Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 6802967, 11 pages
https://doi.org/10.1155/2022/6802967

Research Article

An Internet of Things (IoT)-Based Optimization to Enhance Security in Healthcare Applications

Ali M. Al Shahrani,[1] Ali Rizwan,[2] Manuel Sánchez-Chero,[3] Carmen Elvira Rosas-Prado,[4] Elmer Bagner Salazar,[5] and Nancy Awadallah Awad[6]

[1]*Faculty of Computer Studies, Arab Open University, Saudi Arabia*
[2]*Department of Industrial Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[3]*Universidad Nacional de Frontera, Sullana, Peru*
[4]*Universidad Alas Peruanas, Lima, Peru*
[5]*Universidad César Vallejo, Piura, Peru*
[6]*Department of Computer and Information Systems, Sadat Academy for Management Sciences, Cairo 11742, Egypt*

Correspondence should be addressed to Ali Rizwan; arkhan71@kau.edu.sa

Received 27 June 2022; Revised 29 July 2022; Accepted 5 August 2022; Published 30 September 2022

Academic Editor: Amandeep Kaur

The Internet of Things (IoT) is a network that connects a large number of items. Each thing uses sensors to create and gather data from its surroundings and then sends to other objects or a central database through a channel. Keeping and transforming this created data is one of the most difficult tasks in IoT today, and it is one of the top worries of all enterprises that deploy IoT technology. Sensing equipment together with communication, storing, and display devices get benefit from technological advancements in the healthcare sector. Moreover, medical parameters and postoperative days require close observation. Therefore, the most cutting-edge approach to healthcare communication is adopted, which makes use of the Internet of Things (IoT). We can use the Internet of Things to speed changes in the healthcare environment, such as enhancing patient involvement and outcomes and shifting healthcare from reactive to proactive accessibility. Nonetheless, the growth of IoT exposes healthcare practitioners and their patients to new vulnerabilities, risks, and security concerns. However, there is currently a scarcity of research on how to improve IoT security in healthcare. Existing studies tend to concentrate only on the installation of IoT peripherals in a healthcare setting and to include a secure application solution. Because healthcare data and information are extremely sensitive, it is critical to have a secure health IoT application in place. As the IoT gets more widely used in healthcare, there will inevitably be more instances of sensitive patient information being made public. This paper proposes an optimized hashing algorithm with digital certificates to enhance the security. Initially, the health data are collected and preprocessed using normalization. The data are then stored in the IoT device. Here, the digital certificates are used for authentication purpose. The proposed discrete decision tree hashing algorithm (DDTHA) with ant colony optimization (ACO) hashes the unsigned digital certificates. The blowfish algorithm is used for encryption, and the signed digital certificate is obtained which is used for authentication purpose. The performance of the proposed system is evaluated and compared with conventional methodologies to prove the efficiency of the system.

1. Introduction

Today, IoT is an interesting topic in communication networks because it has the power to link the Internet with nearly endless kinds and numbers of sensors and devices and has a direct influence on our daily lives. There have been a lot of studies done in this area on the integration of various applications with the Internet of Things (IoT) [1, 2]. Although this technology has lately been intensively considered in the field of mobile healthcare, it has not yet been broadly implemented. To put it another way, m-health, or mobile healthcare, is the use of mobile devices to gather and store real-time health data from people and then make it available to healthcare practitioners, hospitals, and

insurance companies over the Internet. In recent years, m-health has been a major emphasis in the healthcare industry, with the most prominent example being portable diabetes management systems [3]. Figure 1 depicts the general framework of the IoT healthcare system.

Data gathered by sensing devices are the cornerstone of IoT systems and applications; nevertheless, the fact is that such data obtained by the sensor network are unreliable. To execute a wide range of difficult duties, sensor nodes are randomly placed in harsh environments and deserted regions, and they play a vital role in many different industries such as surveillance systems and smart cities, health monitoring, and intrusion detection. The underlying sensor network is more susceptible to assaults because of its complicated surroundings. There are many forms of assaults that may occur on network systems and resources; therefore, it is important to keep them safe. Attacks on WSNs may be classified as either internal or external, depending on where they originate. Existing research shows that assaults on the IoT network from the inside are significantly more damaging than attacks from the outside. To make matters worse, the security techniques for encrypted identification as well as routing protocols are efficient against external assaults but ineffective against internal ones. If a network has any network users, a quick and easy way to deal with them is to use trust assessment. Security on the other hand is a vital building block of modern systems [4]. Every once in a while, security mechanisms for authentication compel both classical and comment occurrences to be rigorously scrutinized, and they also call for cutting-edge security solutions for IoT devices with limited resources and performance to continue using IoT-based services in the real universe. Access control techniques that are computationally safe are thus an absolute need with the ever-computational craze. As a result, hash-based signature (HBS) schemes are a strong contender, as they provide security assurances based on reasonable hash features and are now the subject of cutting-edge certification activities [5]. Figure 2 depicts wearable healthcare devices.

The memory controller, on the other hand, oversees the network and ensures that only a single sensor node is ever in use. Carrier sensing may then be used by the master to minimize collisions with other networks running in the same frequency range as the master. Using the controller prevents problems. Either the memory controller selects the network devices as needed for information, or the sensor networks contact the controller for authorization to send data. A sensor network must also continuously listen for the next signal when it loses sync with the network master. Because of its greater power source, the master can send more power and serve as a portal to the surrounding world [6]. Healthcare services management has recently been regarded as an information-driven subject. Healthcare services management can only be improved via the use of information systems [7]. Despite ongoing breakthroughs in this field, the existing healthcare system faces several difficulties. There are technological advances like haze and the IoT capable of providing new services to the patients and adapting individuals from conventional healthcare control techniques to fresh technology processes due to growing life

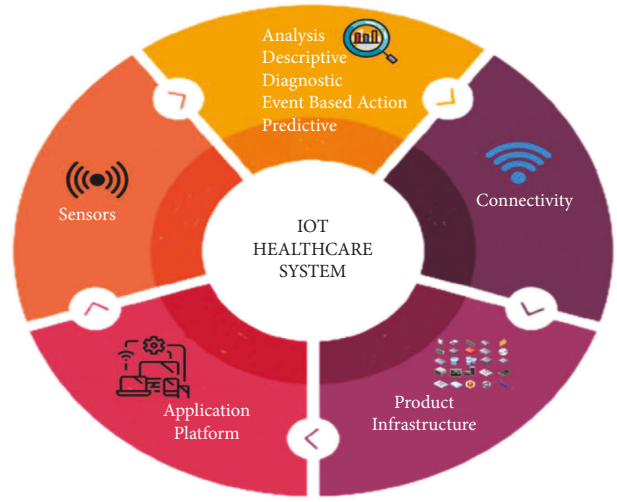

Figure 1: General framework of IoT healthcare system.

Figure 2: Wearable healthcare devices.

span, aging process citizens, and irreversible rapid population difficulties. There is possible cooperation between staff and service users (or those seeking support to improve overall comfort and wellbeing) at several levels in the administration of healthcare services. Lack of frequent and continuous usage has often resulted in the failure of innovative healthcare systems based on unique concepts like the Internet of Things [7].

1.1. Contribution of the Paper. The paper's main contribution is the security enhancement model in IoT using an optimized hashing algorithm with digital certificates for healthcare applications.

(i) To eliminate the unrelated or duplicated data from the raw datasets, the normalization approach is used.

(ii) The proposed DDTHA is used to boost the security of data, and ACO is also used to optimize the DDTHA's performance.

(iii) To convert the data into encoded data, the blowfish algorithm is used.

2. Literature Review

In this study, we provide a system for employing a secure IoT network to store, exchange, and transmit healthcare data. Here, we provide a summary of recent studies that are pertinent to our strategy and implementation. Share creation techniques and secret sharing methodology combined with improvement models are widely applied approaches to address several issues like impact of security and effectiveness of the plan. The shortcomings caused by the length and form of the secret target key have been expressly addressed by these improvement models. As mentioned in the study's major findings, distinct enticing ideal outcomes with changes based on the secret target key's varying lengths were shown. The study went further in addressing the drawbacks of the counting-based secret sharing generating techniques that were first developed [8]. The author [9] suggested using a unique algorithm to increase picture transmission security. Here, every input picture is resized, transformed into an audio file, and then delivered as an audio recording rather than being directly encrypted. The wav input is once more shrunk at the recipient's end to recover the output picture. It is far more challenging to identify any data contained in the audio because the data are in the form of audio. Information may be altered, data can be introduced that are not verified and are fake, etc., through intrusion. Using smart machines and blockchain technology, a contract is created to prevent these sorts of assaults from occurring. Several AI-based intelligent agents and blockchain are used throughout this suggested architecture. Adding biometric-based solutions for increased security may be a future improvement to this work. Again for purpose of identifying weaknesses in current security and privacy-preservation methods of EHR sets of data and developing a fresh approach for improving them, this study is being conducted [10]. Electronic health records, which store medical data electronically, have taken the role of older paper-based methods. The electronic health information system's susceptibility to attack vectors that adversely impact the security and privacy of medical information is one of the most crucial elements. We will discuss various security models and data privacy with e-health information in this essay. E-healthcare networks are often threatened by unauthorized availability of electronic devices, manipulation of data, denial-of-service assaults, and phishing. It is critical to developing a position access control because of the wide range of people obtaining this critical information from electronic health systems [11]. This research [12] examines how changing centralized databases to corner ones might reduce data manipulation. Cloud, fog, blockchain, and IoMT are all parts of the system. An IoMT was self-contained. The network standard method was also tested with public cloud resources. Several research initiatives use this encryption for its privacy benefits. Building a privacy-preservation mechanism to protect classified data transfers is difficult. Data transfer via an IoT network must be secure and maintain data integrity. It is tricky. Adaptive IoT security makes it difficult to distinguish between routine and attack events. The author [13] recommended using blockchain and public key infrastructure to limit patient access to electronic medical information. Information communication is hindered by an incompatible provider and hospital systems. Since the focus here is on the preservation of privacy in smart healthcare, this article has focused on the topic of electronic prescription transmission privacy assurances (ETP). Another flaw in the healthcare industry's strategy is there is no way to provide individual users' rights well beyond those granted to the group [14]. To sustain patients' credibility and confidence in digital healthcare, a major scientific improvement is needed. This paper examines the e-health cloud's cryptographic and noncryptographic security techniques to safeguard privacy components and their limitations in the growing digital world. ABE's downside is requiring data owners to utilize an authorized user's public key for encryption. KP-ABE has limited scalability, and the data owners cannot pick who decodes the encrypted data since they must trust the key issuer [15]. For the sake of this study [16], they enhanced FL with a new, more lightweight security and privacy mechanism. As part of the federation training, they target devices powered by IoHT that required a privacy guarantee for privately owned health information. Each node in the federation employed DP to prevent data leaking. It is still impossible to have fully decentralized FL since no federation nodes have training capability, there are not enough good trained data, and training data must be traced back to their source. The goal of this study [17] is both COVID-19 and non-COVID-19 blockchain applications and services. Medline, SpringerLink, IEEE Xplore, ScienceDirect, arXiv, and Google Scholar were searched till July 29, 2021. Prototypes of clinical and technical designs were featured. Distributed databases are a well-established platform in healthcare organizations. However, systems have major disadvantages, including not being able to exchange data among peers, being vulnerable to outside threats (such as hacking), and not having an unchangeable data model. The healthcare system can sustain the trade-off between security and cost for prompt sickness diagnosis since security and cost problems are handled in this research. To prevent the compromising of private medical data on open networks, Schnorr signature encryption utilizing HECC was developed. When employed for accurate health diagnosis, sensor nodes that communicate data to the medicine server (MS) via the base station (BS) provide privacy and security risks to users [18]. The security and privacy of IoT in healthcare and issues with developing security standards, including security and privacy alternatives, are all covered in this article [19]. Homomorphic encryption allows computation on encrypted data. Due to IoT devices' limited processing capacity, low battery, and other restrictions, smart healthcare systems' security architecture is disregarded, resulting in countless security breaches. The author [20] reviewed EHS security considerations. EHS data protection is a hot topic. Various security measures have been developed for preventing threats and assaults. Due to EHS's sensitivity and openness, the proposed solutions do not ensure total security [21]. They

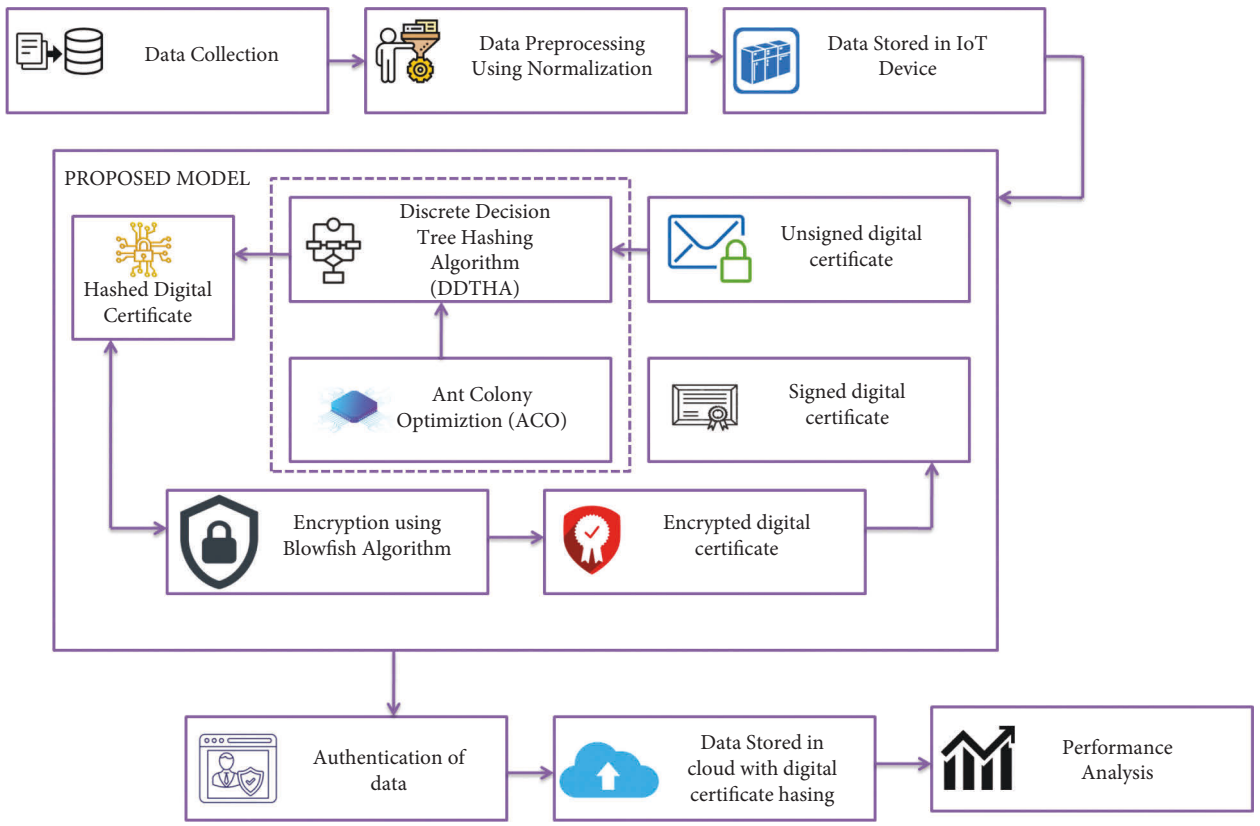

Figure 3: Proposed methodology of this research.

explored EHS security in this article. The most study focuses on protecting EHS data. Several security solutions have been offered for various threats and assaults. Due to EHS's sensitivity and openness, the provided methods are insufficient for total security. This paper [22] presents a cloud computing overview and reviews recent security concerns and solutions. Encrypting data in the cloud offer protected data access. They also faced certain cloud security engineering problems. Identifying these issues is the first step in addressing them; subsequent research must propose more practical answers. Due to solution protocol intricacies, they could not explain. To let others address and work on the concerns, they omitted certain solution specifics and procedures.

3. Proposed Methodology

IoT data management is one of the most challenging jobs in IoT today, and it is a major concern for all businesses that use IoT technology. This study suggests a digital certificate-enabled, optimized hashing technique to increase security. The health information is first gathered and normalized as part of the preprocessing. Digital certificates are used in this situation for authentication. Digital certificates that have not been signed are hashed using the proposed discrete decision tree hashing algorithm (DDTHA) with ant colony optimization (ACO). A signed digital certificate is acquired, and the blowfish technique is used to encrypt data for authentication. Figure 3 depicts the proposed methodology of this research.

Two datasets [23] on cardiovascular disease from Cleveland and Hungary were used to evaluate the proposed methodology. Those sets of data originate from the "University of California, Irvine (UCI)." There are 303 cases all in the original Cleveland database. There are a total of 294 cases in the Hungarian database.

3.1. Data Preprocessing Using Normalization. Typically, healthcare databases are made up of a range of heterogeneous data sources, and the data extracted from them are different, partial, and redundant, all of which have a significant impact on the final mining outcome. As a result, healthcare data must be preprocessed to guarantee that it is accurate, full, and consistent, as well as has privacy protection. Data normalization is a preprocessing procedure that scales or changes data to ensure an equitable contribution. Normalization enables us to construct a unique range from an existing one. It can anticipate or foresee advantages. Normalization adjusts raw data, so each characteristic contributes consistently. It solves dominant features and outliers, two fundamental machine learning data issues. Many methods for normalizing raw (un-normalized) data within a specified range have been devised. This research normalizes. These techniques are categorized by how they normalize raw data's statistical properties. It retains information relationships. It is a basic approach for fitting information inside predefined bounds.

As per this normalization method,

$$A' = \left(\frac{A - \min \text{value of } A}{\max \text{value of } A - \min \text{value of } A}\right) * (B - C) + C. \quad (1)$$

A represents real data, while D represents mapped data.

Parameter normalization uses mean and standard deviation to normalize unstructured data. (2) shows how to normalize unstructured data using the z-score variable:

$$f_i' = \frac{f_i - \overline{Y}}{\text{std}(Y)}, \quad (2)$$

where f_i' illustrates normalized values and f_i illustrates rate of the row Y of the *ith* column

$$\text{std}(Y) = \sqrt{\frac{1}{(m-1)} \sum_{i=1}^{m} (f_i - \overline{Y})^2}, \quad (3)$$

$$\overline{Y} = \frac{1}{m} \sum_{i=1}^{m} f_i \text{ or mean value.}$$

This method may be used to normalize each row above. Imagine a row where every value is the same, the standard deviation is 0, and every value is 0. Normalization indicates 0-1 values. Decimal scaling ranges from −1 to 1. This strategy

$$f_i = \frac{f}{10^q}. \quad (4)$$

Here, f_i represents the scaled values, f denotes the range of values, and q illustrates the smallest integer $\text{Max}(|f_i|) < 1$.

The data that have been preprocessed are subsequently saved to an IoT device. Then, the stored data are subsequently transmitted to a procedure called hashing, which is used for authentication purposes.

3.2. Discrete Decision Tree Hashing Algorithm (DDTHA). A discrete decision tree hashing algorithm is used to hash the unsigned digital certificate. The following is a definition of DH's objective function:

$$\min_{V,C,E} \|V - JE\| C2 + \lambda \|E\|_C^2 + b\|V - C(I)\|_C^2 d.p.V \int \{-1, 1\}^{m \times h}. \quad (5)$$

There are two ways to look at this: DH looks at the relationship between the two variables and the relationship between the two variables and the other. To speed up the procedure, we believe that regressing J into V is equivalent to regressing J into V. As long as there is no third term in DH, binary codes for each class will be unique. There are two types of binary code differences: one is across classes, and the other is between all samples.

There are three unknown variables in the mixed binary integer program of the problem. To get around this, we are going to repeatedly solve the issue using alternating optimization. The optimization of SDH in that each iteration alternately updates E, T, and V. We have got all the information right here.

S-step

$$T = \left(\phi(I)^P \phi(I)\right)^{-1} \phi(I)^P V. \quad (6)$$

Q-step may be rewritten as

$$\begin{aligned} &\min_e pq\left((JE - V)^P (JE - V) + \lambda pq\left(E^P E\right)\right) \\ &\quad = \min_e pq\left(E^P \left(J^P J + \lambda X\right) E\right) - 2pq\left(E^P J^P V\right). \end{aligned} \quad (7)$$

E can be solved using a closed-form solution if the derivative concerning E is set to zero:

$$E = \left(J^P J + \lambda X\right)^{-1} J^P V. \quad (8)$$

T-step: let us rework the story when S and E are repaired

$$\begin{aligned} &\min_V pq\left(\left(V - JE\right)^P (V - JE)\right) + bpq\left(V - C(I)\right)^P \\ &\quad \cdot (V - C(I)) d.p.V \int \{-1, 1\}^{m \times h}. \end{aligned} \quad (9)$$

$pq(V^P v)$ is a constant and has the same meaning as (B).

$$\min_V -pq\left(V^P (JE + bC(I))\right) d.p.V \epsilon \{-1, 1\}^{m \times h}. \quad (10)$$

To get a closed-form solution to T, use the formula below.

$$V = sgn(JE + bC(I)). \quad (11)$$

DH's T-step uses cyclic coordinate descent to learn the hash code bit by bit. Instead of using many steps to solve each bit, the T-step of DH uses just one, making it significantly quicker than DH. Algorithm 1 explains how to solve the DH problem. Algorithm 1 depicts the DDTHA.

A convex surrogate loss is often used to replace the zero-one loss in binary classification. Exponential loss is often used in boosting strategies like this one. Learning the f-th hash function is a challenge because of this difficulty. As a result, we use AdaBoost to overcome this issue. A decision tree and its weighting coefficient are learned in each boosting iteration. A binary decision tree has a decision stump at every node. The goal of training a stump is to minimize the weighted classification error by determining the optimal feature size and threshold. The next step is to simultaneously choose features and learn the hash function. In the literature, several effective decision tree learning strategies may considerably speed up the training process.

3.3. Ant Colony Optimization (ACO). Ant colony optimization is a technique that is used to improve the efficiency of the hash function operation. The first version of the ACO has historical relevance since it serves as the prototype for many different ant algorithms that, when combined, implement the ACO paradigm. ACO already matches the preceding subsection's framework, with the parts listed below:

$$t_{n\psi}^s = \begin{cases} \dfrac{\tau_{n\psi}^\alpha + \eta_{n\psi}^\beta}{\sum_{(n\zeta) \notin tabu_s} \left(\tau_{n\zeta}^\alpha + \eta_{n\zeta}^\beta\right)}, & \text{if } (n\psi) \notin tabu_s, \\ 0, & \text{otherwise.} \end{cases} \quad (12)$$

Inputs: training examples $\{i_x, j_x\} = 1$; code length h; maximum iteration number p; parameter λ
Output: binary codes $\{v_x\}_{x=1}^{m} \epsilon \{-1, 1\}^{m \times 1}$
Randomly select n examples $\{z_y\}_{x=1}^{n}$ from the trainingexamples and get the $\phi(x)$;
Initialize v_x as a $\{-1, 1\}$l vector randomly;
Initialize J as $J = \{J_{xy}\} \epsilon Q^{m \times f}$ where $J_{xy} = \begin{cases} 1, & if\ y_i = j \\ 0, & \text{otherwise} \end{cases}$;
Use (9) to initialize W;
Use (7) to initialize P;
Repeat
    T-step: Use (12) to solve T;
    K-step: Use (9) to solve E;
    S-step: Use (7) to solve T;
To acquire the hash function q_f, we must first train trees
Until convergence

Algorithm 1: DDTHA.

{Initialization}
Initialize $\tau_{n\psi}$ *and* $\eta_{n\psi}, \forall (n\psi)$
{Construction}
For each ant s (currently in state n) do
repeat
choose in probability the state to move
append the chosen move to the s-th ant's set $tabu_s$
until ant s has completed its solution.
end for
{Trail update}
For each ant move $(n\psi)$ *do*
compute $\Delta\tau_{n\psi}$
update the trailing matrix.
end for
{Terminating condition}
If not (end test) go to step

Algorithm 2: ACO.

$\begin{cases} \tau_{n\psi}^{\alpha} + \eta_{n\psi}^{\beta} / \sum_{(n\zeta) \notin tabu_s} (\tau_{n\zeta}^{\alpha} + \eta_{n\zeta}^{\beta}) & \text{if } (n\psi) \notin tabu_s \\ 0 & \text{otherwise} \end{cases}$ used in formula (10) indicates the effect of trail and attraction on $tabu_s$.

Formula (10) is used to update the trails after each iteration of the algorithm, i.e., after all ants have finished a solution.

$$\tau_{n\psi}(\tau) = \rho \tau_{n\psi}(\tau - 1) + \Delta\tau_{n\psi}. \tag{13}$$

For each step that an ant makes, (nψ), it contributes an equal amount of trail contributions, based on how well it solves its problem. This means that a better solution means a bigger contribution.

Using the TSP as an example, movements correspond to graph arcs; thus, a route ending at node x may correspond to the state n, while the state would correspond to the same path but with the arc (xy) added at the end (xy). Formula (12) becomes $\tau_{xy}(p) = \rho \tau_{xy}(p - 1) + \Delta\tau_{xy}$, if the length N_S of the tour discovered by the ant is used to measure the quality of the ant's answer to s.

$$\Delta\tau_{xy} = \sum_{s=1}^{f} \Delta\tau_{xy}^{s},$$
$$\Delta\tau_{xy}^{s} = \begin{cases} \dfrac{W}{N_s}, & \text{if ant } s \text{ uses are } (xy) \text{ initstour,} \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

W is a constant parameter in this example.

Ants build solutions in parallel and then update the trail levels in the main loop of the ant system. Various parameters must be tuned correctly for the algorithm's performance to be at its best τ_{xy} (0). These parameters include α, β, f, the number of insects used to define the quality of the solution, and W (which is used to define the relative relevance of ρ, trail, and attraction). Algorithm 2 depicts the ACO.

The process of hashing turns an unsigned digital certificate into a hashed one, which is subsequently changed

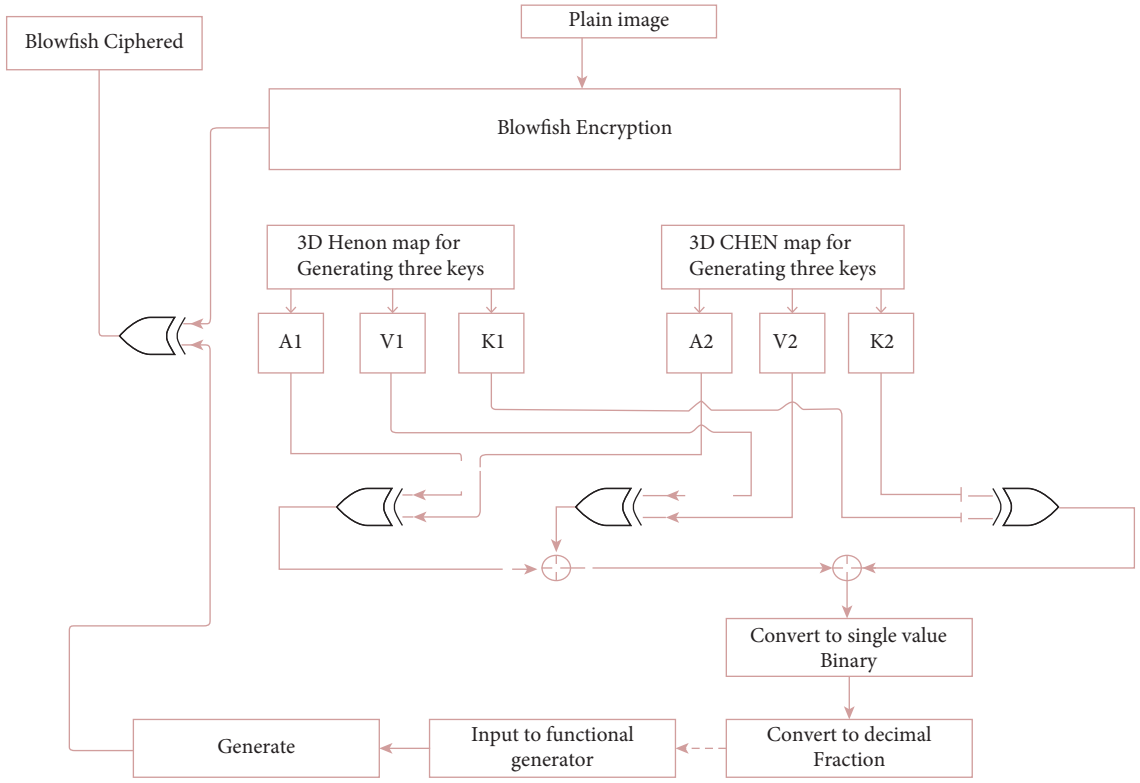

Figure 4: Framework of blowfish algorithm.

into an encrypted one via encryption. Finally, a signed digital certificate may be produced after the final encryption step.

3.4. Encryption Using Blowfish Algorithm (BA). During the process of encryption, the blowfish technique is used in our study to transform the plain text into cipher text. After the certificates have been encrypted, the hashed digital certificate then converts them into an encrypted digital certificate from which the final signed digital certificate is obtained.

In the BA framework, 3-dimensional Henon (Hn) and Chen (Ch) maps for encryption provide a supplement to numerical formulations and encrypted variables. BA is used to preprocess data from cloud databases. Figure 4 depicts the BA framework.

The mathematical expression for Hn map was provided as

$$\begin{aligned} x_{i+1} &= a - y_i^2 - bz_i, \\ x_{i+1} &= x_i, \\ y_{i+1} &= y_i. \end{aligned} \tag{15}$$

In comparison with the maps made out of extra current chaotic attractors, the stated attractor creates more challenging Hn maps. The following numerical equations serve as representations for the iterative map of Ch:

$$\begin{aligned} x_{i+1} &= a(y_i - z_i), \\ y_{i+1} &= (c-a)x_i - x_i z_i + cy_i, \\ z_{i+1} &= x_i y_i + bz_i. \end{aligned} \tag{16}$$

The unusual three-dimensional complexity of the dynamic attribute, in addition to the dimensionality, makes the system rather challenging. At last, the digital certificate that has been encrypted is saved in the cloud together with the digital certificate hashing.

4. Results and Discussion

In this paper, we investigate the security enhancement model in IoT using an optimized hashing algorithm with digital certificates for healthcare applications. "Waikato Environment for Knowledge Analysis (Weka)" and Java were used to establish this system's back end. To start this study, the datasets are collected from UCI. There are 303 cases all in the original Cleveland database. There are a total of 294 cases in the Hungarian database. The parameters are encryption time, decryption time, execution time, avalanche effect, and energy consumption. The existing methods are Lamport Merkle Digital Signature [LMDS (25)], Lightweight Mutual Authentication and Key Agreement [LMAKA (26)], PIRATE [PIRATE (27)], and Proxy Re-Encryption using RSA [PRER (28)].

Figure 5 depicts the encryption time. Encryption time discusses and indicates the average time needed to encrypt input media content files. It is measured in seconds. When it comes to encryption, the amount of time it takes to encrypt a given media data is directly related to the input media content file size. The LMDS was evaluated with an encryption time of 98 seconds. LMAKA was evaluated with an encryption time of 90 seconds. PIRATE was evaluated with an encryption time of 80 seconds. Proxy Re-Encryption

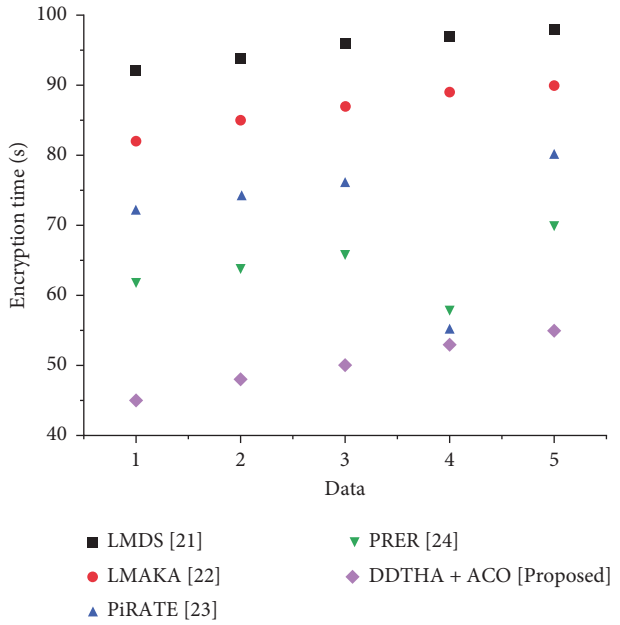

Figure 5: Comparative analysis of encryption time in suggested and traditional methods.

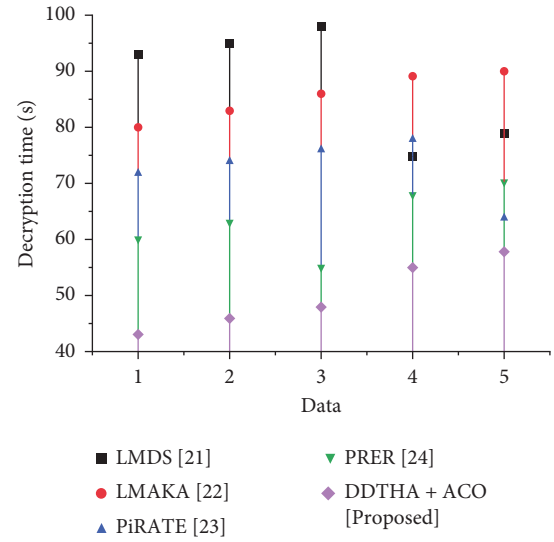

Figure 6: Comparative analysis of decryption time in suggested and traditional methods.

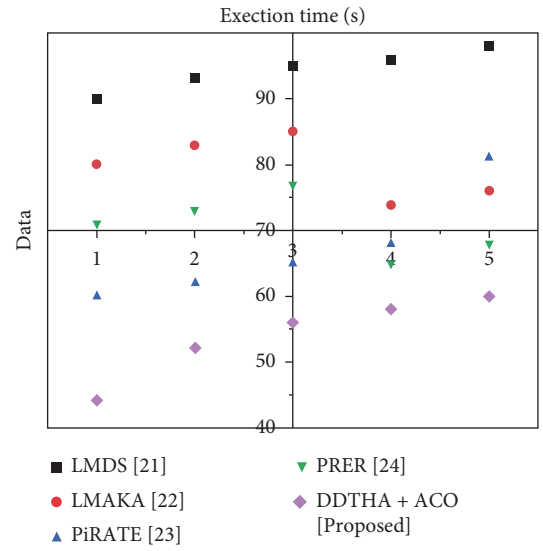

Figure 7: Comparative analysis of execution time in suggested and traditional methods.

using RSA was evaluated with an encryption time of 70 seconds. The proposed method discrete decision tree hashing algorithm with ant colony optimization (DDTHA + ACO) was evaluated with an encryption time of 55 seconds. Time taken by the proposed DDTHA + ACO technique for encryption was lesser compared to existing approaches like LMDS, LMAKA, PIRATE, and PRER. Thus, the proposed method encrypts data efficiently.

Decryption refers to the process of converting encrypted data back to its original state. Reverse encryption is often used. It decodes encrypted data so that only authorized users can do so since decryption needs a secret key or password.

Figure 6 depicts the decryption time. The Lamport Merkle Digital Signature was evaluated with a decryption time of 79 seconds. LMAKA was evaluated with a decryption time of 90 seconds. PIRATE was evaluated with a decryption time of 64 seconds. Proxy Re-Encryption using RSA was evaluated with a decryption time of 70 seconds. The proposed method discrete decision tree hashing algorithm with ant colony optimization (DDTHA + ACO) was evaluated with a decryption time of 58 seconds. Time taken by the proposed DDTHA + ACO technique for decryption was lower when compared with existing approaches like LMDS, LMAKA, PIRATE, and PRER.

The amount of time the system spends executing runtime or system operations on its behalf is taken into account when calculating the execution time of a job. The implementation determines the technique for calculating execution time.

Figure 7 depicts the execution time. The Lamport Merkle Digital Signature was evaluated with an execution time of 98 seconds. LMAKA was evaluated with an execution time of 76 seconds. PIRATE was evaluated with an execution time of 81 seconds. Proxy Re-Encryption using RSA was evaluated with an execution time of 68 seconds. The proposed method discrete decision tree hashing algorithm with ant colony optimization (DDTHA + ACO) was evaluated with an execution time of 60 seconds. Time taken by the proposed DDTHA + ACO technique for execution time was less when compared with existing approaches like LMDS, LMAKA, PIRATE, and PRER.

Using the avalanche effect, it is possible to compare the effectiveness of suggested and traditional algorithms in assuring media data security. It is estimated based on the algorithm's resilience to threats and on-the-fly attacks during media data transfer. The avalanche effect in encryption methods is defined as the proportion of changed bits in the cipher text to the total number of bits in the cipher text.

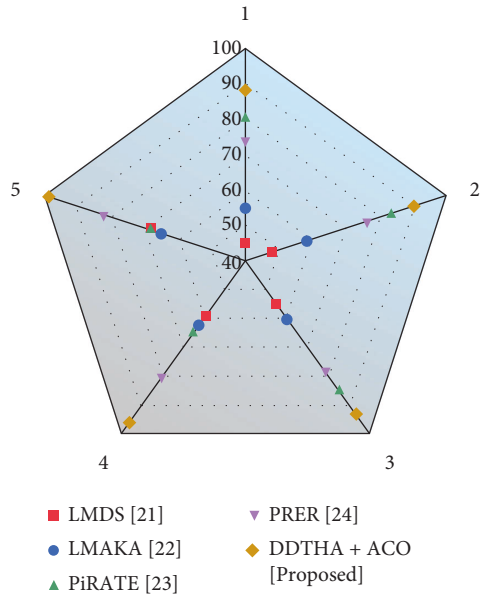

Figure 8: Comparative analysis of avalanche effect in suggested and traditional methods.

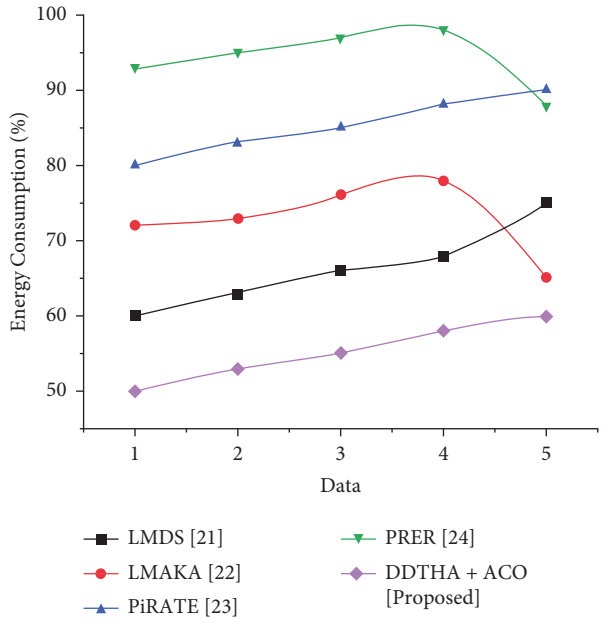

Figure 9: Comparative analysis of energy consumption in suggested and traditional methods.

Figure 8 depicts the avalanche effect. The Lamport Merkle Digital Signature was evaluated with the avalanche effect of 68 percent. LMAKA was evaluated with the avalanche effect of 65 percent. PIRATE was evaluated with the avalanche effect of 68 percent. Proxy Re-Encryption using RSA was evaluated with the avalanche effect of 82 percent. The proposed method discrete decision tree hashing algorithm with ant colony optimization (DDTHA + ACO) was evaluated with the avalanche effect of 98 percent. Compared to the current approaches, the suggested method exhibits more significance. When compared to the suggested technique, the current methods LMDS, LMAKA, PIRATE, and PRER reveal less effectiveness.

Energy consumption refers to the amount of power or energy consumed to encrypt data.

Figure 9 depicts energy consumption. The Lamport Merkle Digital Signature was evaluated with an energy consumption of 75 percent. LMAKA was evaluated with an energy consumption of 65 percent. PIRATE was evaluated with an energy consumption of 90 percent. Proxy Re-Encryption using RSA was evaluated with an energy consumption of 88 percent. The proposed method discrete decision tree hashing algorithm with ant colony optimization (DDTHA + ACO) was evaluated with an energy consumption of 60 percent. The suggested method shows less than the current approaches. The existing approaches, LMDS, LMAKA, PIRATE, and PRER, demonstrate high efficacy when compared to the proposed technique.

Precision is the resolution of the representation, often determined by the number of decimal or binary digits, whereas accuracy is the proximity of a computation to the true value.

The ability of a classifier to identify all positive samples is referred to as recall. Value (%) for recall, precision, and accuracy is shown in Figure 10. The Lamport Merkle Digital

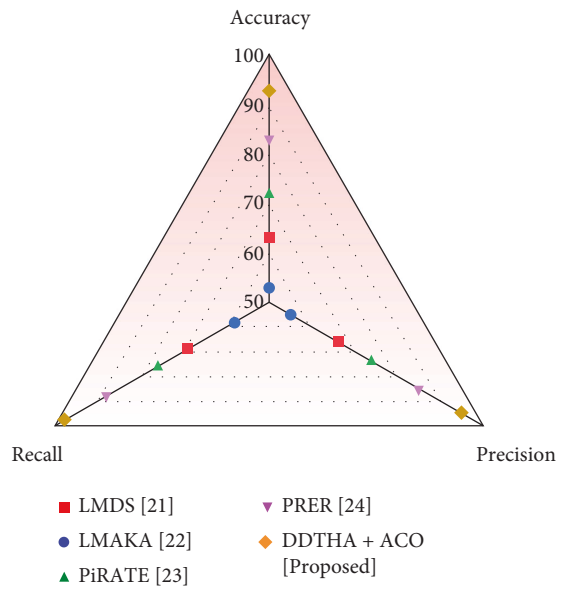

Figure 10: Comparative analysis of suggested and traditional methods.

Signature was evaluated with recall, precision, and accuracy of 69, 66, and 63 percent, respectively. LMAKA was evaluated with recall, precision, and accuracy of 58, 55, and 53 percent, respectively. PIRATE was evaluated with recall, precision, and accuracy of 76, 74, and 72 percent, respectively. Proxy Re-Encryption using RSA was evaluated with recall, precision, and accuracy of 88, 85, and 83 percent, respectively. The proposed method discrete decision tree hashing algorithm with ant colony optimization (DDTHA + ACO) was evaluated with recall, precision, and accuracy of 98, 95, and 93 percent, respectively. The

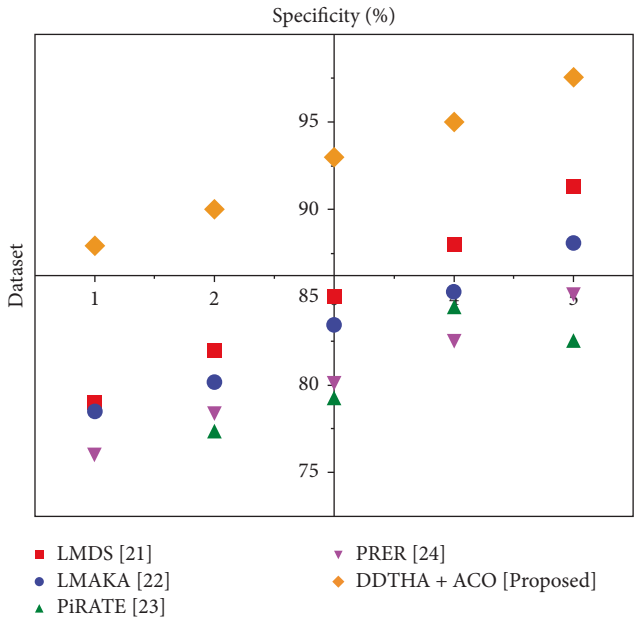

Figure 11: Comparative analysis of specificity.

suggested method shows higher than the current approaches. The existing approaches, LMDS, LMAKA, PIRATE, and PRER, demonstrate less when compared to the proposed technique.

LMDS specificity was 91.3%. LMAKA had 88.1% specificity. PIRATE's specificity was 82.4%. PRER was 85.3% specific. The DDTHA + ACO technique was 97.6% specific. The suggested method is better than the current approaches. The existing techniques are less successful than the suggested technique.

Figures 5 to 11 depict comparison of comparing the suggested approach with the current models. Existing methods used in this study are LMDS [21], LMAKA [22], PIRATE [23], and PRER [24]. Figures clearly show that the suggested approach performs better than the current techniques because of the existing method's drawbacks. The following are the drawbacks of the existing methods. LMDS requires more processing time, LMAKA is less secured, PIRATE requires high computational cost, whereas PRER has the issue of a processed lag brought on by dumping a major amount of computing work to the proxy for re-encryption, as well as the computationally intensive data in transit encryption as well as users' decryption procedures brought on by asymmetric cryptographic usage.

5. Conclusion

It is exceedingly challenging to guarantee the safety and confidentiality of an IoT-based health service. It is considerably more challenging by the fact that IoT is frequently used to link clients to healthcare organizations among a wide network of services who are dispersed across several domains and with various trust authorities. This makes it more difficult to secure patient information. A lot of researchers have come up with a variety of authentication and authorization strategies in order to avoid and preserve the sensitive data that are acquired with the assistance of wearable Internet of Things devices. However, there is a need for end-to-end security solutions in order to protect and control the data on patients' health. For this reason, it is crucial to implement stringent safety measures to protect this patient's information. In light of this, the research presented here suggests an improved hashing method that makes use of digital certificates in order to increase security. The unsigned digital certificates can be hashed using the discrete decision tree hashing algorithm (DDTHA) with ant colony optimization (ACO) that has been developed. In order to encrypt the data, the blowfish method is utilized, and then a signed digital certificate is created for subsequent usage in the authentication process. The proposed approach was analyzed and compared with existing approaches, as well as the proposed approach attained the greatest performance in terms of encryption time (55 s), decryption time (58 s), execution time (60 s), avalanche effect (98%), and energy consumption (65%) than those existing approaches.

5.1. Future Scope. However, there are still some restrictions on how quickly data may be encoded and decoded according to this study. That means it will have to be improved soon. The efficiency of this study could be greatly improved with the use of optimization methods for the problem of improving encryption and decryption speeds. Furthermore, the focus of this study is on only heart problems. More disease observation is needed in the future to help this field advance. As a result, we advise that, in the near future, a novel security method be developed in order to identify misbehaving greedy nodes in IoT networks.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank Arab Open University, Saudi Arabia, for supporting this study.

References

[1] A. Rizwan, D. A. Karras, J. Kumar, M. Sánchez-Chero, M. M. Mogollón Taboada, and G. C. Altamirano, "An internet of things (IoT) based block chain technology to enhance the quality of supply chain management (SCM)," *Mathematical Problems in Engineering*, vol. 2022, Article ID 9679050, 12 pages, 2022.

[2] A. Rizwan, D. A. Karras, M. Dighriri et al., "Simulation of IoT-based vehicular ad hoc networks (VANETs) for smart traffic management systems," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 3378558, 11 pages, 2022.

[3] A. Choudhuri, J. M. Chatterjee, and S. Garg, "Internet of Things in healthcare: a brief overview," *Internet of Things in Biomedical Engineering*, pp. 131–160, 2019.

[4] M. Usak, M. Kubiatko, M. S. Shabbir, O. Viktorovna Dudnik, K. Jermsittiparsert, and L. Rajabion, "Health care service delivery based on the Internet of things: a systematic and comprehensive study," *International Journal of Communication Systems*, vol. 33, no. 2, Article ID e4179, 2020.

[5] H. Z. Almarzouki, H. Alsulami, A. Rizwan, M. S. Basingab, H. Bukhari, and M. Shabaz, "An internet of medical things-based model for real-time monitoring and averting stroke sensors," *Journal of Healthcare Engineering*, vol. 2021, pp. 1–9, 2021.

[6] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "On the role of hash-based signatures in quantum-safe internet of things: current solutions and future directions," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 1–17, 2021.

[7] R. Krishnamoorthi, S. Joshi, H. Z. Almarzouki et al., "A novel diabetes healthcare disease prediction framework using machine learning techniques," *Journal of Healthcare Engineering*, vol. 2022, Article ID 1684017, 10 pages, 2022.

[8] M. Al-Ghamdi, M. Al-Ghamdi, and A. Gutub, "Security enhancement of shares generation process for multimedia counting-based secret-sharing technique," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16283–16310, 2019.

[9] M. Saravanan and A. Priya, "An algorithm for security enhancement in image transmission using steganography," *Journal of the Institute of Electronics and Computer*, vol. 1, no. 1, pp. 1–8, 2019.

[10] F. F. Alruwaili, "Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records," *PeerJ Computer Science*, vol. 6, p. e323, 2020.

[11] G. I. Ahmad, J. Singla, and K. J. Giri, "Security and privacy of E-health data," in *Multimedia Security*, pp. 199–214, Springer, Berlin, Germany, 2021.

[12] M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, and O. Almomani, "A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS," *Sensors*, vol. 22, no. 4, p. 1448, 2022.

[13] M. T. De Oliveira, L. H. Reis, R. C. Carrano et al., "Towards a blockchain-based secure electronic medical record for healthcare applications," in *Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Shanghai, China, May 2019.

[14] M. A. Azad, J. Arshad, S. Mahmoud, K. Salah, and M. Imran, "A privacy-preserving framework for smart context-aware healthcare applications," *Transactions on Emerging Telecommunications Technologies*, Article ID e3634, 2019.

[15] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.

[16] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020.

[17] W. Y. Ng, T. E. Tan, P. V. H. Movva et al., "Blockchain applications in health care for COVID-19 and beyond: a systematic review," *The Lancet Digital Health*, vol. 3, no. 12, pp. e819–e829, 2021.

[18] J. Iqbal, M. Adnan, Y. Khan et al., "Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis," *Journal of Healthcare Engineering*, vol. 2022, pp. 1–19, 2022.

[19] S. M. Karunarathne, N. Saxena, and M. K. Khan, "Security and privacy in IoT smart healthcare," *IEEE Internet Computing*, vol. 25, no. 4, pp. 37–48, 2021.

[20] A. Singh and K. Chatterjee, "ITrust: identity and trust based access control model for healthcare system security," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 28309–28330, 2019.

[21] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, 2020.

[22] M. Mehrtak, S. SeyedAlinaghi, M. MohsseniPour et al., "Security challenges and solutions using healthcare cloud computing," *Journal of Medicine and Life*, vol. 14, no. 4, pp. 448–461, 2021.

[23] F. Ali, S. El-Sappagh, S. R. Islam et al., "A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion," *Information Fusion*, vol. 63, pp. 208–222, 2020.

[24] J. A. Alzubi, "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare," *Computer Communications*, vol. 170, pp. 200–208, 2021.