Hindawi
Journal of Sensors
Volume 2022, Article ID 8457116, 17 pages
https://doi.org/10.1155/2022/8457116

Research Article

Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism

Adil O. Khadidos,[1] S. Shitharth,[2] Alaa O. Khadidos,[3] K. Sangeetha,[2] and Khaled H. Alyoubi[3]

[1] *Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[2] *Department of Computer Science and Engineering, Kebri Dehar University, Kebri Dehar 250, Ethiopia*
[3] *Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*

Correspondence should be addressed to S. Shitharth; shitharth.it@gmail.com

Received 3 January 2022; Accepted 12 May 2022; Published 2 June 2022

Academic Editor: Panagiotis Papageorgas

Providing security to the healthcare data stored in an IoT-cloud environment is one of the most challenging and demanding tasks in recent days. Because the IoT-cloud framework is constructed with an enormous number of sensors that are used to generate a massive amount of data, however, it is more susceptible to vulnerabilities and attacks, which degrades the security level of the network by performing malicious activities. Hence, Artificial Intelligence (AI) technology is the most suitable option for healthcare applications because it provides the best solution for improving the security and reliability of data. Due to this fact, various AI-based security mechanisms are implemented in the conventional works for the IoT-cloud framework. However, it faces significant problems of increased complexity in algorithm design, inefficient data handling, not being suitable for processing the unstructured data, increased cost of IoT sensors, and more time consumption. Therefore, this paper proposed an AI-based intelligent feature learning mechanism named Probabilistic Super Learning- (PSL-) Random Hashing (RH) for improving the security of healthcare data stored in IoT-cloud. Also, this paper is aimed at reducing the cost of IoT sensors by implementing the proposed learning model. Here, the training model has been maintained for detecting the attacks at the initial stage, where the properties of the reported attack are updated for learning the characteristics of attacks. In addition to that, the random key is generated based on the hash value of the data matrix, which is incorporated with the standard Elliptic Curve Cryptography (ECC) technique for data security. Then, the enhanced ECC-RH mechanism performs the data encryption and decryption processes with the generated random hash key. During performance evaluation, the results of both existing and proposed techniques are validated and compared using different performance indicators.

1. Introduction

Artificial Intelligence (AI) [1–3] is one of the modern and highly demanding technology used in many real-time application systems due to its enormous benefits of ensured security, ability to handle more complex data, reduced duplicates, and unknown threat identification [4, 5]. Also, the Internet of Things (IoT) [6, 7] is a kind of intelligent framework that helps to connect various sensors [8] and devices with the cloud for reliable data communication and transmission. The IoT applications have gained significant attention in many research fields with the benefits of increased efficiency and autonomous characteristics. In this system, the IoT device [9] can use various sensors to gather the data from the environment and transfer it to the connected devices, which passes the information to the cloud through wireless links. However, this process faces many security challenges [10, 11] by the vulnerabilities and harmful attacks against the network. Hence, security is one of the major concerns that need to be resolved in the cloud-IoT environment [12] to preserve confidential information's trustworthiness. In recent days, increasing the security of healthcare systems is highly demanded to protect the users' private and confidential information. For this type of application, AI technology is more suitable for improving the security of healthcare applications deployed in an IoT-cloud environment. Typically, there are different types of AI techniques that have been used in many application systems, which come under the categories of rule-based methodologies, machine learning techniques, and deep learning models. The general illustration of various AI techniques with their types is represented in Figure 1.

1.1. Motivation and Incitement. This research work intends to develop an intelligent AI-based feature learning methodology for predicting attacks in an earlier stage by training the features of the user data. Moreover, the random hash key is generated and incorporated with the ECC methodology for data encryption and decryption processes.

1.2. Research Gap. The conventional works developed different encryption and classification methodologies [13, 14] to ensure secure data storage and retrieval in the IoT-cloud domain. Generally, the encryption techniques [15] like Advanced Encryption Standard (AES) [16], Rivest Shamir Adleman (RSA), SHA-512, and Elliptic Curve Cryptography (ECC) have been widely used in many data security systems [17]. Moreover, it helps decrypt the raw data before storage and retrieval processes with guaranteed security [18]. Still, it faces the major problems of increased time consumption, high computational complexity, and slow processing at the time of key generation and authentication. Also, the classification methodologies [19–21] limit the issues of high error rate, inefficient prediction results, and delay in the process, which degrades the performance of the entire security system. In order to solve these problems, the proposed work is aimed at developing an intelligent security scheme based on AI technology for healthcare systems.

1.3. Contribution and Organization. The major contributions of this paper are as follows:

(i) To ensure the security of healthcare data stored in IoT-cloud, the Random Hashing (RH) technique is developed for generating the random keys used for data encryption and decryption

(ii) To establish the secured data transmission from IoT to cloud based on the user query input processing

(iii) To guarantee the secured data retrieval with attack detection and feature learning models, an Artificial Intelligence- (AI-) based Probabilistic Super Learning (PSL) mechanism is implemented

To assess the performance of the proposed PSL-RH technique, various evaluation metrics have been considered. Such as accuracy, precision, recall, key generation time, encryption time, and decryption time. The remaining portions of this paper are segregated as follows: the existing techniques used for data security and attack classification in cloud-IoT domain are reviewed with their advantages and disadvantages in Section 2. The detailed description of the proposed methodology is presented with its clear flow and algorithmic illustrations in Section 3. The performance analysis of existing and proposed data security mechanisms is validated and compared based on various performance measures in Section 4. Finally, the overall paper is summarized with its future scope in Section 5.

2. Related Works

This section discusses some conventional security mechanisms related to AI-based security schemes for IoT systems. Also, it investigates the advantages and disadvantages of each technique based on its working operations and characteristics.

Ghazal [22] developed an IoT framework incorporated with an AI system to ensure healthcare applications' security. The main aim of this paper was to safeguard the privacy and security of patients' data stored on the internet. For this purpose, the Deep Neural Network- (DNN-) based malware detection mechanism was deployed. This helps restrict the authenticated access to the cloud data to avoid unauthorized/malware activities. Also, the key authentication was performed based on the parameters of specific weight and bias values. In order to detect the malware and secure the recognized information, the sigmoid function has been estimated for training the set of extracted features. The key benefits of this work were reduced response time, increased delivery of packets, and minimal delay. Valanarasu [23] constructed a smart and secured IoT framework to increase the hospital environment's security. Here, some of the key policies and regulations of AI technique could be integrated with this framework, including accountability, transparency, data privacy, security, interoperability, and sustainability. Also, it is aimed at detecting the different types of attacks based on the host properties, information disruptions, and network properties. However, this framework does not utilize any specific methodologies for detecting the attacks on the network, which degrades the entire system's performance. Greco et al. [24] investigated the recent trends of IoT-AI systems to develop smart healthcare systems. Here, the three-tier architecture was constructed for designing the Internet of Medical Things (IoMT) systems by incorporating the functionalities of WBSN, field sensor networks, and cloud services.

Bharadwaj et al. [25] conducted a detailed study on various machine learning techniques used for the healthcare IoT (HIoT) systems, where the applications and constraints of each technique have been discussed. This work stated that the parameters like interoperability, reliability, bounded latency, privacy, and security must be satisfied for developing an efficient and secured IoT framework. Here, the different types of similarity matching techniques such as linear regression, logistic regression, K-means, discriminant analysis, and dimensionality reduction methods have been discussed with their operating functions. Based on this study, it is observed that the linear regression model is one of the suitable techniques for estimating the relationship between the dependent/independent variables. Zaman et al.

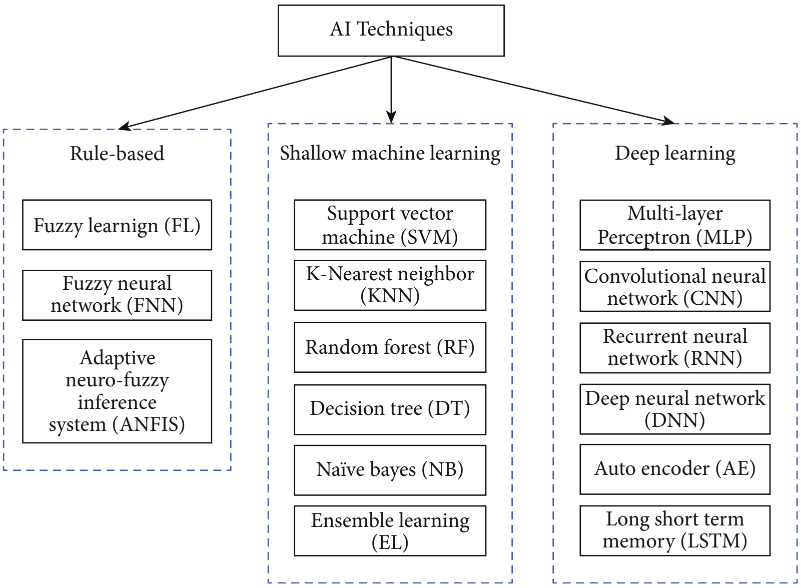
AI Techniques
Rule-based
Fuzzy learnign (FL)
Fuzzy neural network (FNN)
Adaptive neuro-fuzzy inference system (ANFIS)
Shallow machine learning
Support vector machine (SVM)
K-Nearest neighbor (KNN)
Random forest (RF)
Decision tree (DT)
Naïve bayes (NB)
Ensemble learning (EL)
Deep learning
Multi-layer Perceptron (MLP)
Convolutional neural network (CNN)
Recurrent neural network (RNN)
Deep neural network (DNN)
Auto encoder (AE)
Long short term memory (LSTM)

Figure 1: Various AI mechanisms used for security.

[26] presented a comprehensive survey related to various AI mechanisms used to improve IoT networks' security. This paper also discussed the major security challenges that exist in the IoT networks, which include the factors of confidentiality, availability, and source authentication. Amin et al. [27] designed a lightweight authentication protocol to increase IoT-enabled devices' security in the cloud environment. This work includes the processes of user/server registration and authentication. The motive of this system was to authenticate the users for providing access to the confidential information stored on the private cloud. The advantages of this framework were reduced computational and storage cost consumption. Nevertheless, it does not provide an optimal performance outcome regarding high reliability, attack detection, and misclassification rate.

Choi and Choi [28] developed an IoT-cloud security framework by using the context ontology model for identifying the system vulnerabilities. The key motive of this paper was to accurately detect the system intrusions and device vulnerabilities across the IoT-cloud environment by deploying an efficient security mechanism. In this model, the inference rules have been generated based on the pattern of attacks such as data sniffing, memory dump, software attack, and port access. However, this model is more complex for understanding, which requires categorizing the vulnerabilities based on the inference rules. Shen et al. [29] employed an efficient privacy preservation mechanism to ensure the IoT-cloud environment's security. Here, an integrated bilinear map and homomorphic encryption methodologies have been utilized for encrypting the data into an unknown format. Mo [30] suggested a secured data storage method by using an enhanced Ant Colony Optimization (ACO) technique. This paper mainly considers improving the load balancing strategy with optimized completion time for securely storing the data on the cloud. Here, the full-homomorphic encryption and reencryption mechanisms were deployed to store the data on the IoT-cloud in an encrypted format. In [31], the Advanced Encryption Standard (AES) mechanism was utilized to store healthcare data in an IoT-cloud environment securely. This type of encryption model generates the secret key for generating the ciphertext with multiple transformation rounds. The overall quality of this security system has been assessed based on the parameters of accuracy, latency, consistency, and QoS.

Riad et al. [32] implemented a Sensitive and Energetic Access Control (SE-AC) mechanism for improving the security of Electronic Health Records (EHRs) stored in an IoT-cloud environment. The main motive of this paper was to ensure both the privacy and confidentiality of the healthcare data by using the fine-grained access control mechanism. In order to validate the effectiveness of this mechanism, the encryption time, decryption time, storage overhead, and token generation time have been estimated. Guan et al. [33] investigated the data security and privacy issues in cloud computing and fog computing. Here, the major requirements of secured data storage have been discussed, including integrity verification, dynamic support, reduced overhead, access efficiency, authorization, and fine-grained access control. Zhu et al. [34] deployed a new cyber security framework for guaranteeing the privacy and security of healthcare systems. The main aim of this paper was to reduce the computational overhead of the security framework with the use of a machine learning approach. Kalyani and Chaudhari [35] employed an Optimal Homomorphic Encryption (OHE) scheme for increasing the sensitivity of data stored in an IoT environment. Here, the Deep Neural Network (DNN) technique was used for classifying the attack based on the optimal features. In addition to that, the Step Size Firefly (SSFF) optimization technique was also utilized for authenticating the key during the data encryption. Zaman et al. [26] presented a taxonomy of various AI-based security mechanisms used for IoT networks. The layer-wise security threats have been discussed with their attacking activities. The different types of AI technologies investigated in this paper were rule-based machine learning, deep learning, and shallow machine learning. Table 1 presents the review on various AI models used for improving the healthcare IoT data security systems.

Based on this study, it is analyzed that the AI and machine learning techniques are widely used for guaranteeing the countermeasures of IoT threats. These techniques have the ability to self-routine the operations that helps to increase the overall performance of the security system. Still, it limits with major challenges of overfitting problems, handling difficulties in large dimensional data, increased time delay, and data scarcity. In order to resolve these problems, the proposed work is aimed at developing an advanced AI-based security mechanism for enabling the secure data storage and retrieval of healthcare systems.

3. Proposed Methodology

This section presents a detailed description of the proposed methodology with its clear algorithmic and flow illustrations. The main motive of this paper is to securely store and retrieve the data from the IoT-cloud system by implementing an advanced AI technique, where the healthcare-based application system is considered. The original contribution of this work is that the proposed framework utilizes the AI-based Probabilistic Super Learning (PSL) model for efficiently managing the secure data transmission by identifying the properties/features of the data obtained from the IoT devices. The PSL technique is aimed at identifying both the normal and attacking activities with the updated set of features. Also, the PSL technique developed based on the AI model improves feature learning by updating the properties and characteristics of the attacks at each instant. In addition to that, the Random Hashing (RH) technique is utilized in the Elliptic Curve Cryptography (ECC) model for performing the data encryption and decryption processes, which guarantees the data security of both storage and retrieval.

The overall architecture and flow of the proposed AI-based security system are shown in Figures 1 and 2, respectively, which comprise the following stages:

(1) Data transmission from IoT to cloud

(2) User query input processing

(3) Attack detection and feature learning

(4) Secured data retrieval from cloud to user

At first, the users' sensor data has been obtained and encrypted before storing it into the cloud using the proposed RH technique. It is mainly used to encrypt and decrypt the original data based on forming a hash key generation matrix. Then, the AI security mechanism is applied to check whether the data is normal or attacked. Suppose it is identified as the normal flow. In that case, the data arrangement process is performed for storing the data in the cloud. If it is identified as an attack, it can be automatically reported to the firewall or routing system to block the attacks at the initial stage of processing.

Consequently, the training model has been updated with the help of PSL methodology, which updates the properties of the reported attack and arranges the features according to that. Here, the attacking classification is performed based on the updated properties/features of the data maintained in the training model. The user can enter the input query to access the required data during the query input processing. The AI-PSL methodology is used to validate whether the user is normal or an attacker based on the set of updated properties of the trained model. If the user is normal, the query request has been passed to the cloud storage, which provides the retrieved data in the decrypted format. Here, the RH-based decryption process is applied to decrypt the original information by generating the signature matching pattern. At last, the decrypted data has been displayed to the user with ensured privacy and security measures.

3.1. Data Security Using ECC-Based Random Hashing Technique

In this stage, the original data was initially encrypted before storing it into the IoT cloud using the RH technique. In many security application systems, ensuring data security is one of the demanding and challenging processes due to the large volume of data and complex formatting in feature arrangement. Typically, data security has been defined by the processes of secured data storage before encryption and data retrieval after decryption with the proper authentication for accessing the data. For this purpose, there are different types of data encryption, and decryption standards are developed in the conventional works, including AES, DES, RS4, and some other models. However, it has the significant disadvantages of increased time consumption for key generation and encryption, complexity implementation, and computational overhead. Hence, this paper utilized an Elliptic Curve Cryptography-(ECC-) based encryption mechanism [36] with the novel RH key generation technique. This ECC-RH is used to ensure data security based on the encryption and decryption processes. The ECC is one of the widely used encryption standards for increasing the data security of both IoT-cloud domains. In the proposed scheme, the key generation process of the existing ECC technique has been updated with the RH technique. Based on the input data stream with the hash value, the random key has been generated in this model, which is used for encrypting and decrypting the cloud data. The major advantages of using the random hashing-based ECC technique are as follows: the generated keys are small in size, fast encryption and decryption, reduced time consumption, and optimal bandwidth usage. However, it follows some composite computations for generating the hash function in order to ensure the increased level of security.

Initially, it takes the data streams I_n as input and produced the random key points R_V as output, which is used for data encryption and decryption. Here, the weight parameters w and temporary matrix q are initialized at first that are used for generating the hash key matrix. After that, the sequence of parameters such as S_1 and S_2 are updated with respect to each counter iteration as shown in the following:

Table 1: Review on existing models.

Authors and references	Method	Description	Advantages/disadvantages
Ghazal [22]	Deep Neural Network- (DNN-) based AI model	This work objects to improve the privacy and security of patients' data stored on cloud systems by using the AI-incorporated IoT framework.	Advantages: (1) Requires minimal response time (2) Increased delivery of packets (3) Reduced delay Disadvantages: (1) Computational complexity (2) Misclassified predictions
Valanarasu [23]	Smart and secured IoT framework using the AI model	The purpose of this paper is to detect the different types of attacks based on the host properties, information disruptions, and network properties.	Advantages: (1) Simple design (2) Minimal cost consumption Disadvantages: (1) It does not have any specific methodologies for attack detection (2) Increased error outputs
Bharadwaj et al. [25]	Healthcare IoT (HIoT) systems	It presented a comprehensive survey on various similarity matching techniques for securing healthcare data using IoT systems.	Advantages: (1) Ensured data privacy and security (2) Optimal performance Disadvantages: (1) Training model of features requires more time consumption
Zaman et al. [26]	AI model in IoT security	In this paper, a comprehensive review is presented related to various AI models used for IoT security systems.	Advantages: (1) AI models provide accurate prediction results (2) Efficient learning and training Disadvantages: (1) Deep learning models follow complex operating steps
Amin et al. [27]	Light weight authentication protocol for IoT security	This paper developed a light weight authentication mechanism for increasing the security of IoT-cloud systems with the help of the AI model.	Advantages: (1) Minimal computational and storage cost consumption (2) High efficiency Disadvantages: (1) Reduced reliability (2) Increased misclassification results
Riad et al. [32]	Sensitive and Energetic Access Control (SE-AC) mechanism	Here, the SE-AC mechanism is mainly developed for improving the security of Electronic Health Records (EHRs) stored in an IoT-cloud environment.	Advantages: (1) Reduced encryption and decryption time (2) Minimal storage overhead Disadvantages: (1) Increased token generation time (2) It does not have the ability to handle large dimensional data
Kalyani and Chaudhari [35]	Optimal Homomorphic Encryption (OHE) scheme	This paper utilized the OHE-DNN model for classifying the attack based on the optimal features.	Advantages: (1) Better convergence speed (2) Highly efficient Disadvantages: (1) More time consumption (2) Increased storage overhead

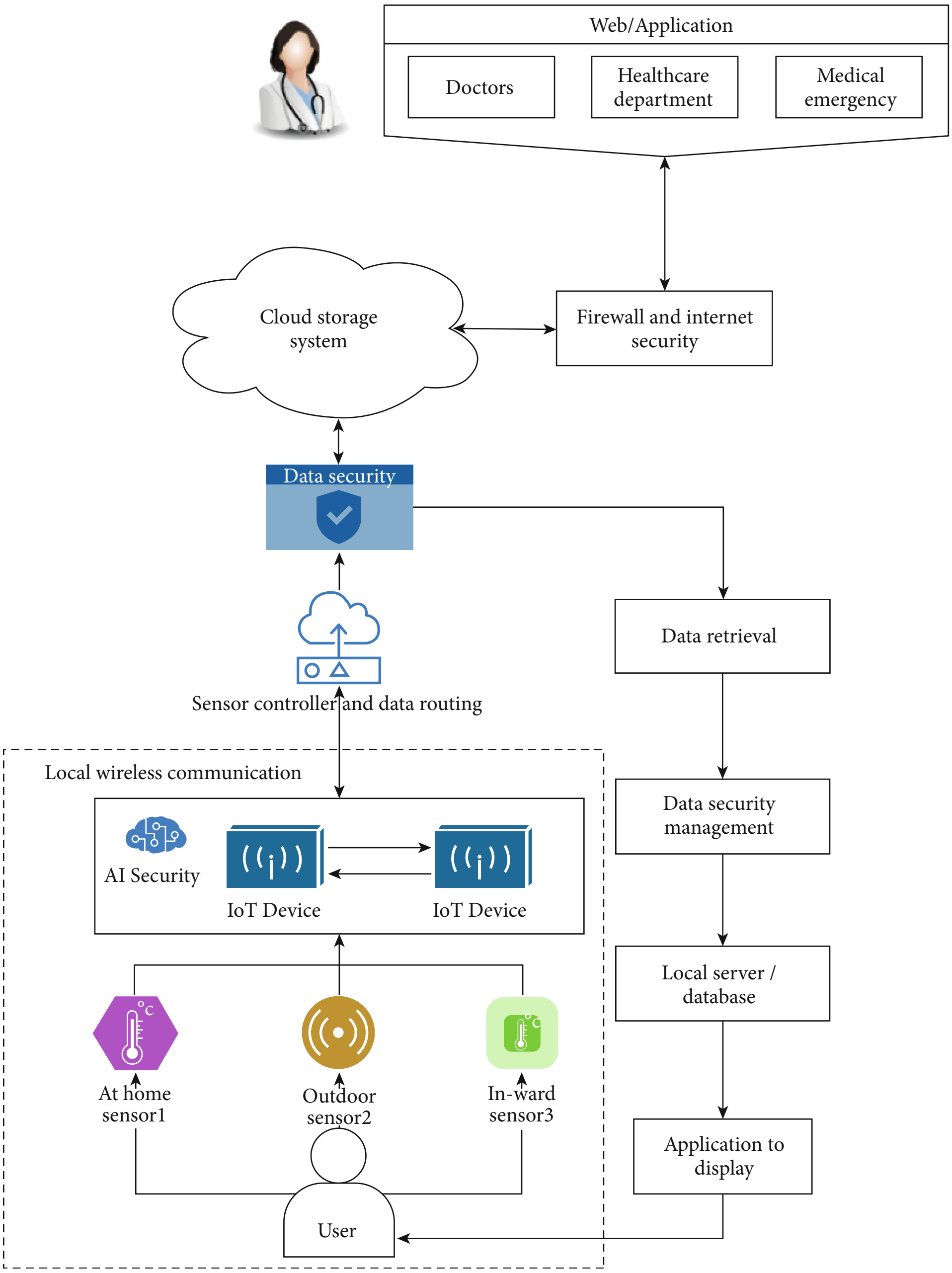

Figure 2: Architecture model of the proposed AI-based healthcare data security scheme in IoT-cloud.

$$S_1 = h_q(m) + (\mathrm{XOR}(A, B, C)) + (\mathrm{XOR}(D, E, F)) + w + k + ch + m, \tag{1}$$

$$S_2 = h_q(4) + h_q(m) + (\mathrm{XOR}(D, E, F)) + w + k + ch, \tag{2}$$

where $A = \{q[1][1 : 0], q[1][32 : 2]\}$, $B = \{q[1][12 : 0], q[1][31 : 13]\}$, $C = \{q[1][21 : 0], q[1][31 : 22]\}$, $D = \{q[5][5 : 0], q[1][31 : 6]\}$, $E = \{q[5][10 : 0], q[1][31 : 11]\}$, and $F = \{q[5][24 : 0], q[1][31 : 25]\}$.

Then, the signature pattern $h_q(x)$ is computed from the generated matrix as shown in the following:

$$h_q(x) = \begin{cases} h_q(x-1), & \forall x = \{2, 3, \cdots m-1\}, \\ S_1, & \text{if } (x == 1), \\ S_2, & \text{if } (x == 5). \end{cases} \tag{3}$$

Consequently, the count has been updated with respect to the size of matrix, and the estimated patterns are represented as follows:

$$ch = \mathrm{XOR}(\mathrm{AND}(q[5], q[6]), \mathrm{AND}(\mathrm{NOT}(q[5]), q[7])), \tag{4}$$

```
Input: Input data streams, $I_n$
Output: Random key points, $R_V$
Step 1: Initialize weight parameter as "$w$"
Step 2: Initialize the temporary matrix "$q$" as
        $q' = \{q1, q2, \cdots qn\}$
Step 3: From this "$q'$" matrix, the sequence $S_1$ and $S_2$
        parameters are updated and arranged for each counter
        iteration as represented in equations (1) and (2)
Step 4: Estimate the signature pattern $h_q(x)$ from the matrix
        by using equation (3)
Step 5: For $x = 2$ to $m - 1$ loop//loop run for 2 to "$m - 1$" size
        of "$q'$" matrix.
            Update counter as counter ++.
            Estimate the pattern such as $ch$ and $mj$ by
            using equations (4) and (5);
            Update $S_1$ and $S_2$ for each counter update;
        End loop "x"
Step 6: This cross computing generates the random key
        $R_V$ for the memory storage which can be represented
        as represented in equation (6)
```

Algorithm 1: Data security using RH generation.

$$mj = \mathrm{XOR}(\mathrm{XOR}(\mathrm{AND}(q[1], q[2]), \mathrm{AND}(q[1], q[3])), \mathrm{AND}(q[2], q[3])). \tag{5}$$

Based on this cross computing, the random key R_V is generated for storing and retrieving the data in cloud that is illustrated in the form of

$$R_V = h_q(\text{counter}). \tag{6}$$

The detailed algorithmic procedure of the random hash key generation process is illustrated in Algorithm 1 as follows:

3.2. PSL Algorithm. In this stage, the feature learning technique is mainly used for detecting the attacks by training the model based on the features of the matrix. The proposed PSL methodology extracts features from the IoT device. It is updated in the training data model with the categories of normal and attacking features. The PSL is developed as the feature learning model for matching the feature attributes with the database for spotting the attacks. The IoT device features are matched with this training model for identifying whether any attacking devices could try to access the data stored in the cloud during the data storage and retrieval process. If the access is legitimate, the normal flow of operations like data storage and retrieval has been performed automatically. If it is identified as an attack, it can be automatically reported to the firewall/routing device that blocks the access at the initial stage. Also, the features and characteristics of this attack are learned and updated with the available training model; then, the overall features of the training model have been entirely updated and arranged to the new attacking features. This trained model can be further used for the consequent data storage and retrieval processes for identifying and blocking the attacks. Hence, this type of AI-based feature learning helps enhance the system's security with accurate detection of attacks. Also, the AI-based attack learning process is carried out in this research based on the parameters of probabilistic distributional features. It identifies the multiple combinations of parameters for grouping and forming it to the cluster, ensuring a better prediction process. The PSL mechanism's key benefits are increased detection accuracy, ensuring data privacy, high security, minimal time consumption, and reduced computational complexity. These advantages are attained by performing AI-based feature learning with probabilistic features. The typical architecture of the PSL methodology with its matrix construction is depicted in Figure 3.

In this algorithm, the input data matrix M_{NID} is taken as the input for processing, and the predicted clustered results A_{ij}, R_{ij}, and C_{id} are produced as the output. Here, the availability and responsibility matrices are constructed at first with respect to the size of matrices S_i and S_j. Based on this, the initial clustering of data A_{ij} has been computed as shown in the following:

$$A_{ij} = \begin{cases} 0.5, & \text{if}\left(M_{\mathrm{NID}}(i,j) \le 0.5\right), \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Consequently, the responsibility and availability matrices are constructed for computing the relevant vector R_{ij} as represented as follows:

$$R_{ij} = \left\{ \begin{array}{cc} M_{\mathrm{NID}}(i,j) - A_{ij}, & \text{if}\left(A_{ij} \le M_{\mathrm{NID}}(i,j)\right) \\ 0, & \text{otherwise} \end{array} \right\}. \tag{8}$$

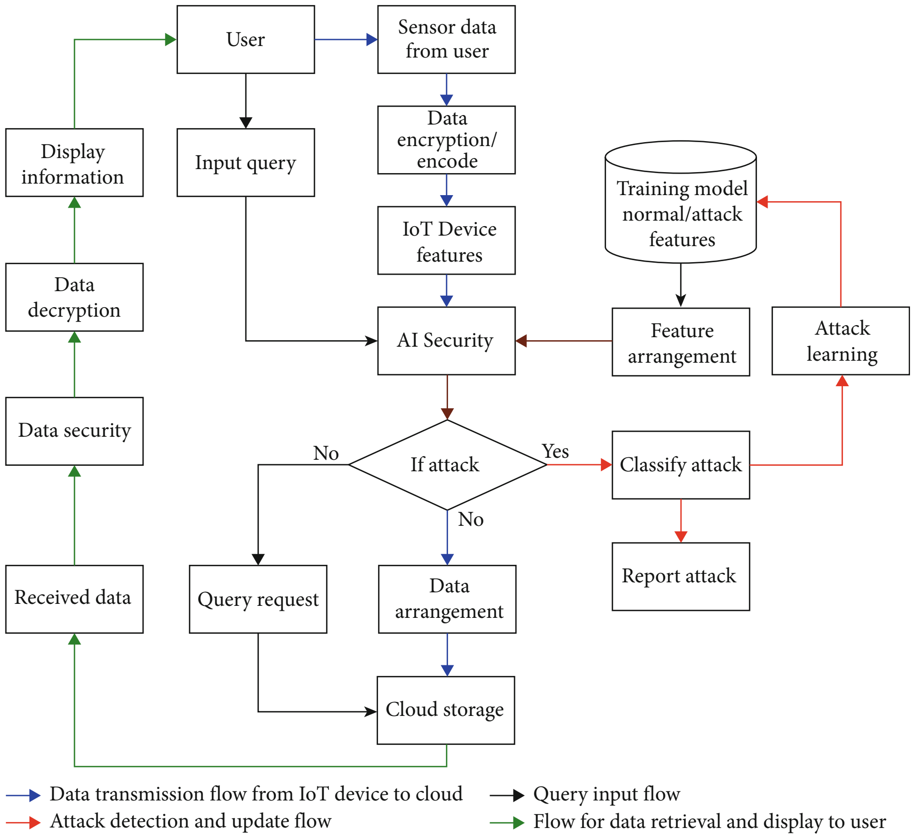

Figure 3: Overall flow of the proposed security system.

Then, the temporary matrix of R_{ij} is estimated and updated with the availability matrix, which is illustrated as follows:

$$\text{temp}_{Rij} = \begin{cases} \text{temp}_{Rij} + R_{ij}, & \text{if} \left(\text{temp}_{Rij} \leq 0 \right), \\ R_{ij}, & \text{otherwise}, \end{cases} \tag{9}$$

$$A_{ij} = \begin{cases} 0, & \text{if} \left(\text{temp}_{Rij} < 0 \right), \\ \text{temp}_{Rij}, & \text{otherwise}, \end{cases} \tag{10}$$

$$A_{ij} = \begin{cases} \text{temp}_{Rij}, & \text{if} \left(\text{temp}_{Rij} > 0 \right), \\ 0, & \text{otherwise}. \end{cases} \tag{11}$$

Consequently, the exponential matrix is formed with the average of relevant vector based on the estimated list index, which is further updated in the list as shown in the following:

$$\text{Exp}m_{ij} = \begin{cases} 1, & \text{if} \left(A_{ij} + R_{ij} \right) > 0, \\ 0, & \text{otherwise}, \end{cases} \tag{12}$$

$$\text{avg}_{\text{idx}} = \frac{1}{x} \sum_{x=1}^{\text{size}(\text{Idx}_{\text{ls}})} R_{i(\text{Idx}_x)}, \tag{13}$$

$$\text{avg}_{\text{list}} \longleftarrow \text{avg}_{\text{idx}}. \tag{14}$$

Then, the related average avg_R of overall vector is computed by using the following model:

$$\text{avg}_R = \frac{\sum_{j=1}^{S_j} R_{ij}}{S_j}. \tag{15}$$

Moreover, the distance is estimated between the average lists and its related parameter is updated as shown in the following:

$$\text{dis}_{ls} = \sqrt{\text{avg}_{\text{List}}^2 - \left(\text{avg}_R{}^2 \right)}, \tag{16}$$

$$\text{Update } C_{id} \longleftarrow \min \left(\text{dis}_{\text{ls}} \right). \tag{17}$$

Then, the clustered outputs are used to predict the classified L based on the minimum distance of parameters with relevancy levels. If the predicted clustered label is an attack, it is automatically blocked by the firewall, and the feature learning is carried out with the update of attacking features in the training model. Then, the updated model is further used for classifying the attacks for ensuring both the secure data storage and retrieval processes. Figure 4 shows the architecture model of the proposed PSL methodology.

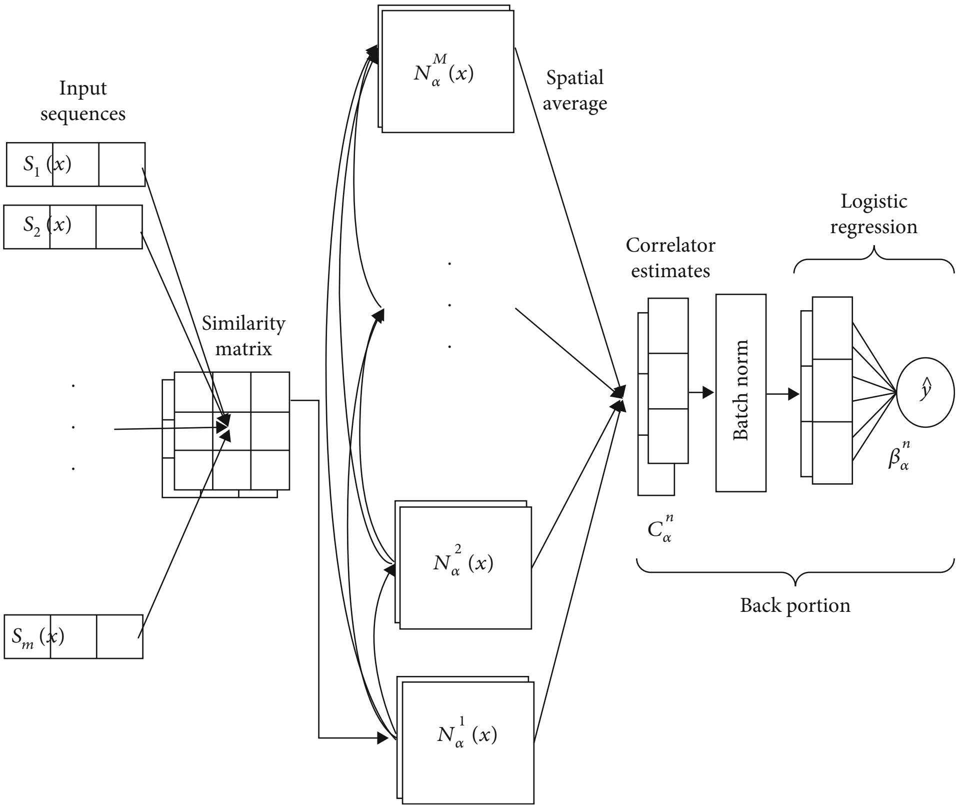

Figure 4: Architecture model of PSL methodology.

The detailed algorithmic steps involved in the proposed PSL-based feature learning model are illustrated in Algorithm 2 as follows:

4. Results and Discussion

This section evaluates the performance and comparative results of both existing and proposed security techniques based on accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), encryption time, decryption time, delay, throughput, packet delivery rate, and computational time.

4.1. Performance Analysis of Existing and Proposed AI Mechanisms. Figure 5 and Table 2 depict the throughput rate of both existing [22] and proposed AI security mechanisms for various IoT devices. Typically, the system's output can be assessed in terms of bytes. The network's output depends highly on the transmission rate of connected devices. Then, the throughput is calculated based on the ratio of the total number of messages created by all nodes of a network and the total number of messages that are successfully received. Here, the existing Securing Things in the Healthcare Internet (ST-HIoT), Intrusion Detection System (IDS), Intelligent Face Recognition and Navigation System (IFR-NS), and Internet of Things-Artificial Intelligence System (IoT-AIS). Based on the results, it is observed that the proposed PSL-RH technique outperforms the other techniques with increased throughput value because the proposed framework enables reliable data transmission between the users and devices by accurately detecting the attacks based on the set of features.

Figure 6 and Table 3 show the delay of existing and proposed techniques with respect to a varying number of IoT devices. Typically, the delay of the network is estimated based on the maximum amount of time required by the data to reach its destination ultimately, and the data rate amounts to the maximum flows are segregated based on the delay. It is also defined by the term of latency between the request sent by the user and the response provided by the cloud server. From the analysis, it is proved that the proposed PSL-RH techniques consume minimum delay when compared to the other techniques. Because, in the proposed system, the users' input query has been processed by checking the features of the request at the initial stage based on the training model. So, it helps to reduce the delay of input query transmission and data retrieval processes.

Figure 7 and Table 4 depict the transmission rate of existing IoT-AIS and proposed PSL-RH techniques with respect to various devices. Here, the data transmission rate is assessed between the flow of data from IoT device to cloud and retrieved data from the cloud to user with effective attack detection. Compared to the existing model, the proposed PSL-RH technique attained an increased data transmission rate with high security. Due to the maintenance of the trained feature model, the attacks are identified and blocked at the initial stage, which helps to improve the data transmission rate of the proposed system. Figure 8

```
Input: Input data matrix [IoT sensor matrix $(M_{NID})$]
Output: Predicted cluster output $A_{ij}$, $R_{ij}$, and $C_{id}$ and classified
        Label $L$
Step 1: Construct availability and responsibility matrices;
    Let consider, $S_i$ and $S_j$ be the size of matrix $(M_{\mathrm{NID}})$
    And set $K = 2$;
    Where $NID$ – Node ID
    For $i = 1$ to $S_i$
      For $j = 1$ to $S_j$
        Compute the initial clustering of data $A_{ij}$ by using
        Equation (7);
    End for $j$;
  End for $i$;
Step 2: Construct and update the responsibility and
    availability matrices;
    For $X_k = 1$ to $k$
      For $i = 1$ to $S_i$
        For $j = 1$ to $S_j$
          Compute the relevant vector $R_{ij}$ by using
          equation (8);
        End for $j$
      End for $i$
      For $i = 1$ to $S_i$
        For $j = 1$ to $S_j$
              Let $\mathrm{temp}_{R_{ij}} = 0$;
              For $m = 1$ to $S_i$
                    $\mathrm{temp}_{R_{ij}} = \mathrm{temp}_{R_{ij}} + R_{im}$;
                End for $m$;
                Compute $\mathrm{temp}_{R_{ij}}$ by using equation (9);
                If $(i! = j)$, then
                  Estimate $A_{ij}$ by using equation (10);
                Else
                  Estimate $A_{ij}$ by using equation (11);
                End if
        End for $S_j$
      End for $S_i$
    End for $X_k$
Step 3: Compute exponential matrix $\mathrm{Exp}m_{ij}$ and the average
    $A_{ij}$ of relevant vector $R_{ij}$ based on the estimated list
    index $\mathrm{avg}_{\mathrm{idx}}$ and update $\mathrm{avg}_{\mathrm{list}}$ in the list by using
    equations (12) to (14);
    For $y = 1$ to $S_j$
      Compute the related average of overall vector
      $\mathrm{avg}_R$ by using equation (15);
      Compute the distance list $\mathrm{dis}_{\mathrm{ls}}$ between the
      average list $\mathrm{avg}^2_{\mathrm{List}}$ and the related parameter
      $\mathrm{avg}_R{}^2$ by using equation (16);
      Update $C_{id}$ with the minimum of $\mathrm{dis}_{\mathrm{ls}}$ as shown
      in equation (17);
    End for $y$;
```

Algorithm 2: Continued.

```
Step 4: The classified label has been predicted based on the
    minimum distance of $A_{ij}$, $R_{ij}$, and $C_{id}$ of these
    matrices, as
    shown below:
    $L = \min\ (A_{ij}, R_{ij}, C_{id})$
    If (the predicted label $L$ is normal)
      Normal flow of data transmission can be enabled;
    Else if (attack)
      It can be automatically blocked by the firewall;
      The learning features of attacks with its
      characteristics are updated in the training model
      as shown below:
        UF = append$(A_F)$; //AF–attacking
        features in the trained model;
    End if;
```

Algorithm 2: PSL-based feature learning.

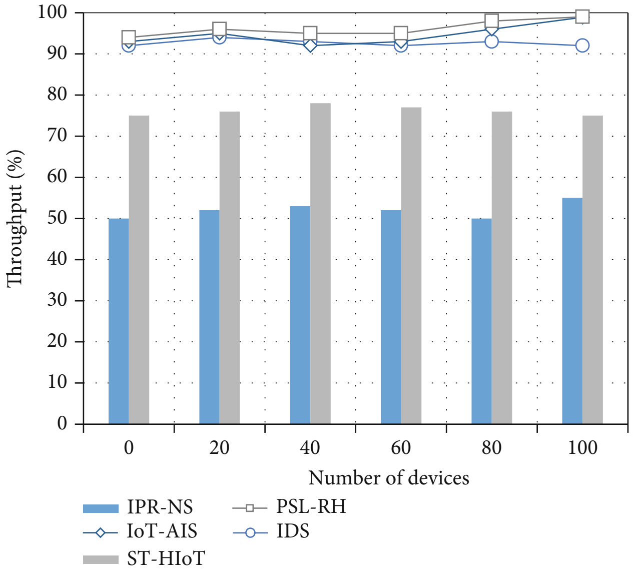

Figure 5: Throughput vs. number of devices.

Table 2: Throughput analysis of existing and proposed techniques.

Number of devices	IPR-NS	ST-HIoT	IDS	IoT-AIS	PSL-RH
0	50	75	92	93	94
20	52	76	94	95	96
40	53	78	93	92	95
60	52	77	92	93	95
80	50	76	93	96	98
100	55	75	92	98.9	99

and Table 5 compare the energy utilization level of both existing and proposed security mechanisms with respect to various devices. The energy usage of the network is assessed based on the communication delay of the IoT devices. These results also state that the proposed scheme requires minimal energy consumption when compared to the other technique.

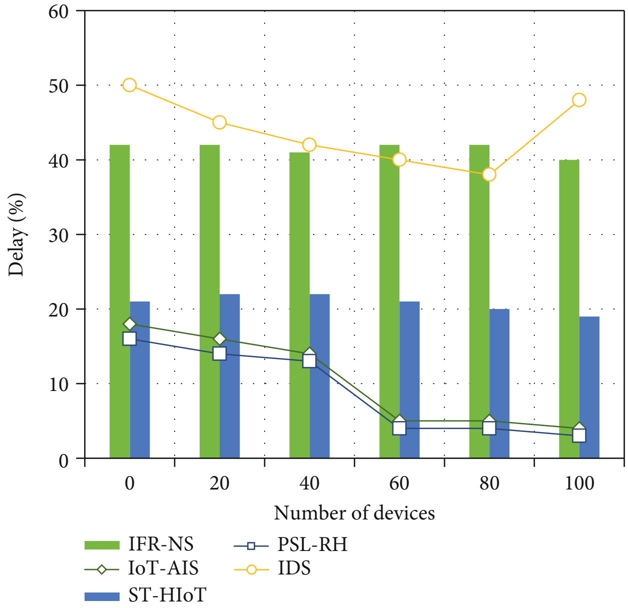

Figure 6: Delay vs. number of devices.

Table 3: Delay of existing and proposed techniques.

Number of devices	IFR-NS	ST-HIoT	IDS	IoT-AIS	PSL-RH
0	42	21	50	18	16
20	42	22	45	16	14
40	41	22	42	14	13
60	42	21	40	5	4
80	42	20	38	5	4
100	40	19	48	4	3

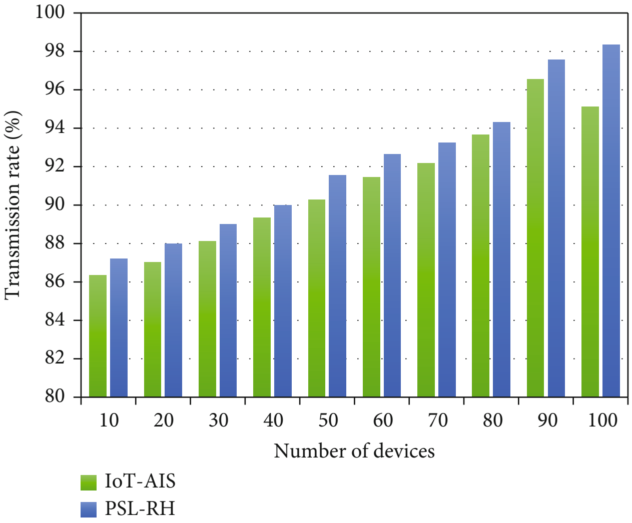

Figure 7: Transmission rate vs. number of devices.

Table 4: Transmission rate of existing and proposed techniques.

Number of devices	IoT-AIS	PSL-RH
10	86.34	87.21
20	87.02	88
30	88.13	89
40	89.33	90
50	90.27	91.56
60	91.45	92.64
70	92.18	93.25
80	93.67	94.31
90	96.56	97.56
100	95.11	98.35

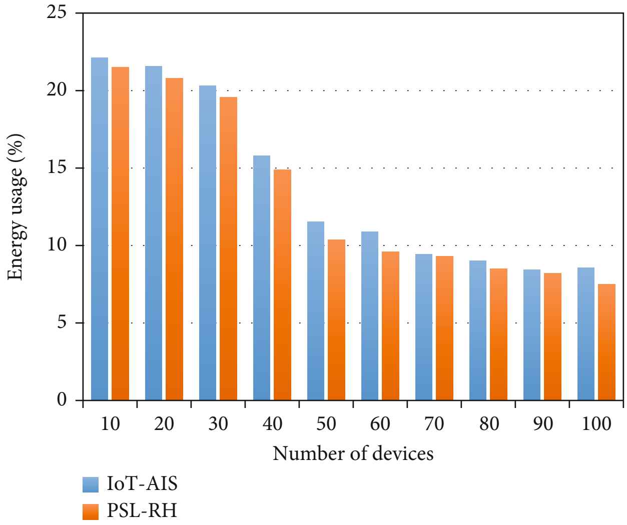

Figure 8: Energy usage vs. number of devices.

Table 5: Analysis of energy usage between existing and proposed techniques.

Number of devices	IoT-AIS	PSL-RH
10	22.11	21.5
20	21.56	20.8
30	20.32	19.56
40	15.78	14.9
50	11.52	10.36
60	10.89	9.6
70	9.45	9.32
80	9.02	8.5
90	8.44	8.2
100	8.56	7.5

Figure 9 and Table 6 compare the overall performance analysis of existing [37] and proposed attack detection techniques based on the measures of accuracy, precision, recall, F1-score, and MCC. Typically, the efficiency of the overall security system highly depends on the measures of accuracy, precision, and recall. Moreover, these measures are mainly computed to determine how the security scheme could actually predict the accurate values at the time of attack identification and prediction, which are calculated as follows:

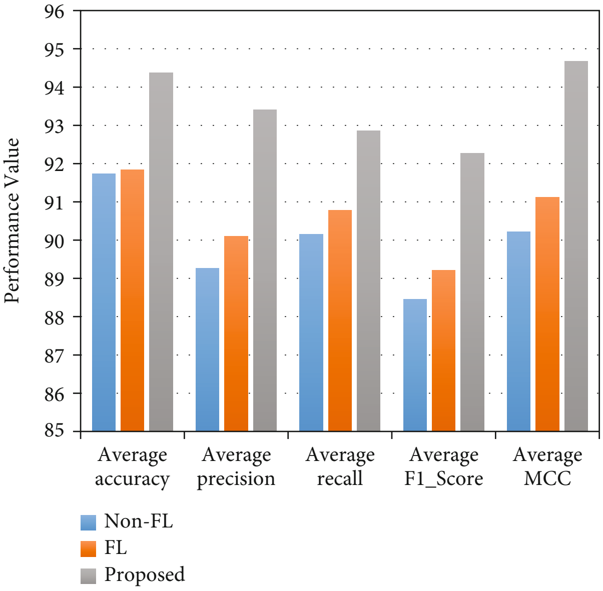

Figure 9: Overall comparative analysis of the existing and proposed techniques.

Table 6: Accuracy, precision, recall, F1-score, and MCC analysis.

	Methods		
Parameters	Nonfederated learning (non-FL)	Federated learning (FL)	PSL-RH
Average accuracy	91.73	91.846	94.377
Average precision	89.27	90.1	93.408
Average recall	90.15	90.785	92.861
Average F1_ score	88.46	89.207	92.274
Average MCC	90.22	91.127	94.672

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \tag{18}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \tag{19}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \tag{20}$$

$$\text{F1-score} = \frac{2\text{TP}}{2\text{TP} + \text{FP} + \text{FN}}, \tag{21}$$

$$\text{MCC} = \frac{\text{TP} \times \text{TN} - \text{FP} \times \text{FN}}{\sqrt{(\text{TP} + \text{FP})(\text{TP} + \text{FN})(\text{TN} + \text{FP})(\text{TN} + \text{FN})}}, \tag{22}$$

where TP indicates the true positive, TN represents the true negative, FP defines the false positive, and FN represents the false negative. Based on these results, it is evident that the proposed PSL-RH technique provides improved performance results compared to the other learning techniques by accurately detecting and blocking the attacks based on the trained model of feature set.

Figure 10 illustrates the Receiver Operating Characteristics (ROC) analysis of both existing and proposed techniques with respect to varying True Positive Rate (TPR) and False Positive Rate (FPR). Here, the ROC of the learning models is computed for validating the performance of attack detection process under different thresholds. Based on this analysis, it is evident that the proposed PSL-RH technique provides an increased TPR, when compared to the other learning models.

Figure 11 and Table 7 show the information entropy analysis of both existing [19] and proposed techniques under different samples. Typically, the information entropy has been measured based on the randomness of information, which is mainly evaluated for estimating the average uncertainty level of ciphertext. This analysis shows that the RH incorporated with the PSL technique could efficiently improve the information entropy by generating the random hash points during key generation.

Figure 12 and Table 8 evaluate the maximum, minimum, and mean values of the Number of Data Unit Change Range (NPCR) and Unified Average Changing Rate (UACI) for both existing and proposed security mechanisms. These measures are computed as follows:

$$\text{UACI} = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} \frac{|A_1(i,j) - A_2(i,j)|}{255} \times 100, \tag{23}$$

$$\text{NPCR} = \frac{1}{X \times Y} \sum_{i=1}^{X} \sum_{j=1}^{Y} B(i,j) \times 100, \tag{24}$$

$$B(i,j) = \begin{cases} 0, & A_1(i,j) = A_2(i,j), \\ 1, & A_1(i,j) \neq A_2(i,j), \end{cases} \tag{25}$$

where $A_1(i,j)$ and $A_2(i,j)$ are defined as the gray values of two ciphertext data at points (i,j). From the evaluation, it is observed that the proposed PSL-RH technique provides improved theoretical values of NPCR and UPCI, when compared to the existing techniques.

4.2. Performance Analysis of Existing and Proposed Data Security Techniques. Figure 13 and Table 9 show the encryption time of both existing [38] and proposed data security techniques for the varying number of IoT devices, including ECC, RSA, IECC, and proposed ECC-RH. Generally, the encryption time is defined by the amount of time taken for encrypting the original data into ciphertext using the generated key. Similarly, the decryption time is defined by the amount of time taken for decrypting the cipher data into original format, which is evaluated for both existing and proposed techniques, as shown in Figure 14 and Table 10. Based on these comparisons, it is stated that the proposed RH technique integrated with the ECC data security

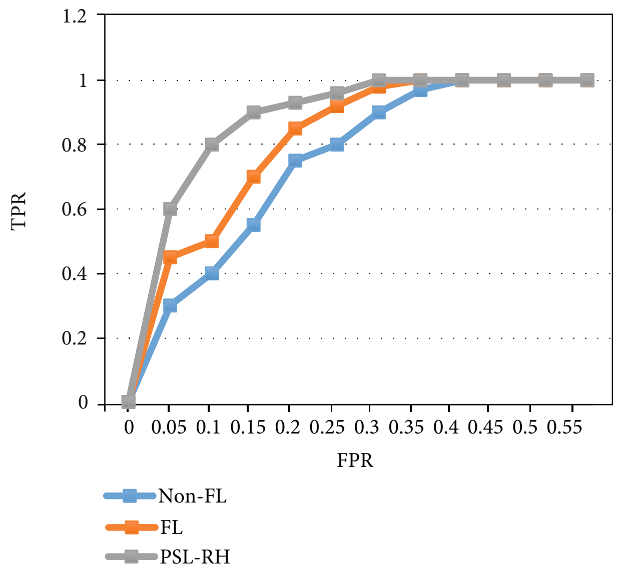

Figure 10: ROC analysis.

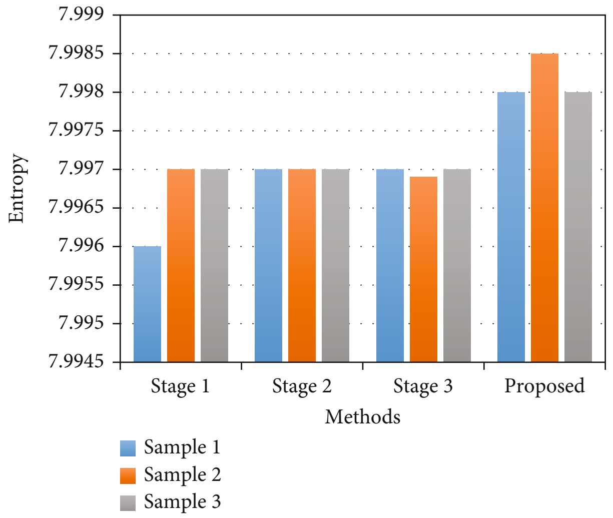

Figure 11: Analysis of entropy with respect to different samples.

Table 7: Entropy of existing and proposed techniques.

Data samples	Methods			
	Stage 1	Stage 2	Stage 3	PSL-RH
Sample 1	7.996	7.997	7.997	7.998
Sample 2	7.997	7.997	7.9969	7.9985
Sample 3	7.997	7.997	7.997	7.998

mechanism requires reduced time consumption for both data encryption and decryption. In the proposed data security scheme, the random key is generated for the input data stream based on the data matrix's random hash value and signature pattern. So, it helps to speed up the processes of data encryption and decryption with reduced time consumption.

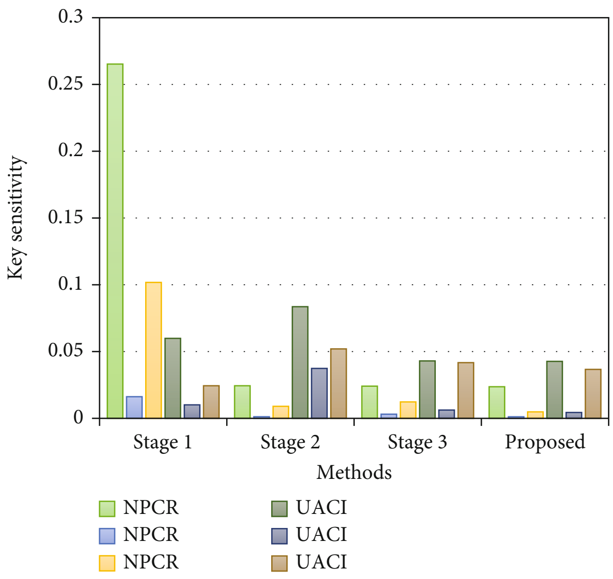

Figure 12: Key sensitivity analysis of existing and proposed techniques based on NPCR and UACI.

Table 8: Analysis of key sensitivity based on NPCR and UACI.

Parameters		Methods			
		Stage 1	Stage 2	Stage 3	PSL-RH
NPCR	Max	0.2653	0.0244	0.0241	0.02366
	Min	0.0162	0.0012	0.0031	0.001167
	Mean	0.1018	0.009	0.0123	0.004847
UACI	Max	0.0599	0.0836	0.043	0.042667
	Min	0.0101	0.0374	0.0062	0.0044
	Mean	0.0244	0.052	0.0417	0.036667

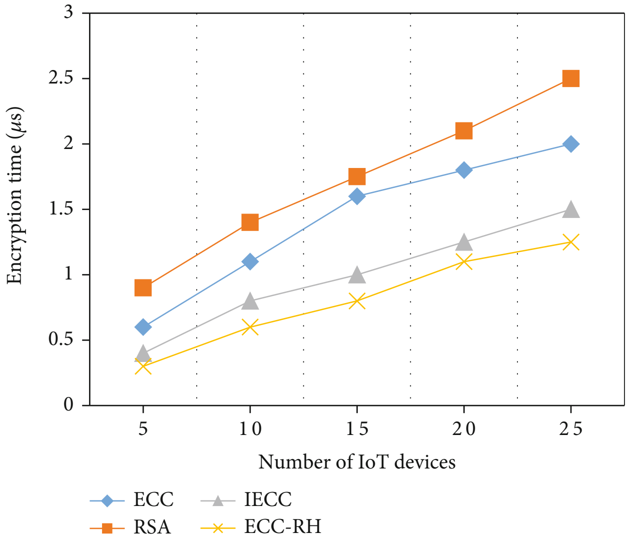

Figure 13: Encryption time vs. number of IoT devices.

Table 9: Encryption time of existing and proposed techniques.

Number of IoT devices	ECC	RSA	IECC	ECC-RH
5	0.6	0.9	0.4	0.3
10	1.1	1.4	0.8	0.6
15	1.6	1.75	1	0.8
20	1.8	2.1	1.25	1.1
25	2	2.5	1.5	1.25

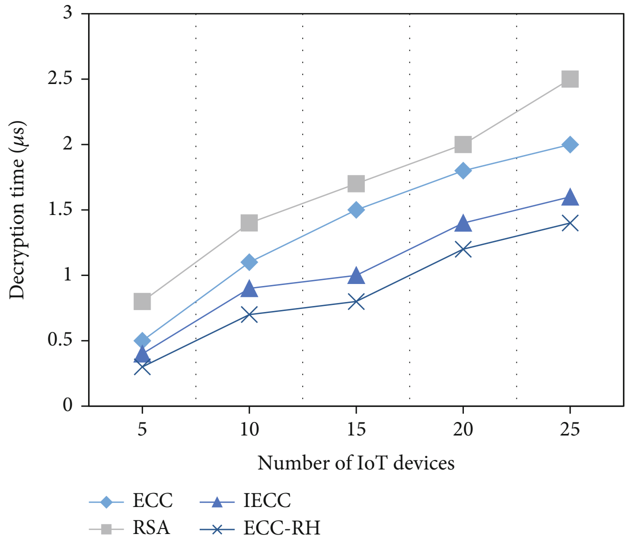

Figure 14: Encryption time vs. number of IoT devices.

Table 10: Encryption time of existing and proposed techniques.

Number of IoT devices	ECC	RSA	IECC	ECC-RH
5	0.5	0.8	0.4	0.3
10	1.1	1.4	0.9	0.7
15	1.5	1.7	1	0.8
20	1.8	2	1.4	1.2
25	2	2.5	1.6	1.4

Consequently, Figure 15 and Table 11 compare the encryption and decryption time of both existing Advanced Encryption Standard (AES), Ciphertext Policy Attribute-Based Encryption (CP-ABE), Modified CP-ABE (MPC-ABE) [39], and proposed ECC-RH techniques with respect to varying key size (bits). Then, Figure 16 and Table 12 show the decryption time of both existing and proposed data security techniques with respect to different key sizes. The obtained results depict that the proposed ECC-RH technique requires the minimal time consumption for both encryption and decryption, when compared to the other existing data security techniques.

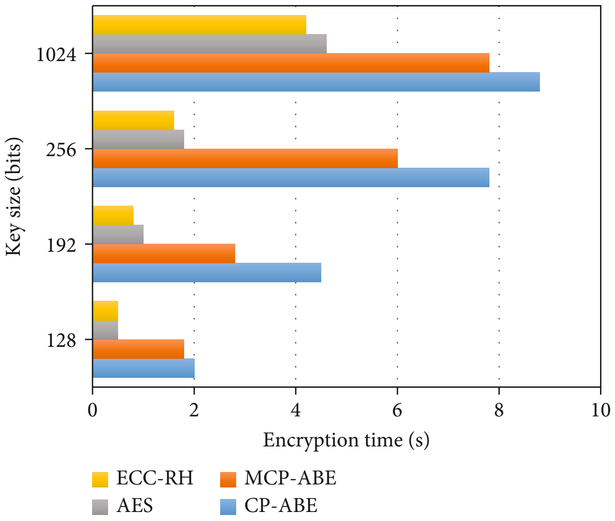

Figure 15: Encryption time vs. key size (bits).

Table 11: Encryption time of existing and proposed data security techniques.

Key size (bits)	CP-ABE	MCP-ABE	AES	ECC-RH
128	2	1.8	0.5	0.5
192	4.5	2.8	1	0.8
256	7.8	6	1.8	1.6
1024	8.8	7.8	4.6	4.2

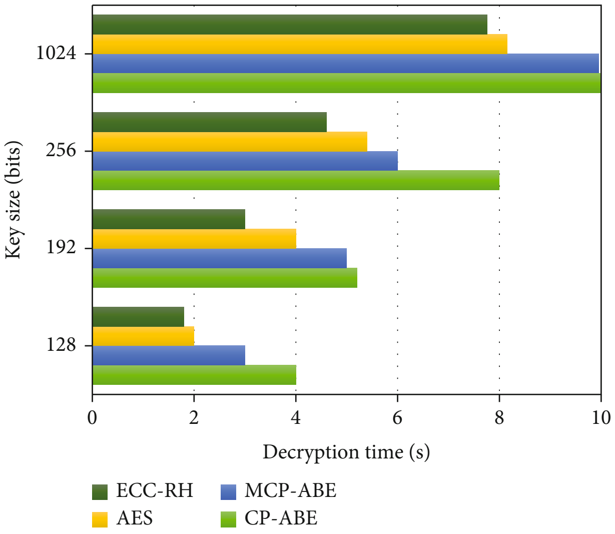

Figure 16: Decryption time vs. key size (bits).

Figure 17 and Table 13 show the average computation time of both existing and proposed data security techniques with respect to a varying number of users. Typically, the computational time is defined based on the amount of time taken by the system to fulfill the user request until the data retrieval is successfully completed. This analysis proves that the proposed ECC-RH technique requires the reduced computational time(s), when compared to the other data security mechanisms by completing the data storage and retrieval processes with increased speed and security. Then, it shows the improved performance rate of the overall AI-based security system deployed in an IoT-cloud environment.

Table 12: Decryption time of existing and proposed data security techniques.

Key size (bits)	CP-ABE	MCP-ABE	AES	ECC-RH
128	4	3	2	1.8
192	5.2	5	4	3
256	8	6	5.4	4.6
1024	12.2	10	8.2	7.8

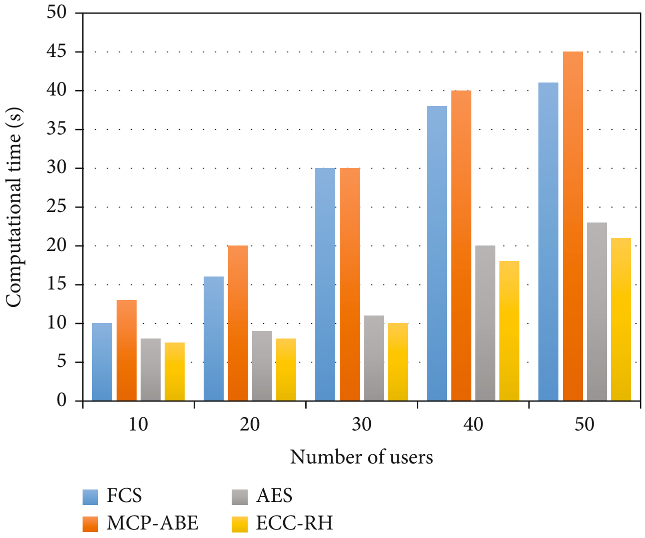

Figure 17: Computation time vs. number of users.

Table 13: Computation time of existing and proposed data security techniques.

Number of users	FCS	MCP-ABE	AES	ECC-RH
10	10	13	8	7.5
20	16	20	9	8
30	30	30	11	10
40	38	40	20	18
50	41	45	23	21

5. Conclusion

This paper presents an intelligent AI-based security system for ensuring the privacy and confidentiality of healthcare applications in an IoT-cloud environment. The main aim of this work is to enable the secured data storage and retrieval processes by implementing an advanced AI methodology. For this purpose, the PSL technique is proposed that intends to predict the attacks in an earlier stage. This ensures the healthcare application system's increased security by training the model with the set of learned features. Consequently, the RH-based key generation process is implemented and incorporated with the ECC mechanism for ensuring secured data storage and retrieval processes. The novel contributions of this AI methodology are that it maintains a trained data model with the set normal and attack features that help identify the attacks at the initial stage of processing. Also, it blocks the attack by reporting to the firewall and updates the trained model by appending the features and characteristics of the detected attack. Also, the data security process could be improved by generating the random key based on the data matrix's hash value and signature pattern. Then, this random key can be used for data encryption and decryption processes, which guarantees secured data storage and retrieval in an IoT-cloud environment. The significant advantages of the proposed AI-based security mechanism are reduced computational complexity, fast process, minimal time consumption, accurate attack detection, and optimal performance outcomes. The proposed AI-based security mechanism results are validated and compared with the existing feature learning, classification, and data security models using various evaluation metrics during the performance analysis. Based on the obtained results, it is stated that the proposed PSL-RH technique outperforms the other techniques with improved performance results.

In the future, this work can be extended by implementing the AI-based security framework to some other real-time application systems. Also, lightweight security models can be developed for ensuring the security of healthcare IoT data based on the processes of random key generation and trust agreement.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors have no potential conflicts of interest, such as financial interests, affiliations, or personal interests or beliefs, that could be perceived to affect the objectivity or neutrality of the manuscript.

Acknowledgments

This project was funded by the Deanship of Scientific Research (DR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia, under grant no. (RG-4-611-43). The authors, therefore, acknowledge with thanks the DSR for technical and financial support.

References

[1] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: a survey," *Security and Communication Networks*, vol. 2020, 13 pages, 2020.

[2] E. Mohamed, "The relationship between artificial intelligence and internet of things: a quick review," *Journal of Cybersecurity and Information Management*, vol. 1, no. 1, pp. 30–34, 2020.

[3] M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud, “Sensors of smart devices in the internet of everything (IoE) era: big opportunities and massive doubts,” *Journal of Sensors*, vol. 2019, 26 pages, 2019.

[4] Z. Ahmed, K. Mohamed, S. Zeeshan, and X. Dong, “Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine,” *Database*, vol. 2020, 2020.

[5] K. Saleem, I. S. Bajwa, N. Sarwar, W. Anwar, and A. Ashraf, “IoT healthcare: design of smart and cost-effective sleep quality monitoring system,” *Journal of Sensors*, vol. 2020, 17 pages, 2020.

[6] M. Anuradha, T. Jayasankar, N. Prakash et al., “IoT enabled cancer prediction system to enhance the authentication and security using cloud computing,” *Microprocessors and Microsystems*, vol. 80, article 103301, 2021.

[7] J.-X. Hu, C.-L. Chen, C.-L. Fan, K. H. Wang, and K.-H. Wang, “An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing,” *Journal of Sensors*, vol. 2017, 11 pages, 2017.

[8] G. B. Mohammada, S. Shitharthb, and P. R. Kumarc, “Integrated machine learning model for an URL phishing detection,” *International Journal of Grid and Distributed Computing*, vol. 14, no. 1, pp. 513–529, 2020.

[9] S. S. Gill, S. Tuli, M. Xu et al., “Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: evolution, vision, trends and open challenges,” *Internet of Things*, vol. 8, article 100118, 2019.

[10] S. Shakya, “An efficient security framework for data migration in a cloud computing environment,” *Journal of Artificial Intelligence*, vol. 1, no. 1, pp. 45–53, 2019.

[11] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, “Efficient and privacy-enhanced federated learning for industrial artificial intelligence,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6532–6542, 2019.

[12] T. Hidayat and R. Mahardiko, “A systematic literature review method on aes algorithm for data sharing encryption on cloud computing,” *International Journal of Artificial Intelligence Research*, vol. 4, no. 1, pp. 49–57, 2020.

[13] S. Shitharth, N. Satheesh, B. P. Kumar, and K. Sangeetha, “IDS detection based on optimization based on WI-CS and GNN algorithm in SCADA network,” in *Architectural Wireless Networks Solutions and Security Issues*, Springer, Singapore, 2021.

[14] R. Aluvalu, V. U. Maheswari, K. K. Chennam, and S. Shitharth, “Data security in cloud computing using Abe-based access control,” in *Architectural Wireless Networks Solutions and Security Issues*,Springer, Singapore.

[15] K. Huang, “Accountable and revocable large universe decentralized multi-authority attribute-based encryption for cloud-aided IoT,” *IEEE Access*, vol. 9, pp. 123786–123804, 2021.

[16] J. H. Anajemba, C. Iwendi, M. Mittal, and T. Yue, “Improved advance encryption standard with a privacy database structure for IoT nodes,” in *In 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 201–206, Gwalior, India, 2020.

[17] K. Rangaraj, V. Veerasamy, and V. Sumathi, “Protection of mental healthcare documents using sensitivity-based encryption,” *International Journal of Cloud Computing*, vol. 10, no. 1–2, pp. 90–100, 2021.

[18] J. Patel, F. Suthar, and S. V. Khanna, “A critical analysis on encryption techniques used for data security in cloud computing and IOT (internet of things) based smart cloud storage system: a survey,” *International Journal of Scientific Research in Network Security and Communication*, vol. 7, no. 2, pp. 101–103, 2019.

[19] B. Li, Y. Feng, Z. Xiong, W. Yang, and G. Liu, “Research on AI security enhanced encryption algorithm of autonomous IoT systems,” *Information Sciences*, vol. 575, pp. 379–398, 2021.

[20] S. L. Nita and M. I. Mihailescu, “On artificial neural network used in cloud computing security-a survey,” in *In 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–6, Iasi, Romania, 2018.

[21] N. Khandare, O. Dalvi, V. Nikam, and A. Pandit, “Enhancing privacy and security in medical information with AES and DES,” in *In International Conference on Intelligent Computing and Smart Communication 2019*, Springer, Singapore, 2020.

[22] T. M. Ghazal, “Internet of things with artificial intelligence for health care security,” *Arabian Journal for Science and Engineering*, vol. 2, no. 1, pp. 1–12, 2021.

[23] M. R. Valanarasu, “Smart and secure IoT and AI integration framework for hospital environment,” *Journal of ISMAC*, vol. 1, no. 3, pp. 172–179, 2019.

[24] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, “Trends in IoT based solutions for health care: moving AI to the edge,” *Pattern Recognition Letters*, vol. 135, pp. 346–353, 2020.

[25] H. K. Bharadwaj, A. Agarwal, V. Chamola et al., “A review on the role of machine learning in enabling IoT based healthcare applications,” *IEEE Access*, vol. 9, pp. 38859–38890, 2021.

[26] S. Zaman, K. Alhazmi, M. A. Aseeri et al., “Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey,” *IEEE Access*, vol. 9, pp. 94668–94690, 2021.

[27] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, “A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment,” *Future Generation Computer Systems*, vol. 78, pp. 1005–1019, 2018.

[28] C. Choi and J. Choi, “Ontology-based security context reasoning for power IoT-cloud security service,” *IEEE Access*, vol. 7, pp. 110510–110517, 2019.

[29] M. Shen, B. Ma, L. Zhu, X. Du, and K. Xu, “Secure phrase search for intelligent processing of encrypted data in cloud-based IoT,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1998–2008, 2018.

[30] Y. Mo, “A data security storage method for IoT under Hadoop cloud computing platform,” *International Journal of Wireless Information Networks*, vol. 26, no. 3, pp. 152–157, 2019.

[31] Y. Winnie, E. Umamaheswari, and D. Ajay, “Enhancing data security in IoT healthcare services using fog computing,” in *In 2018 International Conference on Recent Trends in Advance Computing (ICRTAC)*, pp. 200–205, Chennai, India, 2018.

[32] K. Riad, R. Hamza, and H. Yan, “Sensitive and energetic IoT access control for managing cloud electronic health records,” *IEEE Access*, vol. 7, pp. 86384–86393, 2019.

[33] Y. Guan, J. Shao, G. Wei, and M. Xie, “Data security and privacy in fog computing,” *IEEE Network*, vol. 32, no. 5, pp. 106–111, 2018.

[34] S. Zhu, V. Saravanan, and B. Muthu, “Achieving data security and privacy across healthcare applications using cyber security mechanisms,” *The Electronic Library*, vol. 38, no. 5-6, pp. 979–995, 2020.

[35] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in internet of things using the optimum authentication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.

[36] D. Sadhukhan, S. Ray, G. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *The Journal of Supercomputing*, vol. 77, no. 2, pp. 1114–1151, 2021.

[37] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated learning-based anomaly detection for IoT security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, 2021.

[38] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027, 2020.

[39] S. Atiewi, A. Al-Rahayfeh, M. Almiani et al., "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography," *IEEE Access*, vol. 8, pp. 113498–113511, 2020.