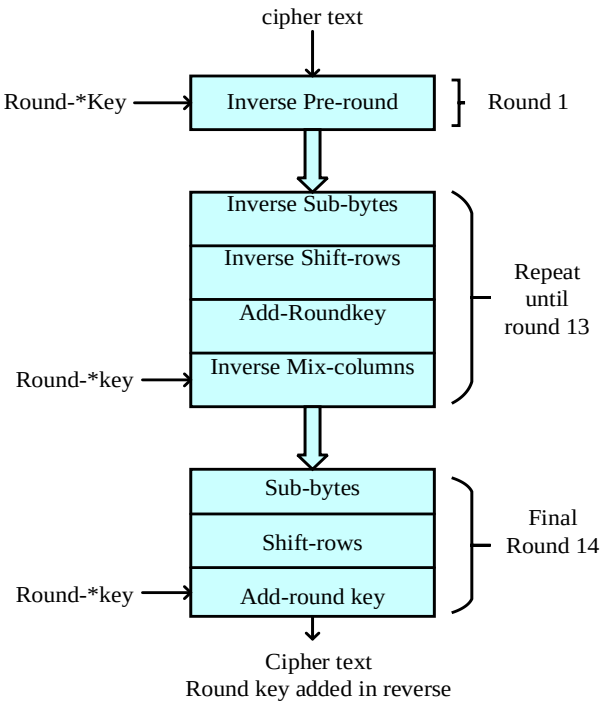

Fig 3: AES Decryption

3.1.2. Twofish algorithm

Twofish is more effective for devices that are integrated in hardware and run-on smaller devices. This enables the implementer to balance performance by adjusting the encryption timing, speed, and code size. Twofish is not patent - protected or open source, so it is free to use. Twofish uses block sizes of 128 bits and key sizes of 128, 192, and 256 bits. The cypher is constructed using GF (28), a Pseudo-Hadamard Transform, bitwise rotations, a fixed 4-by-4 maximum distance discernible matrix, and a carefully designed key schedule. The target F function is built of four key-dependent 8-by-8-bit S-boxes.

1. Plaintext P is classified into four 32-bits.
2. During the whitening input stage, with four keywords, it is XOR-ed.
3. A sixteen-round procedure is followed, in every round, for function g's input the leftmost two words are used.
4. The function g includes S-boxes that are dependent on the key bytes specified; the linear combining phase is then performed using the MDS matrix.
5. For every S-box 8-bit input is required and 8-bit output is produced.
6. Then, four outcomes are transmitted as vectors with length 4 and multiplied by the MDS 4X4 matrix.
7. Two functions outputs are integrated in addition to two keywords by utilizing Pseudo-Hadamard Transform.
8. The words XOR on the right are created by combining these two results.
9. For the next round, the left and right are switched.
10. Once all rounds have been completed, the final round exchange is reversed, and empathy has been XORed with four more keywords to create cypher text.

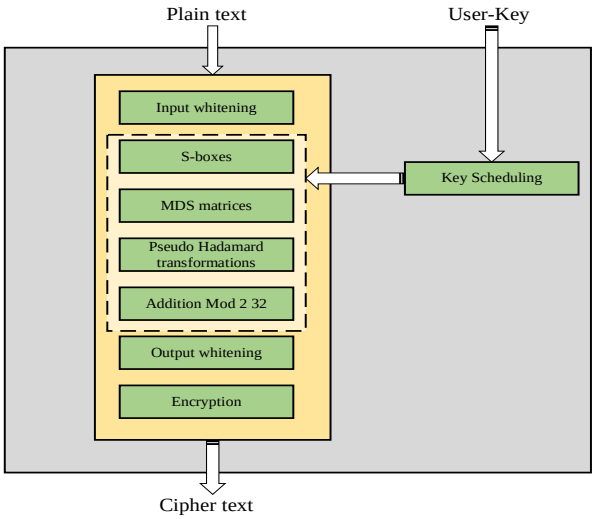

Fig 4: Twofish procedure

3.2. Radial Basis Function network

The Radial Basis Function network (RBFN) is a feed-forward artificial neural network that is widely used. There are three layers in RBFN: the input layer, output layer, and the one hidden layer. RFBN has a hidden layer and the linear output layer that accomplishes a nonlinear mapping into a higher-dimensional space from the input space in which training examples are linearly separated. The hidden layer contains RBF neurons, which all have a similar shape and an activation function. The ith neuron's activation function form is

$$z_j = \varphi\left(-\frac{\|y-\mu_j\|}{\sigma_j^2}\right) \quad (1)$$

Here, the radial basis function is φ, the radial basis function's centre is μ_j, and σ_j represents the peak width around μ_j. Moreover, the norm utilized in the activation function is different from Euclidean, that is the most popular alternative, and the activation function is typically selected to be a Gaussian basis function. Based on the Mayfly-Levy optimization the hidden layers activation function of the RBFN is improved and this helps in generating optimal key.

3.2.1. Mayfly-Levy optimization

3.2.2. Mayfly algorithm

Mayflies are insects that are part of the Ephemeroptera order, which is the palaenoptera family's suborder. These insects are most common in the United Kingdom all through the May month, thus the name "mayfly". Before becoming adult mayflies, immature mayfly's aquatic nymphs spend several years in developing. The male attracts the females by swarming within a few metres of the water. They perform as nuptials, moving in a distinct up-and-down motion sequence. Female mayflies migrate to such swarms to reproduce. It just takes a few seconds for that process to be completed before the eggs are thrown into the water and the cycle is resumed. In this, MA performs all necessary modifications, resulting in improved algorithm performance throughout different sized feature sets. The following are the mayfly's parameters:

• The Male Mayfly's Actions:

Eq. (1) is utilized to update the male mayfly's position:

$$P_x^s = P_x^{s+1} + r_x^{s+1} \quad (1)$$

In this,$P_x^s$is the present state of the male mayfly's more the velocity $r_x^{s+1}$is calculated with the current position, and achieves the next position P_x^{s+1}. The speed is also increased, some spacewhere on top of the water's surface the male mayfly's floats.In Equation 2, the measured male mayfly's velocity is given below.:

$$r_{ly}^{s+1} = H * r_{ly}^s + f_1 * G^{-\beta t_a^2} * (\text{abest}_{ly} - P_{ly}^s) + f_2 * G^{-\beta r_b^2} * (\text{bbest}_y - P_{ly}^s) \quad (2)$$

In this, r_{ly}^srepresents the mayfly's velocity at time s, r_{ly}^s in y dimension where the position of the same mayfly at time s, $f_1, f_2$are the constants of positive attraction where the involvement of social and cognitive factors quantified, b represents the gravitation a coefficient and β represents the fixed visibility's a coefficient, which reduces mayfly visibility to many others. abest_{ly} is the visited mayfly $l$position and it is best and bbest_y is the finest male mayfly's ythcomponent level. bbest_{ly}, minimization problem shown below:

$$\text{abest}_l = \begin{cases} p_l^{s+1} \\ if\ fitness(p_l^{s+1}) < fitness(\text{abest}_l) \end{cases} \quad (3)$$

In this, fitness (p_l^s) provides the fitness value's position, i.e., the standard of the solutions. At last, $t_a$represents the Cartesian distance among p_l and $\text{abest}_l$and t_b represents the Cartesian distance amongt_l and $bbest$. These are evaluated and illustrated below:

$$|p_l - w_l| = \sqrt{\sum_{y=1}^{i}(p_{ly} - w_{ly})2} \quad (4)$$

In this, p_{ly}denotes the element's position as y[th] and the mayfly's position as lth and $w_l$depicts either abest_l or $bbest$. The best mayfly's nuptial dance performance is significant because it randomly assigns acomponent to the algorithm. The mathematical equation for this performance is shown below.

$$r_{ly}^{s+1} = \text{b} * r_{ly}^s + \text{e} * \text{q} \quad (5)$$

In this, edenotes the nuptial dance coefficient, random value is denoted as q∈ $[-1, 1]$. The nuptial dance coefficient gradually decreases as $eitr = e0 \times \delta\ itr$. The initial value of nuptial dance coefficient's is e_0, the current number of the iterations is represented as itr and a random number δ is ∈ [0, 1].

• Female Mayfly Movement:

Female mayflies gather in groups near males to reproduce. The female mayfly is depicted in the succeeding position:

$$w_x^{s+1} = w_x^s + r_x^{s+1} \quad (6)$$

In this, present position of female mayfly's isw_x^sat time s is improved by calculating its velocity r_x^{s+1} . The present solution's attraction quality is a male and female attraction process, i.e., the finest male performance attracts the finest female performance, and so on. According to the equation below, the female velocity is boosted.

$$r_{ly}^{s+1} = \begin{cases} if\ fitness\ (x_l) > fitness(p_l) \\ h * r_{ly}^{s} + f_2 * g^{-\beta t_{vb}^2 * (z_{ly}^{s} - x_{ly}^{s})} \\ else\ if\ fitness(x_l) \leq fitness(p) \\ h * r_{ly}^{s} + bk * q \end{cases} \quad (7)$$

In this, r_{ly}^{s+1}at time s, denotes the yth element of the lth speed of female mayfly, x_{ly}^{s}denotes the female mayfly's position l in dimension y at time s, z_{ly}^{s}denotes the ythcomponent male mayfly position in lat time s, $f_2$and β are fixed constants for the transparency and attraction coefficients, respectively. In Eqn. b is the predetermined gravity coefficient (2), q is the random value which has $\in [-1, 1]$, and $t_{vb}$is the Cartesian distance in both the male and female mayflies depicted in eq (4). When a man is not attractive for female, a random walk coefficient is denoted as bk is and $bk_{itr} = bk_0 \times \delta_{itr}$. Where,$itr$ and δ are two variables that have already been described in equation (5).

• Mayfly's crossover technique:

The crossover procedure begins with identifying a male mayfly, followed by a female mayfly. Fitness value is used to make decisions, with the best male and female pairing. Following a crossing, two descendants are established, as shown in the equation. (9)

$$Offspringm = q_{jb} * male + (1 - q_{jb}) * female \quad (8)$$

$$Offspringn = q_{jb} * male + (1 - q_{jb}) * female \quad (9)$$

Male denotes the male mayfly parent, while female refers to the female mayfly's parent $q_{jb}$is a number among 0 to 1. The primary velocity of the progeny is initially set to 0.

• Mayfly transmutation:

The ability of this algorithm to explore is improved by causing the newly created progeny to mutate. Generally disbursed random digit is included within a variable progeny and is represented as,

$$Offsprings'_q = Offsprings_q + l \quad (10)$$

A random value q used here is normally distributed.

Levy flight method

In this levy flight is used to change the global finest component's position. For exploration purpose the levy flight method is used and for particular search it is associated.

$$R_{max} = Levy(\lambda) * (P_{xmax} - P_{xmin})$$

In this, λ represents the designed scale factor and is fixed as 1.

$$Levy(\lambda) = 0.01\ \frac{q_5\ \sigma}{|q_6|^{1/\beta}}$$

Moreover, σ is evaluated as:

$$\sigma = \left[\frac{\Gamma(1+\lambda)\sin\left(\pi\left(\lambda/2\right)\right)}{\left(\Gamma\left(\left(1+\lambda\right)/2\right)\lambda\left[2^{(\lambda-1)/2}\right]\right)}\right]^{1/\lambda}$$

In this, $\Gamma(w) = (w-1)!$, q_5 corresponds to $q_6$in range [0,1], $1 < \beta \leq 2$, $\beta = 1.5$ is the constant value. $Levy(\lambda)$ Represents the length of the step, mean values and infinite variance are incorporated with levy distribution with$1 < \lambda \leq 3$, λ denotes distribution factor, $\Gamma(.)$ represents gamma distribution function.

3.3. Blocks of Blockchain

In order to accomplish their security goals, privacy-preserving reputation devices employ a variety of building blocks, most of which are cryptographic in nature. Such building blocks encompass homomorphic cryptosystems, secure multi-party computation, blockchain, zero-knowledge proofs, and so on. A distributed data structure called a blockchain is developed as the basis for the Bitcoin cryptocurrency. A public distributed ledger blockchain is made up of a series of blocks connected by cryptographic hashes. Every block contains a record of a set of operations or transactions which have occurred recently among users.

A blockchain has several significant advantages. It records the immutable information that further means that once recorded, the information cannot be changed and its persistence and integrity are assured. Furthermore, it offers transparency because all the information provided is public and every information's block is concatenation in an auditable way. Furthermore, it is decentralised because no reliable outside source or super node has associated on this preservation. In this network, each node validates the integrity of blockchain and start competing for the right to add a new block. This decentralisation also results in a property known as trust lessness, which allows users to collaborate and cooperate without the need to rely on one another. Blockchains helps privacy-preserving reputation frameworks in a variety of ways. Because of its auditability, transparency, and immutability, a blockchain is utilized to generate a reputation framework that allows users to authenticate the reputation score computation's integrity. The encrypted data are kept in the cloud and transmitted using this blockchain blocks.

4. Results and Discussion

In the proposed method, chest X-ray image database is selected. This image dataset is encrypted by using the proposed ATFES technique. Then, to encrypt these data, an optimal key is generated based on Optimized Radial Basis Function Networks (RBFNs) leveraged with Mayfly-Levy optimization algorithm (MLOA) method. Once the data are encrypted, these data are placed in cloud and then transmitted using blocks of blockchain. At last, for

decryption, the same optimal key has to be used to restore the encrypted data. The performance of the suggested method was analysed by several performance metrics such as throughput, energy, delivery ratio, delay, latency, and overhead.

4.1. Performance metrices

Throughput:

Throughput is the number of packets distributed or data transmitted successfully via a communication link to their destination per unit time.

Energy

The average energy efficiency level of mobile nodes during routing and communication

Delivery ratio

The ratio of data bits delivered to the receiver from the sender to the total amount of data bits received is known as the data bit ratio.

Delay

Delay is the length of time it takes for a data packet to get from the sender to the receiver. By dividing the total number of packets acquired owing to the time difference between receiving and transmitting a single packet, the total time difference is determined.

Overhead

Because of node mobility and frequent route searching, frequent links are destroyed.

Latency

The duration that it takes for a data packet to go from its source to its destination is known as latency.

4.2. Performance analysis

In this research, suggested method ATFES were compared with the existing techniques including AES, Elliptic Curve Cryptography (ECC), and Genetic-based Algorithm. The comparison is carried out based on the performance metrics. The overall performance analysis shows that the suggested method is efficient more than the other state-of-art. An implementation is carried out on the platform of MATLAB.

Table 1: Performance comparison of the existing and the proposed methods

Performance metrics	Proposed Technique (ATFES)	Existing Technique		
		AES	ECC	Genetic-based cryptography
Throughput bps	23,000	20,000	21,500	22,000
Energy J	0.9700	0.9300	0.9500	0.9600
Delivery ratio %	6.8000	7.2000	7.1000	7.0000
Delay J	2.5000	3.5000	3.4000	2.9000
Overhead %	54.000	57.000	58.000	55.000
Latencyms	10	15	13	12

The performance of the existing method and the proposed methods on the chest X-ray image database are compared in the table 1. The overall performance shows that the suggested method is greater than the other state-of-art.

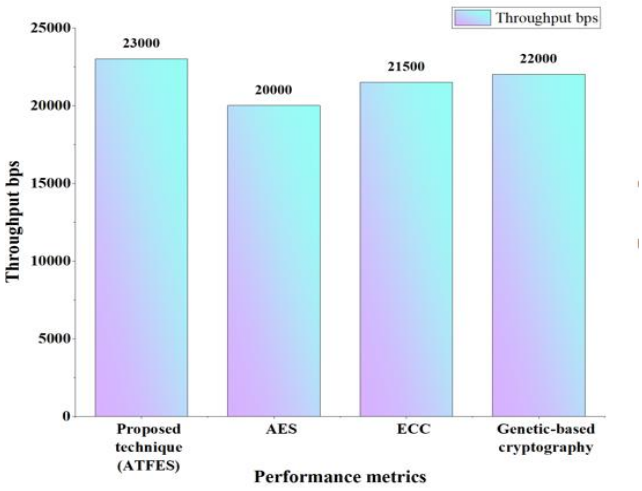

Fig 5: Performance comparison of throughput

In the figure 5, the proposed and the existing methods are compared by using the performance metrics throughput. The suggested method achieves 23000 which is higher than the existing methods AES, ECC, and Genetic-based cryptography 20000, 21500, and 22000.

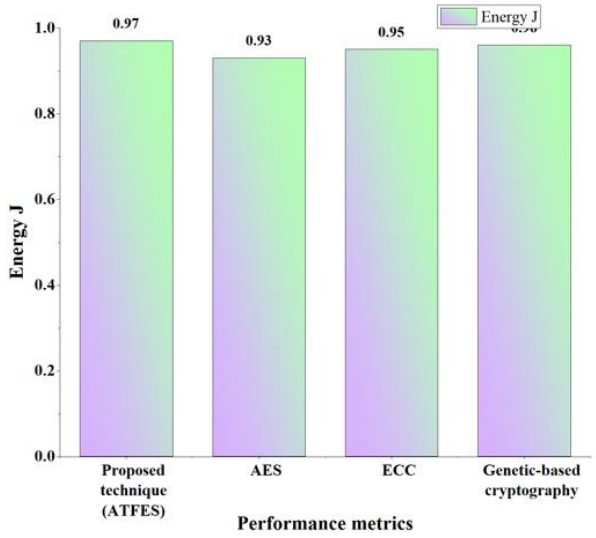

Fig 6: Performance comparison of Energy

In the figure 6, the suggested and the present methods performance metrics energy are compared. The proposed method obtains 0.97 which is higher than the existing methods AES, ECC, and Genetic-based cryptography 0.93, 0.95, and 0.90.

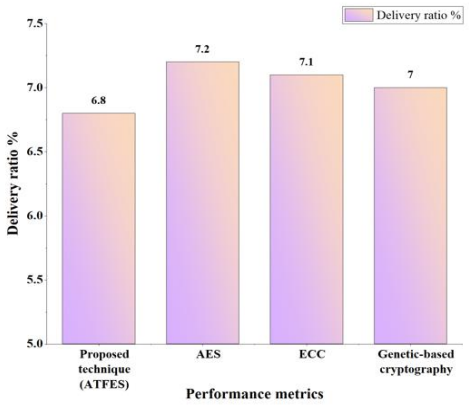

Fig 7: Performance comparison of delivery ratio

In the figure 7, the proposed and the existing methods are compared by using the performance metrics Delivery ratio. The suggested method achieves 6.8 which is higher than the existing methods AES, ECC, and Genetic-based cryptography 7.2, 7.1, and 7.

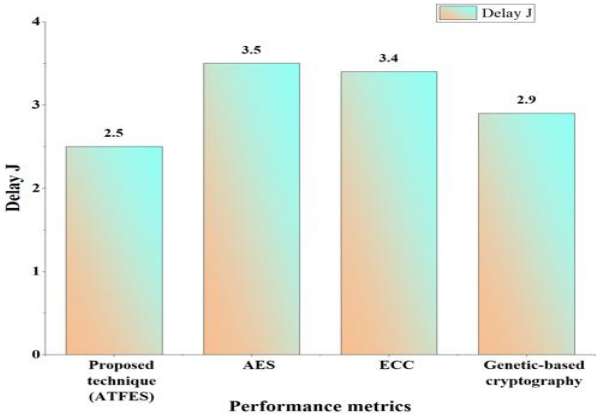

Fig 8: Performance comparison of Delay

In the figure 8, the suggested and the present methods performance metrics Delay are compared. The proposed method obtains 2.5 which is higher than the existing methods AES, ECC, and Genetic-based cryptography 3.5, 3.4, and 2.9.

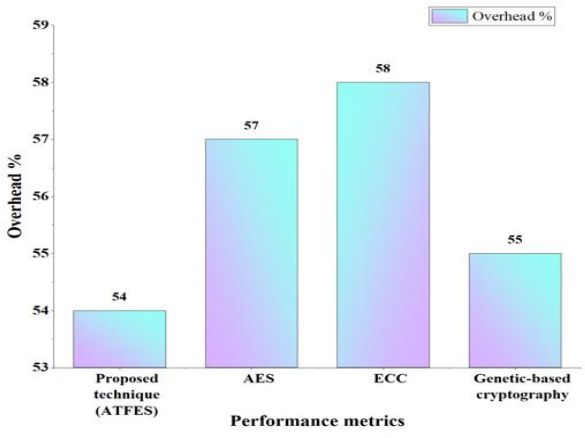

Fig 9: Performance comparison of overhead

In the figure 9, the proposed and the existing methods are compared by using the performance metrics overhead. The suggested method achieves 54 which is higher than the existing methods AES, ECC, and Genetic-based cryptography 57, 58, and 55.

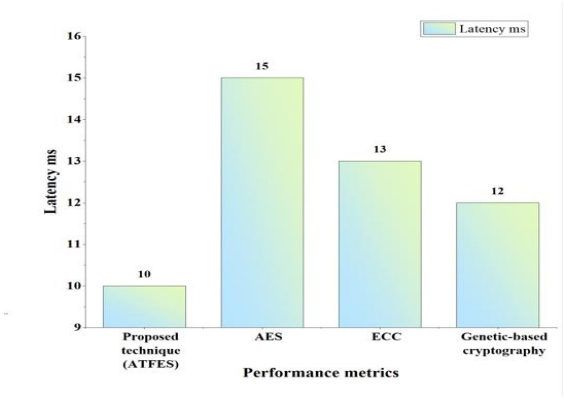

Fig 10: Performance comparison of latency

In the figure 10, the suggested and the present methods performance metrics latency are compared. The proposed method obtains 10 which is higher than the existing methods AES, ECC, and Genetic-based cryptography 15, 13, and 12. The overall performance proves that the suggested ATFES technique is more efficient than existing AES, ECC, and Genetic-based cryptography methods.

5. Conclusion

An effective approach is required to preserve and safeguard people's data privacy in terms of secrecy and dependability. Raw records are gathered and those collected records are encrypted by using a new Advanced Twofish Encryption standard (ATFES) algorithm. For encryption and decryption, an optimal key was generated by using Optimized Radial Basis Function Networks (RBFNs) leveraged with Mayfly-Levy optimization algorithm (MLOA). Then, the data encrypted are placed on cloud and the transferred through blocks of blockchain. Finally, the same optimal key must be used to restore the encrypted data; otherwise, the data cannot be restored. The results of the proposed and the existing techniques were compared by using several performance metrics such as throughput, energy, delivery ratio, delay, overhead, and latency. The overall performance shows that the proposed technique is more efficient than the other state-of-art. Furthermore, privacy preservation for machine learning has to be considered in more complex environments and the privacy preservation for other novel methods also need to be investigated.

References

[1] Chen, Y., Ding, S., Xu, Z., Zheng, H. and Yang, S., 2019. Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), pp.1-9.

[2] Bagloee, S.A., Heshmati, M., Dia, H., Ghaderi, H., Pettit, C. and Asadi, M., 2021. Blockchain: the operating system of smart cities. Cities, 112, p.103104.

[3] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making, 20(1), pp.1-10.

[4] Das, M., Luo, H. and Cheng, J.C., 2020. Securing interim payments in construction projects through a blockchain-based framework. Automation in construction, 118, p.103284.

[5] Ghimire, T., Joshi, A., Sen, S., Kapruan, C., Chadha, U. and Selvaraj, S.K., 2021. Blockchain in additive manufacturing processes: recent trends & its future possibilities. Materials Today: Proceedings.

[6] Dwivedi, V., Norta, A., Wulf, A., Leiding, B., Saxena, S. and Udokwu, C., 2021. A formal specification smart-contract language for legally binding decentralized autonomous organizations. IEEE Access, 9, pp.76069-76082.

[7] Amir Latif, R.M., Hussain, K., Jhanjhi, N.Z., Nayyar, A. and Rizwan, O., 2020. A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. Multimedia tools and applications, pp.1-24.

[8] Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E. and Imran, M., 2019. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Generation Computer Systems, 100, pp.325-343.

[9] Deng, H., Qin, Z., Wu, Q., Guan, Z. and Zhou, Y., 2020. Flexible attribute-based proxy re-encryption for efficient data sharing. Information Sciences, 511, pp.94-113.

[10] Sun, S., Ma, H., Song, Z. and Zhang, R., 2020. WebCloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms. IEEE Transactions on Dependable and Secure Computing.

[11] Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q. and Zheng, D., 2019. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Annals of Telecommunications, 74(7), pp.401-411.

[12] Al-Asli, M., Elrabaa, M.E. and Abu-Amara, M., 2018. FPGA-based symmetric re-encryption scheme to secure data processing for cloud-integrated internet

of things. IEEE Internet of Things Journal, 6(1), pp.446-457.

[13] Sun, J., Xu, G., Zhang, T., Xiong, H., Li, H. and Deng, R., 2021. Share your data carefree: An efficient, scalable and privacy-preserving data sharing service in cloud computing. IEEE Transactions on Cloud Computing.

[14] Awotunde, J.B., Folorunso, S.O., Bhoi, A.K., Adebayo, P.O. and Ijaz, M.F., 2021. Disease diagnosis system for IoT-based wearable body sensors with machine learning algorithm. In Hybrid Artificial Intelligence and IoT in Healthcare (pp. 201-222). Springer, Singapore.

[15] Wang, S., Zhang, Y. and Zhang, Y., 2018. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access, 6, pp.38437-38450.

[16] Jing Li, XiaohuiKuang, Shujie Lina, Xu Ma, Yi Tange, "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes", Information Sciences, Vol. 526, pp. 166-179, 2020.

[17] Qi Wang, Dehua Zhou, Shiyin Yang, Peng Li, Chuansheng Wang, Quanlong Guan, "Privacy Preserving Computations over Healthcare Data", IEEE, 2019.

[18] Haiping Huang, Peng Zhua,b, Fu Xiao, Xiang, Qinglong Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data", Computer & Security, Vol.99, 2020.

[19] Koosha Mohammad Hossein, Mohammad EsmaeilEsmaeili, TooskaDargahi, Ahmad Khonsari, Mauro Conti, "BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications", Computer Communications, vol.180, pp. 31-47, 2021.

[20] A. Sathya, S.Kanaga Suba Raja, "Privacy Preservation Based Access Control Intelligence for Cloud Data Storage in Smart Healthcare Infrastructure", Springer, 2021.

[21] NikunjDomadiya, UdaiPratap Rao, "Improving healthcare services using source anonymous scheme with privacy preserving distributed healthcare data collection and mining", Springer, 2020.

[22] Zijie Yue, Shuai Ding, Lei Zhao, Youtao Zhang, Zehong Cao, M. Tanveer, AlirezaJolfaei, Xi Zheng, "Privacy-preserving Time-series Medical Images Analysis Using a Hybrid Deep Learning Framework", ACM Transactions on Internet Technology, Vol.21, 2021.

[23] Jinwen Liang, Zheng Qin, Sheng Xiao, Jixin Zhang, Hui Yin, Keqin Li, "Privacy-preserving range query over multi-source electronic health records in public clouds", Journal of Parallel and Distributed Computing, vol.135, pp. 127-139, 2020.

[24] R. Ramya Devi, V. VijayaChamundeeswari, "Triple DES: Privacy Preserving in Big Data Healthcare", International Journal of Parallel Programming, 2018.

[25] TehsinKanwal, AdeelAnjum, SaifU.R.Malik, Abid Khan, MuazzamA.Khan, "Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud", Computer Standards & Interfaces, Vol.78, 2021.

[26] Dataset collected from http://www.cell.com/cell/fulltext/S0092-8674(18)30154-5, 2022-10-15

[27] Rajiv, A., Saxena, A.K., Singh, D., Awasthi, A., Dhabliya, D., Yadav, R.K., Gupta, A. IoT and machine learning on smart home-based data and a perspective on fog computing implementation (2023) Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries, pp. 336-349.

[28] Chaudhury, S., Dhabliya, D., Madan, S., Chakrabarti, S. Blockchain technology: A global provider of digital technology and services (2023) Building Secure Business Models Through Blockchain Technology: Tactics, Methods, Limitations, and Performance, pp. 168-193.