Asian Journal of Water, Environment and Pollution Vol. 22, No. 1 (2025), pp. 149-165.
doi: 10.36922/AJWEP025040017

ORIGINAL RESEARCH ARTICLE

Securing smart health in smart cities: Blockchain technology to secure electronic health data sharing

Varsha Mhaske* and P. M. Ashok Kumar*

Department of Computer Science Engineering, College of Engineering, KL University, Guntur, Andhra Pradesh, India

(This article belongs to the *Special Issue: Renewable Energy Systems and Strategies in Smart Grids and Smart Cities Development*)

***Corresponding authors:** Varsha Mhaske (mailvm13@gmail.com); P. M. Ashok Kumar (profpmashok@gmail.com)

Received: January 20, 2025; Revised: February 14, 2025; Accepted: February 25, 2025; Published online: March 24, 2025

Abstract: In the era of smart cities, safeguarding electronic health records (EHRs) is crucial to ensure the privacy and security of citizens' sensitive medical information. Existing medical data transfer methods are vulnerable to privacy breaches, making it challenging to protect patient data. This research proposes a novel blockchain-based approach to secure EHR sharing in smart cities. Our method leverages improved association rule mining to identify sensitive information, which is then encrypted using the Siberian Tiger Integrated Tuna Swarm algorithm to generate an optimal encryption key. The encrypted data are stored on a blockchain, ensuring its integrity and confidentiality. Our proposed model demonstrates maximum robustness against various attacks, including chosen ciphertext attack, chosen-plaintext attack, known ciphertext attack, and known-plaintext attack. This research contributes to the development of secure and privacy-preserving smart health infrastructure in smart cities, enabling the safe sharing of EHRs and promoting better health-care outcomes.

Keywords: Medical data; Improved association rule mining; Blockchain; Optimal key; Siberian tiger integrated tuna swarm algorithm optimization

1. Introduction

Health-care-related data are produced, saved, and used extensively in large quantities. Electronic health records (EHRs) are one of the most significant components of health-care systems, offering numerous benefits to health-care stakeholders.[1-3] For instance, it saves patients from costly testing, radiography, and recurrent imaging while enabling them to access their medical information. Furthermore, clinicians across different health-care institutions can use EHR to access patient information, even if the patient receives care in separate locations. In addition, EHRs allow doctors to review a patient's past medication history, aiding in prescription recommendations.[4-6] The utilization of patient medical information for research of novel treatment approaches is another benefit of employing EHRs.

Ensuring patient privacy is a fundamental concern while utilizing EHRs in the health-care industry[7-9] due to the widespread access to medical information. An additional challenge for EHR is that patients do not own their data; instead, the medicinal centers hold ownership of patient data. A key issue regarding patient privacy is that medical professionals and investigators can access their EHR without the patient's consent.[10,11] From a security standpoint, several challenges arise with the use of EHRs.[12,13] These issues can potentially be addressed through the use of blockchain technology

(BT). BT is an effective distributed ledger system for effectively recording transactions between two parties. Every transaction is stored in a "block," and these blocks are then joined together using encryption to create a blockchain.[14-16] As a decentralized transaction system, BT can also facilitate data management. Secure network transactions are carried out through BT,[17,18] which does not rely on a centralized authority. This ensures data integrity, security, and transparency without intrusion from any external organization. This is one of the key reasons behind the growing interest in BT,[19-21] which in turn creates research opportunities across various fields.[16,17] In addition, homomorphic encryption enables computations to be performed on encrypted data without the need for decryption, enabling secure processing of encrypted health-care data[22,23] while preserving privacy and facilitating analysis and insights.

Below are the contributions of the proposed privacy preservation (PP) model for EHR using BT:

(i) A new PP model is proposed, which introduces an improved association rule (ASR) mining (ARM) method for mining rules. This avoids data leaks and addresses the complexity of interpreting results. In addition, it can uncover complicated and subtle associations in the data and manage data variations over time

(ii) The model introduces the Siberian Tiger Integrated Tuna Swarm algorithm (STI-TSA) optimization for optimal key generation by including the concepts of Secretary Bird Optimization (SBO) and the Tuna Swarm algorithm. The STI-TSA optimization could attain faster convergence and create high-quality solutions.

The review of PP with BT is presented in Section 2. An overview of the proposed work is provided in Section 3. Improved ARM and STI-TSA are explained in Sections 4 and 5, respectively. Data restoration is explained in Section 6. The results and conclusions are presented in Sections 7 and 8.

2. Literature review

Bio-inspired metaheuristic algorithms have recently gained significant attention as effective tools for resolving challenging optimization issues. The Tuna Swarm Optimization (TSO), introduced by Xie *et al*.,[24] improves global optimization performance by imitating the hunting and foraging habits of tuna fish. Their research showed how effective TSO is at solving a range of benchmark and practical optimization issues. The Siberian Tiger Optimization (STO) algorithm, proposed by Trojovský *et al*.,[25] was motivated by the predatory tactics of Siberian tigers. This algorithm demonstrated its ability to handle difficult optimization tasks by performing exceptionally well in engineering optimization problems. The combination of these naturally inspired methods demonstrates the continuous progress in evolutionary computing and swarm intelligence.

In 2021, Verma[26] presented a unique blockchain system to secure health records in the cloud. This technology ensured the authentication and integrity of medical information. To achieve this, they employed an enhanced Blowfish model that ensured authentication features were used to install blockchain with the best encryption. In addition, a novel method known as the Elephant Herding Optimization with Opposition-based Learning (EHO-OBL) was used to generate optimal keys. Thus, the created technique preserved the integrity of the data, and the superiority of the proposed approach was demonstrated through various performance metrics.

In 2023, Irshad *et al*.[27] proposed data restoration and sanitization procedures to generate keys from the collected data, creating an objective function for the information preservation ratio (IPR), modification degree (MD), and hiding failure rate (HFR). To ensure robust security when transferring health-care data to the cloud, they employed the bee-foraging learning particle swarm optimization (BFL-PSO) method to identify the optimal key.

Large datasets have necessitated the development of effective data mining and privacy-preserving methods. A reference point for assessing machine learning models in health-care analytics is the University of California Irvine Heart Disease dataset.[28] An enhanced ARM approach was proposed by Zhao *et al*.[29] to improve the effectiveness of pattern finding in huge datasets, showing notable gains in accuracy and processing time. To improve data security in cloud contexts, Ahamad *et al*.[30] presented a multi-objective PP model that uses a hybrid Jaya-based Shark Smell Optimization technique. Furthermore, a modified Apriori approach was introduced by Baffour *et al*.[31] to speed up and increase the accuracy of frequent itemset creation. These studies collectively contribute to the advancement of data mining, security, and optimization techniques in handling large-scale data.

A new scheme that employed medical experts to monitor patient data and provide extra units was proposed by Saraswat *et al.*[32] in 2023. Several experiments were conducted to evaluate the performance of the suggested

model, and the results show that the proposed method can efficiently handle a large dataset with minimal latency. The proposed research achieved 98% maximum efficiency, 95% transaction latency, 96% overall system execution time, 92% data security, and 95% data scalability.

In 2023, Alsuqaih *et al.*[33] proposed a secure PP diagnostic technique for e-health websites that utilized BT. The suggested work offered a functional access control system, which may allow data owners to specify access controls for their private medical data. Users can efficiently add or remove authorized physicians using their user interactions for key generation. Security evaluations and experimental data demonstrate the suitability of the suggested health-chain framework for intelligent health-care systems. The comprehensive experimental analysis highlights BT's computing efficiency and resilience against various security breaches.

In 2024, Wang[34] skillfully modified data structures to meet the changing requirements of storage control and safe access. He used a unique data structure called the Enhanced Merkle Tree (EMT). To meet the needs of e-healthcare systems (e-HS), Wang adapted the traditional MT design employed by BT. The EMT significantly enhanced data integrity control and strengthened data security for access and storage. With several branches, leaves, and an individual root node, the consistent three-degree MT enables updated data validation, verification, and authentication processes. When the suggested approach was used in the e-HS, the suggested EMT performed better than existing techniques, obtaining a minimum validation duration of 14.26 m for 100 exchanges. As a result, this research advanced the discussion on privacy by offering a creative and practical solution specifically designed to address the unique challenges faced by e-HS.

A blockchain-inspired, safe, and dependable data exchange architecture for the cyber-physical medical industry 4.0 was introduced by Kumar *et al.*[35] in 2023. To enhance Healthcare 4.0, the suggested system used various encryption methods. In addition, a secure health-care architecture powered by blockchain was proposed to manage and access patient and physician information. A patient-centric approach was used to create a blockchain-oriented EHR exchange system. This implied that the owner retains complete ownership over their data, with BT providing security and privacy. According to testing findings, the suggested design can withstand various security threats and restore data, even if two or three nodes fail. The suggested paradigm was patient-centric, ensuring that even system administrators cannot access data without user authorization. This approach empowers patients with control over their data, improving security and privacy.

For increased security and scalability, Sutradhar *et al.*[36] proposed an access and identity management framework. Large data volumes and numerous applications may be supported by the suggested method, which made it a scalable and safe way to control accessibility to the Fabric system. Furthermore, to protect patient privacy and confidentiality, this system used role-based access restrictions depending on the patient's function. The statistical research showed that the suggested method can effectively and safely handle patient information and access, which might revolutionize the health-care sector by boosting data interoperability and strengthening patient security and privacy.

A secure and confidential Global Network Record-sharing consortium blockchain-sequential minimal optimization technique for diagnostic enhancements in Cyber-Physical System e-HS that utilizes the BT was presented by Hemalatha *et al.*[37] in 2023. They used two different strategies, such as consortium blockchains, which were constructed through the creation of consensus procedures and data structures. The public key was secured with keyword search to safeguard data, maintain privacy, manage access, and provide a secured search. The security analysis indicated that the proposed protocol can meet the security objectives. Furthermore, Apache JMeter was used to evaluate the efficacy of the proposed technique. The suggested effort has a 99% forecast accuracy rate at a fair time cost.

In 2023, Yi[38] introduced a cloud-based system, including post-quantum searchable encryption, in which key generation utilizing Physical Unable Functions was a part of it. Medical records were encrypted and stored in the cloud, whereas records were verified by BT and retrieved through the cloud. A safe and effective cloud-oriented health data system was suggested for digital twins by combining cloud encryption, blockchain verification, and cloud retrieval. Compared to similar concepts, this implementation shows that the system offered consumers safe and effective medical record services. This demonstrated how digital twins may revolutionize health care by enabling safe, data-driven, individualized planning, diagnosis, and treatment.

A blockchain-orchestrated deep learning (DL) technique for secure data transmission in an Internet of Things-enabled health-care system was created in 2023 by Kumar *et al.*[39] This approach was referred

to as "BDSDT." In particular, by utilizing the Zero Knowledge Proof technique, a unique adaptable BT was suggested to guarantee confidentiality as well as safe data transfer. To identify intrusions in the HS network, a DL method was designed using the verified data. Then, an efficient intrusion detection system was created by combining bidirectional long short-term memory with deep sparse autoencoder.

The rapid adoption of ubiquitous computing and mobile communication has led to the emergence of mobile health, while urbanization has driven the development of smart cities. The concept of smart health integrates these two trends, creating a context-aware health-care system within smart cities to enhance service efficiency and human-centered care.[40] Context-aware health-care systems that utilize context awareness in smart health-care applications emphasize the importance of user demographics, location, and medical history, which aligns with the concept of smart health within smart cities.[41] With the rapid development of machine learning for the detection of diseases using imaging scans,[42,43] patient records have become an invaluable resource. It facilitates diagnostics, leading to the development of artificial intelligence-based medical techniques. EHRs are simpler to access and manage than paper records, but more caution is needed to ensure that the privacy of the data is maintained. Because of their centralized architecture, traditional and modern EHR systems, which are utilized for exchanging data between medical participants (patients, doctors, insurers, pharmaceuticals, doctors, and researchers), have security and privacy flaws. To prevent breaches of information privacy, several clinics and institutions have prohibited medical data transfer and exchange. Data barriers have arisen as a consequence of health data being dispersed among several health-care providers, exacerbated by concerns over health-care data security and privacy. As a result, BT is proposed as a solution, using encryption to guarantee the security and privacy of EHR systems. BT overcomes the limitations of traditional centralized systems, which are often inaccessible. The existing health-care system is perceived as complicated and expensive, but BT can mitigate these issues by enhancing insurance management and data handling. Furthermore, the decentralized nature of this system eliminates central attack points and reduces the risk of system failures.

3. PP of EHRs using BT

EHRs are digital patient records stored on networks. Still, current storage methods have proven to be quite vulnerable, where hackers and other unapproved parties can readily access the data. This vulnerability not only compromises patient data but restricts access for patients and health-care professionals. The existing approaches are unable to strike a compromise between data accessibility and security. However, BT offers a promising solution to these problems. Blockchain establishes an immutable ledger system that enables decentralized transaction processing. A novel PP technique is proposed for securing EHR, with stages shown in Figure 1.

Initially, the improved ARM approach is used to analyze medical data and find the ASRs between the data characteristics. These rules are important since they aid in identifying sensitive items in the dataset. Improvement in ARM approaches improves the process and guarantees a more precise identification of patterns in sensitive data. After identifying the ASRs, the SBI-TSA method is developed to identify the optimal keys, which are employed to encrypt and decode sensitive data. These optimal keys are derived by considering IPR, HFR, and MD.

The sensitive data are subjected to an exclusive OR (XOR) operation for sanitization using the optimal keys. This sanitized data is then stored on a blockchain. This phase ensures that the stored data cannot be decrypted without the matching key, even in the event of illegal access. When retrieval is necessary, the sanitized data undergoes a reverse XOR process with the optimal key, restoring it to its original format. This decryption process allows authorized individuals to safely access and use the information.

4. Data sanitization using improved ARM

Assume the medical dataset as d^s and D_t as the data within the dataset. This medical data D_t ($D_i = \{D_1, D_2, \ldots D_n\}$) is initially processed using the improved ARM. Data sanitization is vital for conserving privacy by sanitizing data D_t. Sanitization includes precisely identifying the sensitive information within the data to protect data privacy while preserving the data validity.

4.1. Conventional ARM

ARM analyzes input medical data D_t to find significant correlations or links between different elements, including diseases, therapies, indications, and other factors. By finding important patterns in huge datasets, this approach seeks to provide insights that might improve patient care and decision-making. These methods selectively hide some ASRs that may otherwise

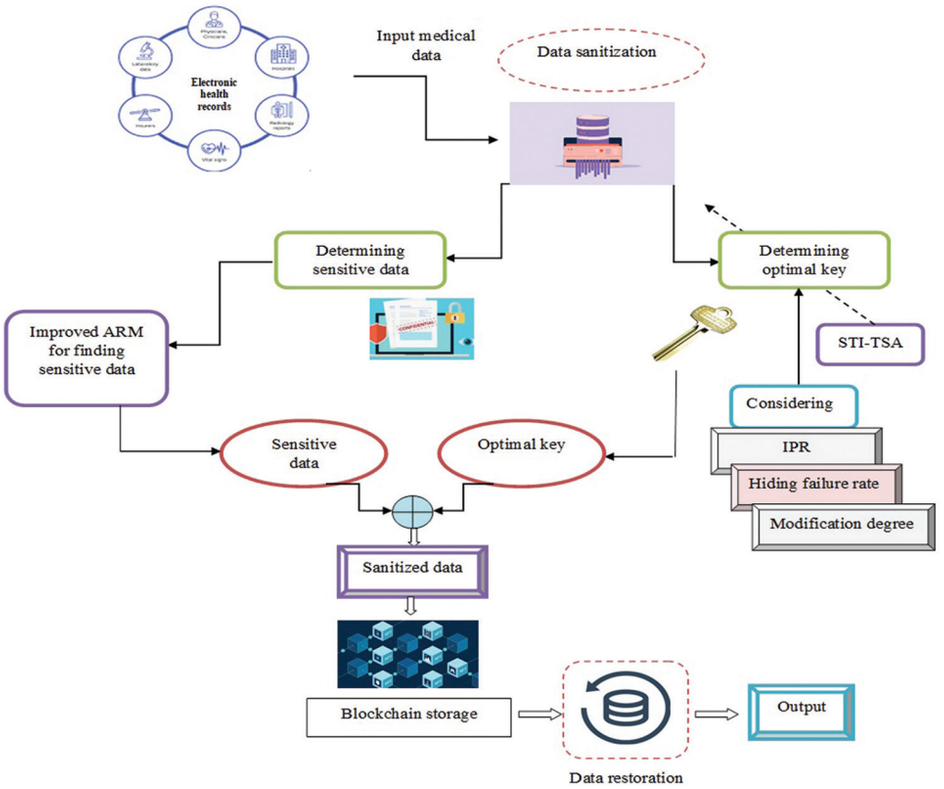

Figure 1. The architecture of privacy preservation for electronic health records using blockchain technology
Abbreviations: ARM: Association rule mining; IPR: Information preservation ratio; STI-TSA: Siberian tiger integrated tuna swarm algorithm.

uncover delicate patterns seen in the medical data D_i. The section that follows provides a thorough procedural description, and Figure 2 displays the flow chart for conventional ARM.[37]

(i) Step 1: Frequent item set generation
The first step is to identify frequent distinct items. Items that meet a minimum support threshold (MST), "minsup," are noted as M (1). Recognize the frequent items (M [1]) that occur in transactions with a threshold equal to or greater than the "minsup" threshold.

(ii) Step 2: Candidate item (CI) generation
The frequent item sets identified in Step 1, (M [1]), should be used to generate CI (F^i [L + 1]). Merge frequent item sets of length l (from M [L]) to generate CI with length L + 1. Eliminate any CI that contains subsets that are not frequent, those that do not exist in M (L).

(iii) Step 3: Examining support in the database
The transaction database D^{base} is scanned to count the occurrence of individual CI (F^i [L + 1]). Compute the support of every CI (F^i [L + 1]) by evaluating the transactions. If CI support is above or equivalent to "minsup," it is said to be a frequent item set and summed to M [L + 1].

(iv) Step 4: Iteration and completion
Repeat Steps 2 and 3 until no further frequent item sets M [L + 1] can be created. The anticipated result is the combination of entire frequent item sets attained across diverse lengths: the union of M [1] and M [2]. The process stops when no novel frequent item sets (M [L + 1]) are generated.

The ultimate result is derived by merging every frequent item set revealed during the iterations. The frequent item sets jointly signify the associations in d^s that satisfy the MST.

However, the traditional ARM method is more susceptible to data leaks and suffers from interpretation complexity. This might result in poor-quality data that causes erroneous rules, leading to imprecise transaction records.

To overcome these drawbacks, an improved ARM method is introduced in this work. The improved ARM could mine the rules quicker with large datasets. It

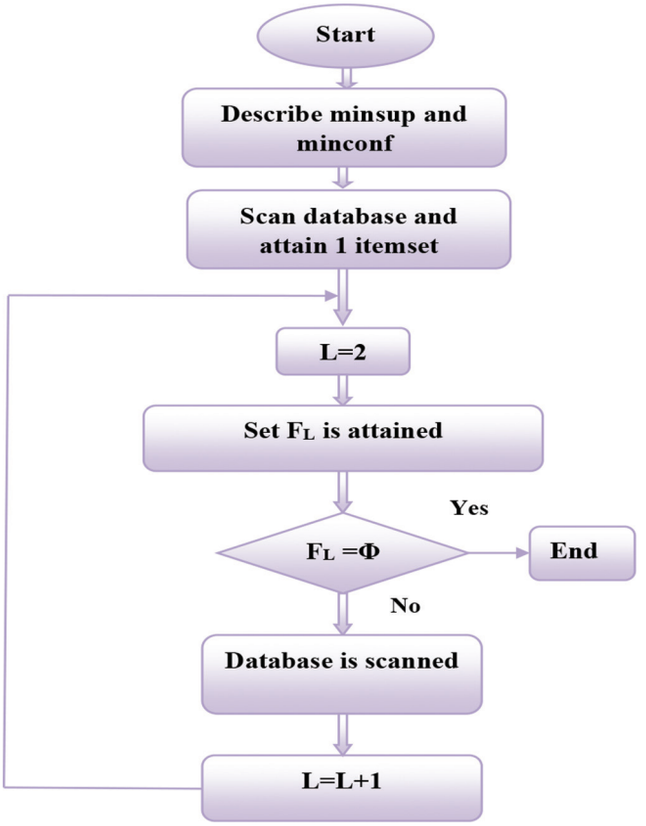

Figure 2. Flowchart for conventional association rule mining
Abbreviations: L: Length; minsup: Minimum support threshold.

creates more meaningful and precise rules. The improved ARM could identify complicated and subtle associations in the data and manage data variations over time. The procedure for the improved ARM is detailed below.

4.2. Improved ARM

The proposed improved ARM is detailed below with a flowchart representation illustrated in Figure 3.

(i) Initialization and database scanning
Initiate the process by scanning the dataset to detect frequent items that fulfill a predetermined MST. The MST is assessed in Equation I, where *Maxi* and *Mini* refer to maximum and minimum threshold values. Table 1 shows an exemplary demonstration of MST computation.

$$MST = (Maxi + Mini)/2 \quad \text{(I)}$$

In Table 1, the maximal occurrence is seven, and the minimal occurrence is two. The mean of these values is computed in Equation II.

$$MST = \frac{(7+2)}{2} = 4.5 \simeq 5 \quad \text{(II)}$$

In Table 2, the frequent items are identified as Items A and B, with a value of seven each, surpassing the MST of 5. Likewise, Item C has a value of 6 that surpasses the MST. Subsequently, an array is formed to store these frequent items. Based on Table 2, the uncommon items are eliminated. Subsequently, Table 3 shows a sample dataset, and Table 4 reveals the sample dataset after eliminating the uncommon items.[39]

(ii) Generating combinations.
After eliminating the uncommon items, the frequent items are united, as shown in Table 5.

After implementing the procedure of combination generation, the following stage is dynamic itemset counting.

(iii) Dynamic itemset counting:
The blank item sets are spotted with a solid box. All the item sets are spotted in dashed rounds. The transaction experimental values that range from 1 to 55 are read and marked with a dashed circle. When the count of dash circles goes beyond the threshold, it turns into a dash square. The support threshold (*ST*) is computed as in Equation III, where *TSC* denotes the total count of transactions.

$$ST = \left\{ \left[\frac{MST}{100} \right] \times TSC \right\} \quad \text{(III)}$$

Item sets that appear frequently in the transactions are regarded as frequent, and after the final count, these sets are identified as solid. After dynamic item set counting, the item set is represented as a Boolean matrix, which is then converted to its 2's complement. The subsequent stage checks for redundant items in the dataset. If yes, eliminate redundant items using transaction compression methods. If not, continue to the following step of database scanning.

Fix L size as 2 and item set F_j is attained. If F_j = 0, remove redundant item sets using transaction compression approaches. Otherwise, continue to the following step of database scanning and increase L by 1.

Replicate the procedure of producing and verifying CI F_j till no further item sets that meet the MST can be identified. The algorithm halts when no novel F_j can be created. Thus, the ASR is created through improved ARM. After creating *ASR*, the next step involves extracting the sensitive data P^d. Thus, from *ASR*, the sensitive data P^d is obtained.

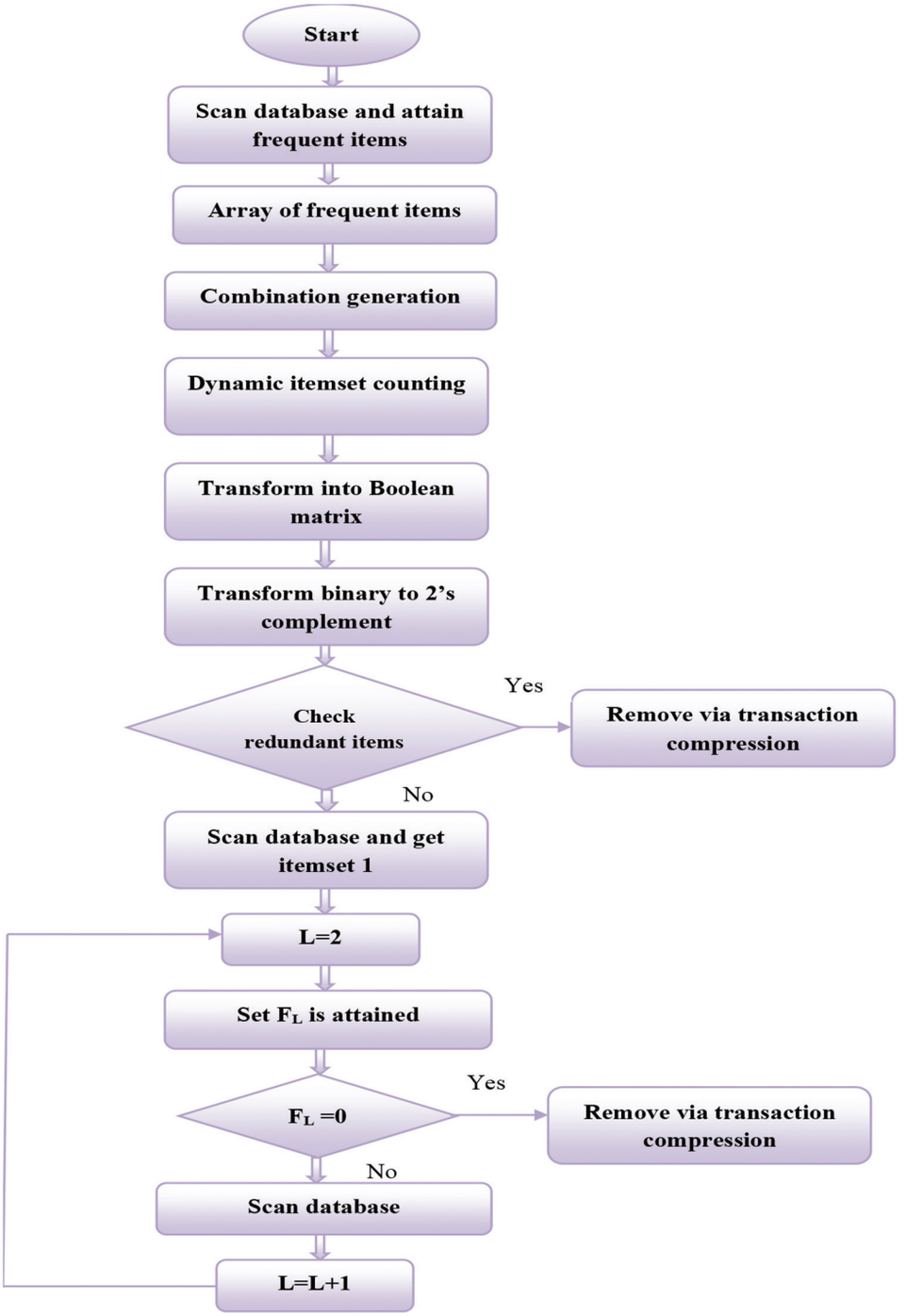

Figure 3. Flowchart for proposed improved association rule mining
Abbreviation: L: Length.

5. STI-TSA for optimal key generation

Following the extraction of sensitive data P^d, optimum keys are produced based on certain constraints. The goal of optimal key generation is to generate or choose keys that optimize utility while lowering the possibility of privacy violations. The STI-TSA technique is deployed for optimal key generation, taking into account HFR, MD, and IPR. The STI-TSA method aids in the identification of keys, ensuring that the optimal keys are strong and well-designed to satisfy both operational and security criteria.

Table 1. Example of minimum support threshold computations with items and their occurrences

Item	Occurrence
A	7
B	7
C	6
D	2
E	4
F	4

Table 2. Frequent items and occurrences

Items	Occurrence
A	7
B	7
C	6

Table 3. Sample dataset

Item 1	Item 2	Item 3	Item 4	Item 5
A	B	C		
A	C			
B	D	E		
A	C	F		
A	B	C	D	E
B	F			

Table 4. Dataset after eliminating the uncommon items

Item 1	Item 2	Item 3	Item 4	Item 5
A	B	C		
A	C			
B				
A	C			
A	B	C		
B				

Table 5. Generation of item combinations

Row 1: AB, AC, BC
Row 2: AC
Row 3: -
Row 4: AC
Row 5: AB, AC, BC
Row 6: -

5.1. Objective function

The STI-TSA is deployed to generate optimal keys for PP. This algorithm takes into account HFR, MD, and IPR. Consequently, the objective function is represented by Equation IV, where weight is denoted by *w*.

$$OF = \min\left(W_1 \times [1 - IPR] + W_2 \times HFR + W_3 \times MD\right) \quad \text{(IV)}$$

In Equation IV,

$$W_i = \frac{Constraints_i}{Sum\ of\ constraints_{(i)}} \quad \text{(V)}$$

HFR is the proportion of sensitive data P^d to the total count of P^d in d^s, as well-defined in Equation VI. In Equation VI, P^* specifies the sanitized data.

$$HFR = \frac{Count\ of\ sensitive\ data\ exposed\ in\ P^*}{Count\ of\ sensitive\ data} \quad \text{(VI)}$$

MD[38] offers specifics on the degree of modification happening among P^d and P^*, as shown in Equation VII.

$$\text{MD} = \text{Euclidean}\ [P^D, P^*] \quad \text{(VII)}$$

The IPR indicates the variance between the count of non-sensitive data and P^* to the total count of non-sensitive data in Equation VIII.

$$IPR = \frac{Non - sensitive\ data\ count - P^*}{Non - sensitive\ data\ count} \quad \text{(VIII)}$$

5.2. Solution encoding

During optimization, candidate keys are provided as input to the STI-TSA. During optimization, STI-TSA refines the keys continuously based on certain constraints that prioritize effective PP. The iterative procedure of STI-TSA strikes a balance, ensuring the candidate keys meet the objectives of preserving privacy in EHRs.

5.2.1. STI-TSA

Tuna search for their prey using two different foraging techniques. Initially, the population in the field of search space is generated arbitrarily for the TSA's optimization. Each tuna chooses one of the two foraging techniques to use. All TSA individuals were kept informed until the final requirement was fulfilled. The optimal solution and the corresponding fitness value were then returned. This section describes the precise model of the STI-TSA.

While the TSA offers better solutions, it is prone to converging to local optima instead of finding the global optimum. Moreover, excessive exploration can cause

the algorithm to miss the optimal solution, whereas too much exploitation may result in getting stuck in local minima. Therefore, to overcome these challenges, we included the concept of STO in our work.

The new algorithm, including the concepts of SBO[33] and TSA,[32] is termed STI-TSA. The hybrid TSA with SBO could attain faster convergence and create high-quality solutions, including diverse optimizing approaches. In addition, STI-TSA could balance both local and global searches.

(i) Initialization: TSA begins with the arbitrary generation of initial populations as shown in Equation IX, where, Z_l^{in} points out initial individuals, *LB* and *UB* point out lower and upper limits, *O* points out the tuna population, and *rnd* points out random values between 0 and 1

$$Z_l^{\text{in}} = rnd.\left(UB - LB\right) + LB,\ \ l = 1,2...O \tag{IX}$$

(ii) Spiral foraging: The entire school of fish forms a tight configuration by continuously changing its swimming direction to prevent predators from latching onto a victim. At that point, the tuna group forms a tight spiral shape to pursue the prey. Although many fish possess a sense of direction, when a small group of fish begins swimming in a certain direction, other fish in the vicinity often follow suit. The fish in the leading group share a common objective and initiate the hunt. Furthermore, all tuna communicate with each other. The mathematical formula for spiral foraging behavior is provided in Equation X.

$$Z_l^{T+1} = \begin{cases} \gamma_1.\left(Z_{best}^T + \delta.\left|Z_{best}^T - Z_l^T\right|\right) + \gamma_2.Z_l^T, & l = 1 \\ \gamma_1.\left(Z_{best}^T + \delta.\left|Z_{best}^T - Z_l^T\right|\right) + \gamma_2.Z_{l-1}^T & l = 2,3,...,O \end{cases} \tag{X}$$

The computation of γ_1, γ_2, δ, and *le* are shown in Equation XI to Equation XIV.

$$\gamma_1 = co + \left(1 - co\right).\frac{T}{T_{\max}} \tag{XI}$$

$$\gamma_2 = \left(1 - co\right) - \left(1 - co\right).\frac{T}{T_{\max}} \tag{XII}$$

$$\delta = w^{ble}.\cos\left(2\pi b\right) \tag{XIII}$$

$$le = w^{3\cos\left(\left(\left(T_{\max} + \frac{1}{T}\right) - 1\right)\pi\right)} \tag{XIV}$$

Here, l^{th} individual at $T + 1$ iteration is signified by Z_l^{T+1}, whereas Z_{best}^T symbolizes the current optimal individual, and γ_1 and γ_2 symbolize weighting coefficients. The extent to which tuna follows the optimal and prior individual is assessed by *co*, whereas T and $T_{\max}$ signify the iteration count and maximal iteration, and *b* signifies the random figure between 0 and 1.

Each tuna can more effectively utilize the search phase when swimming in a spiral pattern around the bait. This strategy allows the tuna to cover a larger area, enhancing TSA's potential to explore the search space on a global scale, as stated in Equation XV.

$$Z_l^{T+1} = \begin{cases} \gamma_1.\left(Z_{rnd}^T + \delta.\left|Z_{rnd}^T - Z_l^T\right|\right) + \gamma_2.Z_l^T, & l = 1 \\ \gamma_1.\left(Z_{rnd}^T + \delta.\left|Z_{rnd}^T - Z_l^T\right|\right) + \gamma_2.Z_{l-1}^T & l = 2,3,...,O \end{cases} \tag{XV}$$

The symbol Z_{rnd}^T represents an arbitrary reference point in the field of search space. The TSA changes the spiral foraging indicators from arbitrary to optimum ones as the iteration rises. It may be found numerically in Equation XVI.

$$Z_l^{T+1} = \begin{cases} \gamma_1.\left(Z_{rnd}^T + \delta.\left|Z_{rnd}^T - Z_l^T\right|\right) + \\ \gamma_2.Z_l^T,\ l = 1, \\ \gamma_1.\left(Z_{rnd}^T + \delta.\left|Z_{rnd}^T - Z_l^T\right|\right) + \\ \gamma_2.Z_{l-1}^T,\ l = 2,3,...,O, \\ \gamma_1.\left(Z_{best}^T + \delta.\left|Z_{best}^T - Z_l^T\right|\right) + \\ \gamma_2.Z_l^T,\ l = 1 \\ \gamma_1.\left(Z_{best}^T + \delta.\left|Z_{best}^T - Z_l^T\right|\right) + \\ \gamma_2.Z_{l-1}^T,\ l = 2,3,...,O \end{cases} \begin{array}{l} \\ \\ ,if\ rnd < \dfrac{T}{T_{\max}}, \\ \\ \\ \\ ,if\ rnd \geq \dfrac{T}{T_{\max}}, \\ \\ \end{array} \tag{XVI}$$

(iii) Proposed parabolic foraging: Here, tuna forms a parabolic shape using food as a point of reference. They also search their surroundings in search of nourishment. Two methods were used simultaneously, with the assumption that each had a 50% chance of being selected. Its numerical version is given in Equation XVII. *tf* is an arbitrary number with a value of either −1 or 1.

$$Z_l^{T+1} = \begin{cases} Z_{best}^T + rnd.\left(Z_{best}^T - Z_l^T\right) + \\ tf.\left(A\right)^2.\left(Z_{best}^T - Z_l^T\right), & if\ rnd < 0.5, \\ tf.\left(A\right)^2.Z_l^T, & if\ rnd \geq 0.5, \end{cases} \quad \text{(XVII)}$$

$$A = \left(1 - \frac{T}{T_{\max}}\right)^{\left(T/T_{\max}\right)} \quad \text{(XVIII)}$$

As per STI-TSA, Equation XVIII is converted, as shown in Equation XIX.

$$\begin{aligned} Z_l^{T+1} &= Z_{best}^T + rnd.\left(Z_{best}^T - Z_l^T\right) + tf.\left(A\right)^2.\left(Z_{best}^T - Z_l^T\right) \\ &+ Z_l^{T+1} = tf.\left(A\right)^2.Z_l^T \\ \hline 2Z_l^{T+1} &= Z_{best}^T + rnd.Z_{best}^T - rnd.Z_l^T + tf.\left(A\right)^2.Z_{best}^T \end{aligned} \quad \text{(XIX)}$$

Finally,

$$Z_l^{T+1} = \frac{Z_{best}^T + rnd.Z_{best}^T - rnd.Z_l^T + tf.\left(A\right)^2.Z_{best}^T}{2} \quad \text{(XX)}$$

Furthermore, the update from the modified STO is integrated with TSA to form a new update. The update from the modified STO is shown in Equation XXIII.

$$Z_{i,j}^{p1s2} = Z_{i,j} + R_{i,j}.\frac{\left(UB_j - LB\right)}{T},\ i = 1,2...N,\ j = 1,2...B \quad \text{(XXI)}$$

$$Z_{i,j}^{p1s2} = Z_{i,j} + \frac{R_{i,j}.UB_j}{T} - \frac{R_{i,j}.LB_j}{T} \quad \text{(XXII)}$$

$$Z_{i,j} = Z_{i,j}^{p1s2} - \frac{R_{i,j}.UB_j}{T} + \frac{R_{i,j}.LB_j}{T} \quad \text{(XXIII)}$$

On substituting Equation XXIII in Equation XX, we get Equation XXVIII.

$$Z_l^{T+1} = \frac{\begin{array}{l} Z_{best}^T + rnd.Z_{best}^T - rnd. \\ \left[Z_{i,j}^{p1s2} - \frac{R_{i,j}.UB_j}{T} + \frac{R_{i,j}.LB_j}{T}\right] + tf.\left(A\right)^2.Z_{best}^T \end{array}}{2} \quad \text{(XXIV)}$$

$$\begin{aligned} Z_{best}^T + rnd.Z_{best}^T + rnd.\frac{R_{i,j}.UB_j}{T} \\ Z_l^{T+1} - \frac{rnd\,Z_{i,j}^{p1s2}}{2} = \frac{-rnd.\frac{R_{i,j}.LB}{T} + tf.\left(A\right)^2.Z_{best}^T}{2} \end{aligned} \quad \text{(XXV)}$$

$$\begin{aligned} Z_{best}^T + rnd.Z_{best}^T + rnd.\frac{R_{i,j}.UB_j}{T} - \\ Z_l^{T+1}\left[1 + \frac{rnd}{2}\right] = \frac{rnd.\frac{R_{i,j}.LB_j}{T} + TF.\left(sf\right)^2.Z_{best}^T}{2} \end{aligned} \quad \text{(XXVI)}$$

$$Z_l^{T+1}\left[1 + \frac{rnd}{2}\right] = \left[\begin{array}{l} Z_{best}^T + Z_{best}^T\left(rnd + tf.\left(A\right)^2\right) + \\ \frac{rnd.\frac{R_{i,j}.UB_j}{T} - rnd.\frac{R_{i,j}.LB_j}{T}}{2} \end{array}\right] \quad \text{(XXVII)}$$

Finally,

$$Z_l^{T+1} = \frac{\left[\begin{array}{l} Z_{best}^T + Z_{best}^T\left(rnd + tf.\left(A\right)^2\right) + rnd.\frac{R_{i,j}.UB_j}{T} - \\ \frac{rnd.\frac{R_{i,j}.LB_j}{T}}{2} \end{array}\right]}{\left[1 + \frac{rnd}{2}\right]} \quad \text{(XXVIII)}$$

Here, Equation XXVIII replaces Equation XVI.

On hybridizing TSA with SBO, faster convergence could be attained and high-quality solutions could be created by including diverse optimizing approaches. In addition, STI-TSA could balance both local and global searches.

The pseudocode for STI-TSA optimization is shown in Algorithm 1.

Algorithm 1: Siberian Tiger Integrated Tuna Swarm algorithm

Initializing the population
Initializing$_{co}$ and probability I
While $T < Tmax$
  Compute fitness
  Update Z_{best}^{T}
  For every tuna
    $\gamma 1$, $\gamma 2$, and A are updated
    If rnd <I
    Position is updated through Equation IX
    Else if $rnd \geq$I
      If rnd <0.5
        If $\frac{T}{T_{\max}} < rnd$
          Position is updated through Equation XV
        else
          Position is updated through Equation X
      Else if $rnd \geq 0.5$
        Position is updated through proposed Equation XXVIII by integrating the update of STO
  End for
$T=T+1$
Return the best solution

From STI-TSA, the optimal key K^o is attained.

(iv) Sanitization process: The XOR operation among sensitive data P^d and the optimum key K^o yields the sanitized data as given in Equation XXIX. By successfully masking the original data, this bitwise operation improves security and privacy. From Equation XXIX, P^* implies the output sanitized data.

$$Sanitized\ data\left(P^*\right) = P^d \oplus K^o \quad \text{(XXIX)}$$

6. Blockchain-based sensitive data storage

(i) Block creation: Sanitized data are grouped into blocks. Each block may contain multiple encrypted records
(ii) Hashing: Each block is hashed to generate a unique digital fingerprint. The hash includes the block's data and the hash of the previous block, creating a chain of blocks
(iii) Block addition: The block is added to the blockchain after being verified by the network's consensus mechanism
(iv) Access control: The access control to access the sensitive data is given below:
  a. Public and private keys: Patients have private keys K^o (optimal key) that allow them to decrypt their health records. Health-care providers have their keys to access the data as well
  b. Permission management: Access to the data is controlled through a system of permissions. For instance, a patient's consent is required before a health-care provider can access or update their records. The process of restoring the original data is discussed below.

7. Data restoration

Reversing the steps taken throughout the privacy-preserving stage is the last step in the process of recovering the original data. Recovering sensitive data while protecting data privacy requires this procedure. The formula for obtaining the original data using the reverse procedure is given in Equation XXX.

$$P^d = P^* \oplus K^o \quad \text{(XXX)}$$

Using an optimal key generated from ASRs, the XOR operation is crucial in concealing sensitive data during data sanitization. The inverse XOR procedure needs to be used to recover the original sensitive data. Employing the inverse XOR, the sanitized data are broken down in this reverse process, guaranteeing an exact reconstruction of the original data. Similar to this, ASRs that recognize delicate patterns in the data are produced using the improved ARM algorithm. Reverse algorithms or processes capable of reversing the impact of these privacy-preserving approaches are used to return the original data from its sanitized version. This preserves the sensitive data while guaranteeing that initial medical data D_i may completely be retrieved for additional examination or use.

8. Results and discussion

8.1. Simulation procedure

The introduced approach for PP for EHR using BT was executed in Python. The simulation was run on a system equipped with an 11th Gen Intel(R) Core (TM) i3-1115G4 @ 3.00 GHz processor and 8.00 GB (7.74 GB usable) of RAM. The assessment was conducted using STI-TSA, comparing its performance against STO, TSA, Puffer Fish Optimization (PFO), SBO Algorithm (SBOA), Bat Algorithm (BA), EHO-OBL,[34] and BFL-PSO.[35] The

dataset used in this study is the Heart Disease dataset from the UCI Machine Learning Repository.[36]

This database contains 76 attributes, but previous experiments have focused on a subset of 14. The goal field refers to the presence of heart disease in the patient, with integer values ranging from 0 (no presence) to 4. The names and social security numbers of the patients were recently removed from the database and replaced with dummy values. One processed file containing the Cleveland database is available, while the remaining four unprocessed files are also included in this directory.

8.2. Analysis of IPR, HFR, and MD

Figure 4 shows the performance of IPR, HFR, and MD for proposed STI-TSA optimization over extant optimization schemes, such as STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO.[35] Regarding fitness, the IPR and HFR have to be higher for better performance, whereas MD has to be lower. From the graphs in Figure 4, it can be observed that the proposed STI-TSA-based optimization has fulfilled this statement. Particularly, the IPR is higher when data are at 30%. For datasets with 10% and 20%, the proposed STI-TSA-based optimization achieves a higher IPR compared to STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO.[35] When data are 10%, the proposed STI-TSA-based optimization attained a high IPR of 0.93%; with 20% data, the IPR reaches 0.94%; and with 30% data, the IPR attains 0.95%. In contrast, at 30% of data, extant optimization schemes, such as STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO[35] achieved lower IPR values of 0.89, 0.9, 0.87, 0.9, 0.87, 0.89, and 0.88, respectively.

The new STI-TSA algorithm, incorporating the concepts of SBO and TSA, could attain faster convergence and create high-quality solutions that

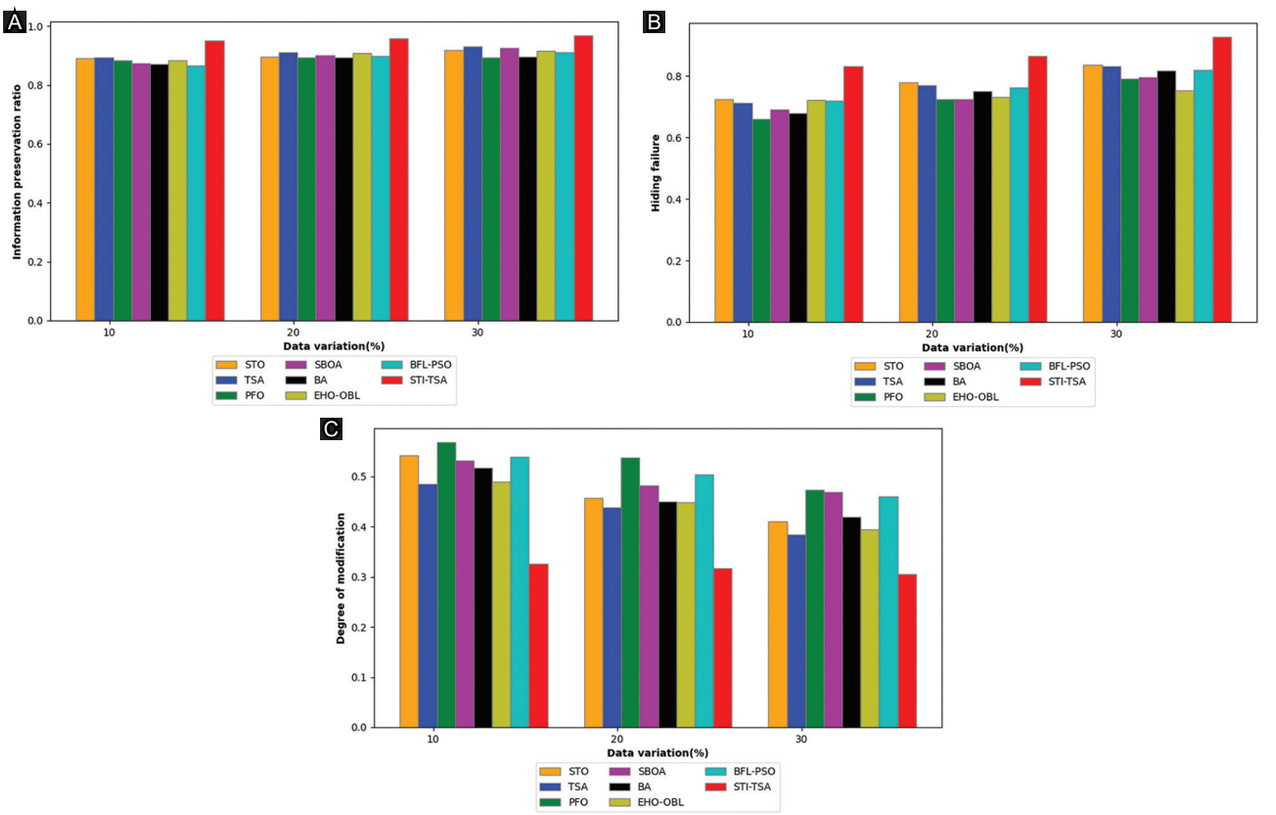

Figure 4. Performance of privacy preservation for electronic medical records using blockchain technology. Performance of the Siberian Tiger Integrated Tuna Swarm algorithm (STI-TSA) over extant optimization approached for (A) information preservation ratio, (B) hiding failure rate, and (C) modification degree.
Abbreviations: BA: Bat Algorithm; BFL-PSO: Bee-foraging learning particle swarm optimization; EHO-OBL: Elephant Herding Optimization with Opposition-based Learning; PFO: Puffer Fish Optimization; SBOA: Secretary Bird Optimization Algorithm; STO: Siberian Tiger Optimization; TSA: Tuna Swarm algorithm.

include diverse optimizing approaches. Similarly, in the case of HFR, the proposed STI-TSA-based optimization obtained a high value of 0.95 when the data were 30%. In contrast, lower HFR values were achieved when data were at 10% and 20%. However, for all data variations, the proposed STI-TSA-based optimization attained high HFR over STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO.[35]

As required, the MD is low for the proposed STI-TSA-based optimization over STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO.[35] A significantly low MD value (approximately 0.3) was obtained when data were at 30%, whereas extant optimization approaches obtained high MD values. Thus, with its balanced approach, STI-TSA delivers superior performance.

8.3. Ablation study

Table 6 presents the ablation study for validating the enhancement of the proposed STI-TSA with improved ARM, compared to both the version without ARM and the version with traditional ARM. After modifying the existing ARM, we achieved better performance using the improved ARM. In Table 6, the proposed STI-TSA with improved ARM shows a high IPR of 0.958626, whereas the versions without ARM and with traditional ARM show lower IPR. The improved ARM could mine the rules quicker with large datasets and create more meaningful and precise rules. The improved ARM could identify complicated and subtle associations in the data and manage data variations over time. This is evident from the HFR, where the proposed STI-TSA with the improved ARM reaches a value of 0.8645, compared to 0.792064 and 0.813284 for the versions without ARM and with traditional ARM, respectively. The MD metric using the proposed STI-TSA with improved ARM is lower (around 0.317), whereas the versions without ARM and with traditional ARM exhibit higher MD values.

8.4. Attack analysis

Table 7 presents an analysis of various attack types, namely, chosen ciphertext attack (CCA), chosen-plaintext attack (CPA), known ciphertext attack (KCA), and known-plaintext attack (KPA) with respect to key breaking time. CCA is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. CPA is an attack model for cryptanalysis that presumes that the attacker can obtain the cipher texts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme. KPA is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib) and its encrypted version (cipher text). KCA is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

A message tampering attack (MTA) entails the harmful alteration of information, whereas an eavesdropping attack (EDA) refers to the unauthorized real-time interception of private communication through modern hacking technologies. Attack analysis reflects the level of protection against these threats – lower values indicate that the attacker takes more time to decrypt the sanitized data. For all data variations, the proposed STI-TSA with improved ARM has attained lower values over extant STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO.[35] This shows that the hacker needs more time to decrypt the sanitized data.

Table 7 presents the results of CCA, where the proposed STI-TSA with improved ARM attained a lower value of 0.227 at 30% data, compared to relatively higher values for STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO,[35] which are 0.294249, 0.286082, 0.292351, 0.290481, 0.292558, 0.323516, and 0.304436, respectively. Moreover, the 30% data shows lower attack values compared to data variations of 10% and 20%. For KCA, the proposed STI-TSA with improved ARM achieved a value of 0.218, while for KPA, it obtained a value of 0.171256. In regards to CPA, the proposed STI-TSA with improved ARM attains a low value of 0.21335. Moreover, for MTA and EDA, the proposed STI-TSA with improved ARM achieved

Table 6. Ablation analysis using Siberian Tiger Integrated Tuna Swarm algorithm with improved association rule mining over conventional works

Metrics	Proposed without association rule mining	Proposed with conventional association rule mining	Siberian Tiger Integrated Tuna Swarm algorithm with improved association rule mining
Information preservation ratio	0.912531	0.928175	0.958626
Hiding failure rate	0.792064	0.813284	0.86452
Modification degree	0.427843	0.410396	0.317007

Table 7. Attack analysis on privacy preservation with blockchain technology

Type of attack	Data variation (%)	STO	TSA	PFO	SBOA	BA	EHO-OBL	BFL-PSO	STI-TSA
Chosen ciphertext attack	10	0.351921	0.339407	0.34287	0.365965	0.349648	0.37791	0.367569	0.253009
	20	0.339255	0.308546	0.302815	0.312861	0.305106	0.341916	0.324134	0.240593
	30	0.294249	0.286082	0.292351	0.290481	0.292558	0.323516	0.304436	0.227043
Chosen-plaintext attack	10	0.377369	0.311311	0.382294	0.329612	0.374634	0.367101	0.405775	0.257965
	20	0.357544	0.296104	0.373377	0.306939	0.326005	0.336375	0.38882	0.231773
	30	0.334005	0.285204	0.355613	0.293705	0.295356	0.298582	0.37005	0.213351
Known ciphertext attack	10	0.345052	0.32823	0.340936	0.356009	0.347683	0.362589	0.372112	0.257533
	20	0.322449	0.311838	0.333301	0.327906	0.331565	0.329808	0.340978	0.236284
	30	0.293598	0.28121	0.329029	0.298151	0.317375	0.304013	0.32031	0.218906
Known-plaintext attack	10	0.358404	0.349322	0.362844	0.399397	0.391895	0.351093	0.333991	0.214906
	20	0.333724	0.315239	0.350371	0.382028	0.373978	0.342707	0.30128	0.192158
	30	0.262814	0.256571	0.308598	0.316097	0.321592	0.269359	0.279833	0.171256
Message tampering attack	10	0.431751	0.404186	0.437191	0.395072	0.435468	0.445301	0.430577	0.30485
	20	0.386429	0.363971	0.403125	0.362718	0.472377	0.401626	0.397691	0.283366
	30	0.316525	0.305065	0.335472	0.309952	0.332473	0.342722	0.330549	0.269973
Eavesdropping attack	10	0.424193	0.344404	0.412145	0.436951	0.43424	0.4271	0.36815	0.307106
	20	0.358123	0.329038	0.358288	0.395517	0.365027	0.34271	0.339393	0.293574
	30	0.318197	0.302423	0.332521	0.348741	0.332513	0.310608	0.311976	0.272066

Abbreviations: BA: Bat Algorithm; BFL-PSO: Bee-foraging learning particle swarm optimization; EHO-OBL: Elephant Herding Optimization with Opposition-based Learning; PFO: Puffer Fish Optimization; SBOA: Secretary Bird Optimization Algorithm; STO: Siberian Tiger Optimization; TSA: Tuna Swarm algorithm.

values of approximately 0.269973 and 0.272066, respectively.

8.5. Data sanitization and restoration analysis

Restoration signifies the reconstructing or recovery of data and systems to their original state after loss or corruption. When combined, they provide system recovery, data integrity, and privacy protection. The sanitization analysis and restoration analysis are shown in Tables 8 and 9, respectively. For better PP of EHR, the sanitization values must be lowered to confirm slight alteration of sensitive data. In contrast, the values of restoration must be high to enable accurate retrieval of original data. This statement is well accomplished by the proposed STI-TSA with improved ARM. In Table 8, STI-TSA with improved ARM reveals a minimal sanitization value of 0.2617 for data at 30%. At the same time, STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO[35] attain high sanitization values of 0.352917, 0.33179, 0.344319, 0.343102, 0.347302, 0.397624, and 0.368462, respectively. In the case of restoration, the proposed STI-TSA with improved ARM obtains a high value of 0.953422, while extant methods show lower restoration values.

Table 8. Data sanitization analysis on privacy preservation of electronic health records with blockchain technology

Methods	10%	20%	30%
STO	0.389357	0.389299	0.352917
TSA	0.423491	0.380429	0.33179
PFO	0.424748	0.400766	0.344319
SBOA	0.394453	0.372241	0.343102
BA	0.393901	0.363528	0.347302
EHO-OBL	0.428647	0.410471	0.397624
BFL-PSO	0.409735	0.39719	0.368462
STI-TSA	0.306117	0.287711	0.261784

Abbreviations: BA: Bat Algorithm; BFL-PSO: Bee-foraging learning particle swarm optimization; EHO-OBL: Elephant Herding Optimization with Opposition-based Learning; PFO: Puffer Fish Optimization; SBOA: Secretary Bird Optimization Algorithm; STO: Siberian Tiger Optimization; TSA: Tuna Swarm algorithm.

The low sanitization values confirm that the proposed STI-TSA with improved ARM incurs slight alteration of sensitive data over others. The high restoration values confirm the accurate retrieval of original data using the STI-TSA with improved ARM over extant ones.

Table 9. Data restoration analysis on privacy preservation for electronic health records with blockchain technology

Methods	10%	20%	30%
STO	0.850778	0.870158	0.892701
TSA	0.860621	0.881882	0.904179
PFO	0.834467	0.864743	0.876605
SBOA	0.822115	0.835485	0.862898
BA	0.814612	0.823373	0.847861
EHO-OBL	0.809184	0.824774	0.86858
BFL-PSO	0.826664	0.82739	0.886539
STI-TSA	0.933553	0.945149	0.953422

Abbreviations: BA: Bat Algorithm; BFL-PSO: Bee-foraging learning particle swarm optimization; EHO-OBL: Elephant Herding Optimization with Opposition-based Learning; PFO: Puffer Fish Optimization; SBOA: Secretary Bird Optimization Algorithm; STO: Siberian Tiger Optimization; TSA: Tuna Swarm algorithm.

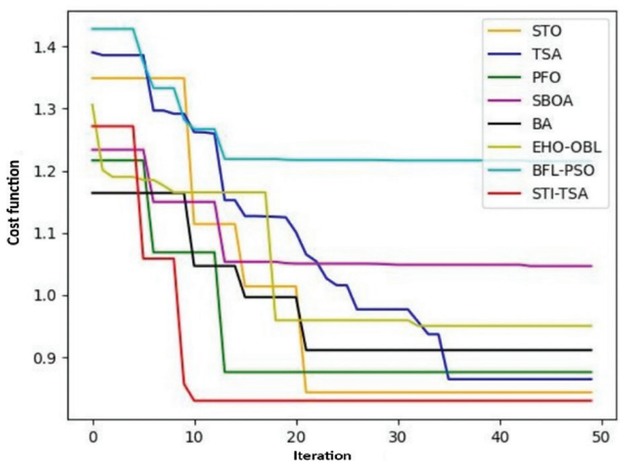

Figure 5. Convergence study of privacy preservation for electronic health records using blockchain technology. Abbreviations: BA: Bat Algorithm; BFL-PSO: Bee-foraging learning particle swarm optimization; EHO-OBL: Elephant Herding Optimization with Opposition-based Learning; PFO: Puffer Fish Optimization; SBOA: Secretary Bird Optimization Algorithm; STO: Siberian Tiger Optimization; TSA: Tuna Swarm algorithm.

8.6. Convergence analysis

Figure 5 shows the cost analysis using the proposed STI-TSA with an improved ARM over STO, TSA, PFO, SBOA, BA, EHO-OBL,[34] and BFL-PSO.[35] To ensure better PP, the cost values should be low with fast convergence. This is well accomplished using the proposed STI-TSA with an improved ARM approach. At initial iterations, the costs are high for all algorithms. However, with increasing iterations, the costs are reduced. Among all, the proposed STI-TSA with improved ARM shows lower cost values and has a faster convergence rate compared to other algorithms. Thus, the STI-TSA model could attain faster convergence and create high-quality solutions by including diverse optimizing approaches.

9. Conclusion

This work presented a novel PP approach for EHR utilizing BT. The method used an organized procedure that included data sanitization and restoration. First, improved ARM was used to detect sensitive information. The STI-TSA then finds the best key to improve data security. Sensitive information was safeguarded by applying an XOR operation among the sensitive data and the optimum key to sanitize the data. Next, blockchain storage was used to store the sanitized data. When necessary, the restoration procedure undoes the XOR operation to retrieve the original sensitive data. In the end, the reverse procedure of improved ARM was used to recover the original health data. From the analysis, when data were 10%, the proposed STI-TSA-based optimization attained a high IPR of 0.93%. In comparison, IPR of 0.94% and 0.95% were achieved when data were at 20% and 30%, respectively. At 30% of data, extant optimization schemes, such as STO, TSA, PFO, SBOA, BA, EHO-OBL, and BFL-PSO, attained low IPR of 0.89, 0.9, 0.87, 0.9, 0.87, 0.89, and 0.88, respectively. In the future, DL approaches can be integrated to improve the privacy of EHR data.

Acknowledgments

None.

Funding

None.

Conflict of interest

The authors declare no conflicts of interest.

Author contributions

Conceptualization: Varsha Mhaske
Investigation: Varsha Mhaske
Methodology: P. M. Ashok Kumar
Writing – original draft: Varsha Mhaske
Writing – review & editing: Varsha Mhaske

Availability of data

The data produced and analyzed in this study are available upon reasonable request from the corresponding author.

References

1. Zhao J, Wang W, Wang D, Wang X, Mu X. PMHE: A wearable medical sensor assisted framework for health care based on blockchain and privacy computing. *J Cloud Comput*. 2022;11:96. doi: 10.1186/s13677-022-00373-8
2. Jayaram R, Prabakaran S. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egypt Inform J*. 2021;22(4):401-410. doi: 10.1016/j.eij.2020.12.003
3. El-Samad W, Atieh M, Adda M. Transforming health insurance claims adjudication with blockchain-based solutions. *Proced Comput Sci*. 2023;224:147-154. doi: 10.1016/j.procs.2023.09.022
4. Wang G, Nurcahyo A. Designing personalized integrated healthcare monitoring system through blockchain and IoT. *Proced Comput Sci*. 2023;25:223-232. doi: 10.1016/j.procs.2023.10.520
5. Chondrogiannis E, Andronikou V, Karanastasis E, Litke A, Varvarigou T. Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain Res Appl*. 2022;2:100049. doi: 10.1016/j.bcra.2021.100049
6. Uppal S, Kansekar B, Mini S, Tosh D. HealthDote: A blockchain-based model for continuous health monitoring using interplanetary file system. *Healthc Anal*. 2023;3:100175. doi: 10.1016/j.health.2023.100175
7. Barbaria S, Mahjoubi H, Boussi rahmouni H. A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case. *Proced Comput Sci*. 2023;219:1436-1443. doi: 10.1016/j.procs.2023.01.433
8. Mubarakali A, Bose SC, Srinivasan K, Elsir A, Elsier O. Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *J Ambient Intell Humaniz Comput*. 2019;15:59. doi: 10.1007/s12652-019-01420-0
9. Omar AA, Bhuiyan MZA, Basu A, Kiyomoto S, Rahman MS. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gener Comput Syst*. 2019;95:511-521. doi: 10.1016/j.future.2018.12.044
10. Huang H, Zhu P, Xiao F, Sun X, Huang Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Comput Secur*. 2020;99:102010. doi: 10.1016/j.cose.2020.102010
11. Kuo TT, Kim J, Gabriel RA. Privacy-preserving model learning on a blockchain network-of-networks. *J Am Med Inform Assoc*. 2020;27(3):343-354. doi: 10.1093/jamia/ocz214
12. Amponsah AA, Adekoya AF, Weyori BA. Improving the financial security of national health insurance using cloud-based blockchain technology application. *Int J Inform Manag Data Insights*. 2022;2(1):100081. doi: 10.1016/j.jjimei.2022.100081
13. Lodha L, Baghela VS, Bhatt R. A blockchain-based secured system using the Internet of medical things (IOMT) network for e-healthcare monitoring. *Meas Sens*. 2023;30:100904.
14. Maher M, Khan I, Prikshat V. Monetisation of digital health data through a GDPR-compliant and blockchain enabled digital health data marketplace: A proposal to enhance patient's engagement with health data repositories. *Int J Inf Manag Data Insights*. 2023;3:100159. doi: 10.1016/j.jjimei.2023.100159
15. Hennebelle A, Ismail L, Materwal H, Kaabi JA, Ranjan P, Janardhanan R. Secure and privacy-preserving automated machine learning operations into end-to-end integrated IoT-edge-artificial intelligence-blockchain monitoring system for diabetes mellitus prediction. *Comput Struct Biotechnol J*. 2014;23:212-233. doi: 10.1016/j.csbj.2023.11.038
16. Mohammed MA, Lakhan A, Zebari DA, *et al*. Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Eng Appl Artif Intell*. 2024;129:107612. doi: 10.1016/j.engappai.2023.107612
17. Azbeg K, Ouchetto Q, Andaloussi SJ. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egypt Inform J*. 2022;23(2):329-343. doi: 10.1016/j.eij.2022.02.004
18. Jena SK, Kumar B, Mohanty B, Singhal A, Barik RC. An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. *Decis Anal J*. 2024;10:100411. doi: 10.1016/j.dajour.2024.100411
19. Varela-Vaca AJ, Gasca RM, Iglesias D, Gónzalez-Gutiérrez JM. Automated trusted collaborative processes through blockchain & IoT integration: The fraud detection case. *Internet Things*. 2024;25:101106.

doi: 10.1016/j.iot.2024.101106
20. Sutradhar S, Majumder S, Bose R, Mondal H, Bhattacharyya D. A blockchain privacy-conserving framework for secure medical data transmission in the internet of medical things. *Decis Anal J*. 2024;10:100419. doi: 10.1016/j.dajour.2024.100419
21. Taloba AI, Elhadad A, Park C, *et al*. A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alex Eng J*. 2022;65:263-274.
22. Zheng H, You K, Hu G. A novel insurance claim blockchain scheme based on zero-knowledge proof technology. *Comput Commun*. 2022;195:207-216. doi: 10.1016/j.comcom.2022.08.007
23. Antwi M, Adnane A, Kerrache CA, *et al*. The case of HyperLedger fabric as a blockchain solution for healthcare applications. *Blockchain Res Appl*. 2021;2:100012. doi: 10.1016/j.bcra.2021.100012
24. Xie L, Han T, Zhou H, Zhang ZR, Han B, Tang A. Tuna swarm optimization: A novel swarm-based metaheuristic algorithm for global optimization. *Comput Intell Neurosci*. 2021;2021:9210050. doi: 10.1155/2021/9210050
25. Trojovský P, Dehghani M, Hanuš P. Siberian tiger optimization: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems. *IEEE Access*. 2022;10:132396-132431. doi: 10.1109/ACCESS.2022.3229964
26. Verma G. Blockchain-based privacy preservation framework for healthcare data in cloud environment. *J Exp Theor Artif Intell*. 2022;36:147-160. doi: 10.3390/electronics13193832
27. Irshad RR, Sohail S, Hussain S, *et al*. A Multi-objective bee foraging learning-based particle swarm optimization algorithm for enhancing the security of healthcare data in cloud system. *IEEE Access*. 2023;11:113410-113421. doi: 10.1109/ACCESS.2023.3265954
28. Available from: https://archive.ics.uci.edu/dataset/45/heart+disease [Last accessed on 25 Jul 2024].
29. Zhao Z, Jian Z, Gaba GS, Alroobaea R, Masud M, Rubaiee S. An improved association rule mining algorithm for large data. *J Intell Syst*. 2021;30(1):750-762. doi: 10.1515/jisys-2020-0121
30. Ahamad D, Hameed SA, Akhtar M. A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. *J King Saud Univ Comput Inform Sci*. 2022;34(6):2343-2358. doi: 10.1016/j.jksuci.2020.10.015
31. Baffour KA, Osei-Bonsu C, Adekoya AF. A modified apriori algorithm for fast and accurate generation of frequent item sets. *Int J Sci Technol Res*. 2017;6(8):169-173.
32. Saraswat B, Kumar A, Sharma S, Anand KB. Health chain-block chain based electronic healthcare record system with access and permission management. *Meas Sens*. 2023;30:100903. doi: 10.1016/j.measen.2023.100903
33. Alsuqaih HN, Hamdan W, Elmessiry H, Abulkasim H. An efficient privacy-preserving control mechanism based on blockchain for E-health applications. *Alex Eng J*. 2023;73:159-172. doi: 10.1016/j.aej.2023.04.037
34. Wang Y. Data structure and privacy protection analysis in big data environment based on blockchain technology. *Int J Intell Netw*. 2024;5:120-132. doi: 10.1016/j.ijin.2024.02.005
35. Kumar M, Raj H, Chaurasia N, Gill SS. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet Things Cyber Phys Syst*. 2023;3:309-322.
36. Sutradhar S, Karforma S, Bose R, Roy S, Djebali S, Bhattacharyya D. Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A block-chain-based approach for security and scalability for healthcare industry. *Internet Things Cyber-Phys Syst*. 2024;4:49-67. doi: 10.1016/j.iotcps.2023.07.004
37. Hemalatha T, Bhuvaneswari A, Poornima N, *et al*. Secure and private data sharing in CPS e-health systems based on CB-SMO techniques. *Meas Sens*. 2023;27:100787. doi: 10.1016/j.measen.2023.100787
38. Yi H. Improving cloud storage and privacy security for digital twin based medical records. *J Cloud Comp*. 2023;12:151. doi: 10.1186/s13677-023-00523-6
39. Kumar P, Kumar R, Gupta GP, Tripathi R, Jolfaei A, Najmul Islam AKM. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *J Parallel Distrib Comput*. 2023;172:69-83. doi: 10.1016/j.jpdc.2022.10.002
40. Solanas A, Patsakis C, Conti M, *et al*. Smart health: A context-aware health paradigm within smart cities. *IEEE Commun Mag.* 2014;52(8):74-81. doi: 10.1109/MCOM.2014.6871673
41. Prasanna KL, Rao YN. Context-Aware Approaches in Iot-Based Healthcare Systems Using Deep Learning Techniques: A Study. In: *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India; 2024. p. 567-570. doi: 10.1109/ICAAIC60222.2024.10575875
42. Aazad SK, Saini T, Ajad A, Chaudhary K, Elsayed K. Deciphering blood cells - method for blood cell analysis using microscopic images. *J Modern Technol*. 2024;1(1):9-18.
43. Kalnoor G, Dasari KS, Suma S, Waddenkery N, Pragathi B. Enhanced brain tumor detection from MRI scans using frequency domain features and hybrid machine learning models. *J Mod Technol*. 2025;1(2):141-149. doi: 10.1007/s00521-025-11031-w