The Development of an AI-Based Network Security Algorithm for an IoT Healthcare Platform

Keith Lungile Ncube[1], Mainford Mutandavari[2]

[1]MTech. Cloud Computing, Harare Institute of Technology
Email: *h200025q[at]hit.ac.zw*

[2]Department of Software Engineering, Harare Institute of Technology
Email: *mmutandavari[at]hit.ac.zw*

Abstract: ***The Internet of things is made up of all IPv6-capable hardware that is linked to and communicates with one another via the Internet. Our civilization uses this common phenomenon on a daily basis. Two of the main obstacles in large-scale IoT installations are data privacy and security. This is especially true for important applications like Industry 4.0 and e-healthcare. Securing the IoT-cloud ecosystem for healthcare data is one of the hardest and tough issues of today. The IoT Cloud infrastructure is particularly susceptible to flaws and attacks because of the numerous sensors utilized to produce enormous amounts of data. This can make the network less secure. The finest technology for healthcare applications is artificial intelligence (AI), as it provides the best method for enhancing data security and reliability. The IoT cloud framework already uses a number of AI-based security mechanisms. Significant flaws in existing algorithms include complicated algorithm design and ineffective data processing. Additionally, they are unsuitable for analyzing unstructured data, which raises the price of IoT sensors. In order to improve the security and privacy of healthcare data stored in IoT clouds, this study introduces Probabilistic Super Learning (PSL) and Random Hashing (RH), two AI-based intelligence feature learning mechanisms. This research also employs the suggested learning approach to reduce the price of IoT sensors. The initial assault is discovered using this training model. The attack's properties are then changed in order to learn how attacks operate. Additionally, the data matrix's hash values are used to generate the random key. Elliptic Curve Cryptography is linked with this method for data security. The upgraded ECC-RH technique uses randomly generated hash keys to encrypt and decode data. Performance evaluation compares and validates the outcomes of various methodologies. A secure network layer is provided for IoT apps connected across 5G networks and beyond in the context of the final analysis of bio-inspired algorithms.***

Keywords: Cloud Computing, Healthcare System, 5th Generation Network; Artificial Intelligence; Biological; Internet of Things (IoT); Network layer; Security; Wireless Sensor Networks

1. Introduction

Artificial Intelligence (AI) is an important technology in modern-day applications, especially those implementing the Internet of Things, (IoT). This is a framework that connects different sensors and devices to the cloud. This enables machine-to-machine (M2M), and machine-to-human (M2H) communication amongst other types of communication. IoT applications are autonomous and have increased efficiency hence the increased interest in recent years. The IoT device can gather data from various sources and transmit it to connected devices. These devices pass the information on to the cloud using wireless links. The vulnerabilities and other attacks that can be made to the network make this process difficult. To protect confidential information's safety, security is an important concern in the cloud environment. AI technology is better suited to improving security for healthcare applications that are hosted in cloud IoT environments. However, having mentioned the advantages of AI techniques above, it also has pitfalls such as scalability, interoperability, heterogeneity, and connectivity. These challenges are taken into account when developing a lightweight IoT solution.

This paper discusses the implementation of a patient monitoring system hardware prototype, which has a mobile client-side application. The system sends patient data to a cloud-hosted server which stores and secures this data. A security model is then developed which is tested on this system to demonstrate the security of data in transit and at rest.
The figure below illustrates the types of AI techniques:

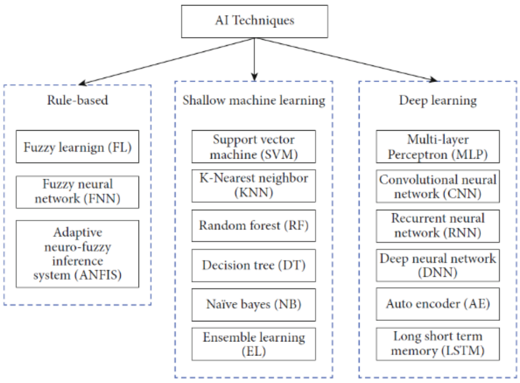

AI Techniques
Rule-based
Shallow machine learning
Deep learning
Fuzzy learnign (FL)
Fuzzy neural network (FNN)
Adaptive neuro-fuzzy inference system (ANFIS)
Support vector machine (SVM)
K-Nearest neighbor (KNN)
Random forest (RF)
Decision tree (DT)
Naïve bayes (NB)
Ensemble learning (EL)
Multi-layer 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.

Figure 1

1.1. Background to the problem

Data security in healthcare IoT systems is a major concern, an impediment, and a serious inhibitor. Since IoT utilization has increased exponentially in recent years, data security, all the most become important. Data prejudice or change or modification has critical consequences in healthcare IoT systems. Lives can be lost if this data is tempered with, worse deleted. It is critical to provide lightweight security to the system since IoT devices are resource constrained and specific to a certain OEM.

1.2 Statement of the problem

Securing the resource-constrained, low-power utilization IoT healthcare system is a challenge and this poses dire consequences to human life if left unchecked.

1.3 Aim

To develop and implement a lightweight network security algorithm in an IoT cloud-based healthcare platform.

1.4 Objectives

- To design and implement a patient monitoring platform that allows doctors to remotely monitor a patient's health.
- To develop a mobile application to be used by the patient.
- To secure data transmission and retrieval from the IoT system into the cloud platform.

1.5. Research questions

- How does a patient monitoring platform work and what are its main components of it?
- How will the mobile application be designed and interface with the patient monitoring platform, and which parameters will be shared, monitored, and secure?
- Which security algorithm will be implemented to secure the healthcare system and justify the choice?
- How is secure data transmission from IoT into the cloud established?
- How is data retrieval guaranteed?

2. Literature Review

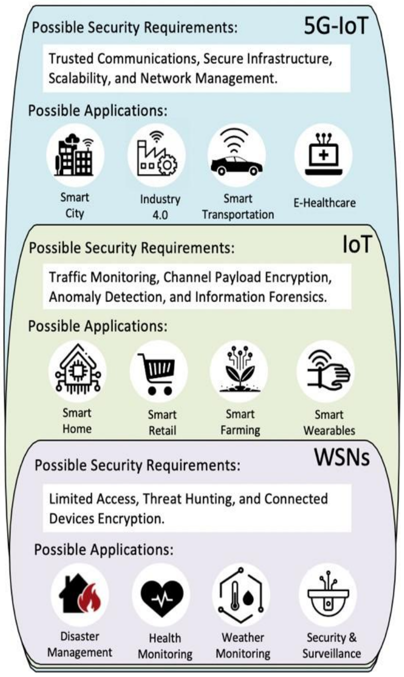
This chapter will offer a critical evaluation of earlier studies on the subject that have been published in the literature. A thorough examination of prior studies and discussions that are pertinent to a topic or field of study is known as a literature review. This chapter's objective is to deliver that data in writing.

2.1 Related Works

In relation to AI-based security plans for IoT systems, this section examines several traditional security procedures. Additionally, it examines each technique's benefits and drawbacks in light of its functional aspects and traits.
Ghazal [22] has created an IoT framework with an AI system that will guarantee security for apps used in the healthcare industry. The paper's major objective was to safeguard the privacy and security of patient data that was stored online. For this, a Deep Neural Network (DNN) malware detection system was created. This permits only approved access to cloud data in order to stop the malicious or illegal behaviour. Using the bias and weight settings, key authentication was also carried out. The sigmoid functions were computed for training the set of extracted features and identifying malware. Fewer delays, faster packet delivery, and shorter reaction times are just a few of the major advantages of this work. A secure IoT framework was created for hospital security by Valanarasu [23]. Some of the fundamental rules and guidelines governing AI technology, such as accountability and transparency, data security and privacy, interoperability, and sustainability, can be incorporated using the framework. It also focuses on the identification of various attack types based on host characteristics, information disturbances, and network characteristics. The framework doesn't employ any special techniques for identifying network assaults. The system as a whole performs worse as a result. Greco et al. [24] investigated the most recent IoT AI systems trends to develop smart healthcare systems. WBSN, field sensor networks, and cloud services were combined to build the three-tier architecture for the Internet of Medical Things.

2.2 Security Requirements in the Network Layer of IoT-over-5G

Fig.1 [27]. In IoT applications, it is crucial to evaluate and address network layer security issues. This makes it possible for businesses and developers to suggest and execute the finest IoT-based solutions. [28] offers a mobile gateway-based remote health solution for the Body Sensor Network that functions as a router (BSN). The body sensors automatically record information about the patient's vital signs, such as their position (through a GPS sensor), heart rate (via an optical pulse sensor), and potential fall detection (via an accelerometer sensor). Data are transmitted to AMBRO (storage side), a platform for real-time analysis and appropriate response in emergency situations, such as an intelligent personal assistant (IPA). Data routing security is essential in this scenario to safeguard sensitive data against fraud. To safeguard the security of data routing between AMBRO and BSN, the authors of [29] advise utilizing the ECG-based Multiple Fiducial points-based Binary Sequence Generation (MFBSG) data encryption technique.


Possible Security Requirements:
5G-IoT
Trusted Communications, Secure Infrastructure, Scalability, and Network Management.
Possible Applications:
Smart City
Industry 4.0
Smart Transportation
E-Healthcare
Possible Security Requirements:
IoT
Traffic Monitoring, Channel Payload Encryption, Anomaly Detection, and Information Forensics.
Possible Applications:
Smart Home
Smart Retail
Smart Farming
Smart Wearables
Possible Security Requirements:
WSNs
Limited Access, Threat Hunting, and Connected Devices Encryption.
Possible Applications:
Disaster Management
Health Monitoring
Weather Monitoring
Security & Surveillance

It is critical that security requirements are recognized and vulnerabilities in IoT applications are fixed as IoT technologies and IoT services evolve. The security needs and vulnerabilities for IoT architectural layers are described in [33]. (Application Network and Edge). There are many services and tasks that fall under the purview of the application layer. Typically, APIs are used to carry out functionalities. The current generation of IoT devices blindly accept any third-party service provider, even if they are shown to have security weaknesses like weak authentication or unreliable service. As a result, the application layer should have a secure API, application verification, and information forensics. The network layer then controls data flow and aids IoT apps in gathering a lot of data. Traffic shaping, channel encryption, and traffic monitoring are essential components of the network layer. It is the layer that carries out the communication between end-point devices and IoT environments. Data encryption, threat detection, restricted accessibility, and minimal authentication are all requirements for this layer. The facts produced at the edge are significant, delicate, and priceless.

2.3 Current 5G Network Security Approaches for IoT Applications

The development of 5G-IoT systems must prioritize network security and privacy. Users' trust, confidence, and personal safety may be impacted by this invention [52]. Recent studies have concentrated on the problem by putting out several strategies to safeguard customer privacy and apply network layer security.

A service-oriented authentication method that allows network slicing is described in [53]. (ES3A). The network's basic architecture can efficiently share resources across a number of services thanks to network slicing. Users can use IoT services anonymously without disclosing the slice or service type thanks to the privacy-preserving slice selection method. To enable secure access to service data, a three-party session key negotiation method was added between regional fog nodes and IoT servers. However, the security algorithm design of the given authentication framework is lacking. In order to guarantee a secure connection between the IoT server and end users, a correct simulation result is also necessary.

2.4 Bio-Inspired techniques to address 5G Network Layer Security for IoT applications

Bio-inspired cybersecurity is crucial in defending the network layer against numerous dangers. [21]. To secure the 5G IoT, it is crucial to acquire and enhance these bio-inspired security methods. The limitations of security infrastructure include its lack of self-awareness, inability to communicate with other network devices, and absence of self-correcting processes. Because of this, it's important to create bio-inspired algorithms that are capable of navigating the constraints of cyberspace [21]. It's crucial to set up networks of assistance and communication for hackers, cybercriminals, and other oddities.

Systems with biological inspiration are renowned for their capacity to adjust to shifting circumstances and for being resistant to damage. Defense algorithms with biological inspiration may be more efficient in tackling challenging cybersecurity issues. Anti-virus software and honeypots are two instances of cybersecurity technology that use bioinspired methodologies. The use of bio-inspired communications and networking approaches has been the subject of numerous studies that have improved cybersecurity.

3. Methodology

This section provides a detailed explanation of the suggested methodology along with the flow and algorithmic illustrations. The major goal of this study is to use cutting-edge AI algorithms to safely store and retrieve data from IoT cloud platforms. Applications based on healthcare are also taken into account. The suggested architecture makes use of the Probabilistic Super Learning Model (PSL), which is based on AI and enables secure data transfer. The characteristics of the data from IoT devices are identified using this model. The PSL approach uses the most recent features to distinguish between legitimate and malicious activity.

The AI model-based PSL technique can enhance feature learning by changing the attributes and traits of each assault. Elliptic Curve Cryptography (ECC) uses Random Hashing (RH), a method that employs random hashing, to carry out the data encryption and decryption procedures. This guarantees the safety of data during storage and retrieval.

The following stages are depicted in Figures 1 and 2, which represent the architecture and flow of the AI-based security systems, respectively.

1) Transmission of data from IoT and cloud
2) Input processing of user query
3) Feature-learning and attack detection
4) Secure data retrieval via the cloud to the user

At first, sensor data from users has been collected and encrypted. Then, using the RH method, it will be kept in the cloud. Using a hash-key generation matrix, it is utilized to encrypt and decrypt the original data. The data is then examined by an AI security system to determine if it is trustworthy or harmful. It might be the usual course of events. In this instance, the data organization procedure is carried out in preparation for cloud storage. The data arrangement procedure can be used to store the data in the cloud if the attack is discovered.

The training model has been updated using PSL approach. The properties are updated, and the features are arranged accordingly. The most recent characteristics or features of the training model data are used in this classification. To get the requested data during query input processing, the user can enter the input query. The AI-PSL is used to assess whether the user is a legitimate user or an attacker based on the model's updated attributes. The query request has been forwarded to cloud storage if the user is not an attacker. It will get the encrypted information. Here, the original data is decrypted using the RH-based encryption procedure, and a signature-matching pattern is produced. The user would be able to view all the privacy and security settings along with the encrypted data.

Licensed Under Creative Commons Attribution CC BY

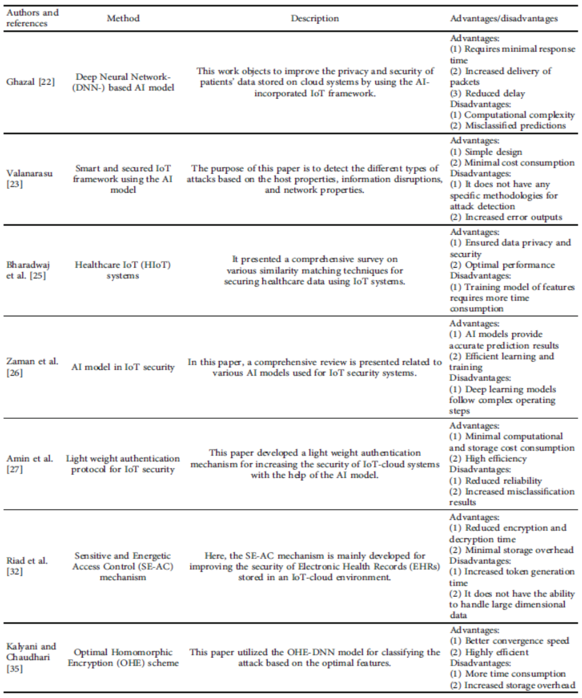
3.1 Data Security with ECC-Based Random Hashing

Prior to being saved in the IoT Cloud at this level, the original data must be encrypted using the RH technique. Due to a large amount of data and intricate feature configurations in many security systems, data security is a challenging and demanding procedure. Data security can be defined as the secure storage of data prior to encryption and the recovery of data following decryption. The data can be accessed thanks to this authentication. There are several methods of data encryption because of this. Decryption standards have also been defined in standard works using models like AES, DES, RS4, and others. The drawbacks of this include increased processing overhead, difficult implementation, and lengthier key generation and encryption times.

This paper combined the RH key-generating method with an Elliptic Curve Cryptography (ECC) based encryption system [36]. Data security is achieved using this ECC/RH, which is based on encryption and decryption. One of the most popular encryption technologies for enhancing data security in the cloud and IoT is ECC. The ECC's key generation procedure is replaced by the RH method. In this concept, a random key was constructed using the hash value and the input data stream. The encryption and decryption of cloud data both require this key. The random hashing-based ECC technique's key benefits are that it is compact, offers quick encryption and decryption, and uses less bandwidth. The algorithm employs a number of calculations to generate the hash function in order to provide a higher level of security.

At first, it receives the data streams and generates the RV of random key points. These are employed in the encrypting and decrypting of data. The temporary matrix and weight parameters are initialized in this way. The hash keys matrix is made using these. Then, for each counter iteration, the sequence parameters S1 and S2 are modified.

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

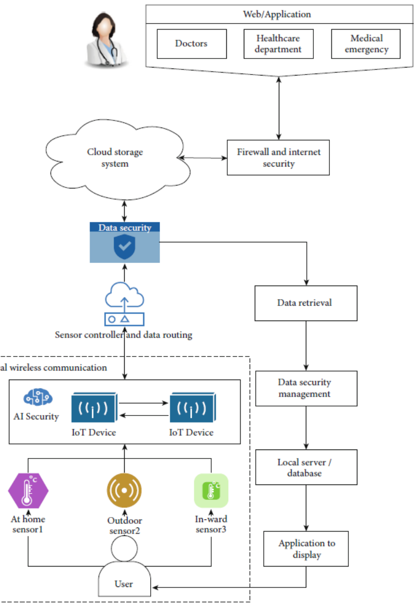


Figure 2: Architecture model of the proposed AI-based healthcare data security scheme in IoT-cloud.

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

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

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, as follows, the resulting matrix is used to calculate the signature pattern h_q:

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

As a result, the count has been adjusted for the matrix's size, and the estimated patterns are shown as follows.:

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

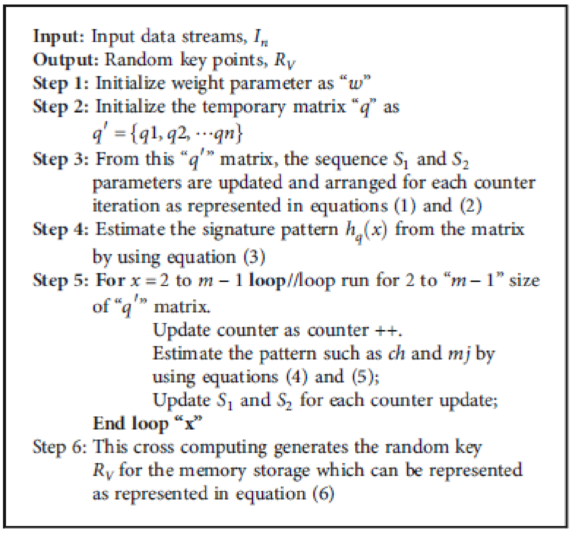
$$mj = \mathrm{XOR}(\mathrm{XOR}(\mathrm{AND}(q[1], q[2]), \mathrm{AND}(q[1], q[3])), \mathrm{AND}(q[2], q[3])). \tag{5}$$

For storing and retrieving data in the cloud, the random key RV is generated based on this cross-computing, as shown in the form of:

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

The following is an illustration of Algorithm 1's detailed computational method for creating random hash keys:

Licensed Under Creative Commons Attribution CC BY



```
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.

3.2 PSL Algorithm

By training the model based on the features of the matrix, the feature learning technique is primarily employed in this stage to detect attacks. The IoT device's features are extracted using the proposed PSL methodology. The categories of normal and attacking features are updated in the training data model. To match feature properties with the database and detect attacks, the PSL is created as a feature learning model. In order to determine whether any threatening devices would attempt to access the cloud-stored data during the data storage and retrieval procedure, the IoT device attributes are matched with this training model. If the access was authorized, automatic activities including data storage and retrieval were carried out. If it is determined to be an attack, it can be automatically reported to the firewall or router that initially restricts access. Additionally, the available training model is used to learn and update the features and characteristics of this attack, after which the general features of the training model have been completely updated and rearranged to match the new attacking features. The subsequent data storage and retrieval operations for detecting and thwarting threats can also employ this trained model. As a result, this kind of AI-based feature learning contributes to the system's security by effectively identifying assaults. Additionally, this research uses probabilistic distributional features as the basis for its AI-based attack learning method. It discovers the many parameter combinations that can be used to group the data and create clusters, improving the accuracy of prediction processes. The primary advantages of the PSL mechanism include improved detection precision, protection of data privacy, high security, minimal processing time, and decreased computational complexity. AI-based feature learning with probabilistic features is used to achieve these benefits. Figure 3 shows the usual PSL approach architecture with its matrix construction.

The input data matrix MNID is used in this approach as the processing input, and the output is the anticipated clustered results Aij, Rij, and Cid. Here, the size of the matrices Si and Sj is taken into consideration when building the availability and responsibility matrices. This information has been used to compute the initial clustering of the data Aij, as illustrated in the following:

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

As a result, the following representation of the responsibility and availability matrices is used to compute the appropriate vector Rij:

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

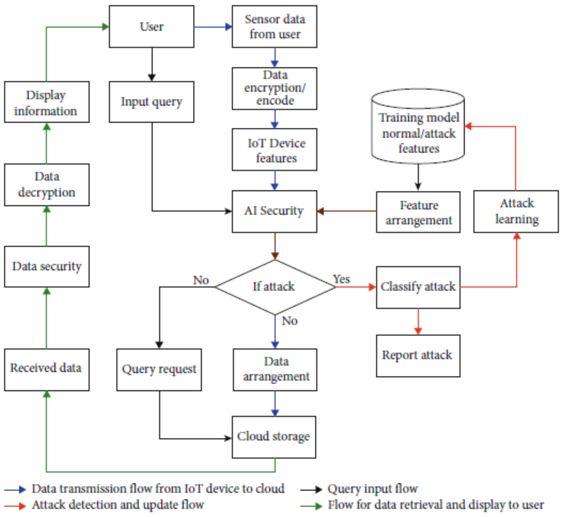


Figure 3: Overall flow of the proposed security system.

The availability matrix is then estimated and updated with the Rij temporary matrix, as seen below:

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

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

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

As a result, using the estimated list index and the average of the pertinent vector, an exponential matrix is created and then updated in the list as follows:

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

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

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

Licensed Under Creative Commons Attribution CC BY

Next, the following model is used to calculate the overall vector's associated average, avgR:

$$\mathrm{avg}_R = \frac{\sum_{j=1}^{S_j} R_{ij}}{S_j}. \qquad (15)$$

Additionally, as seen in the following, the distance between the average lists and its associated parameter is updated:

$$\mathrm{dis}_{ls} = \sqrt{\mathrm{avg}^2_{\mathrm{List}} - (\mathrm{avg}_R{}^2)}, \qquad (16)$$

$$\text{Update } C_{id} \longleftarrow \min(\mathrm{dis}_{\mathrm{ls}}). \qquad (17)$$

The categorized L is then predicted using the clustered outputs based on the shortest distance between parameters with relevant levels. A firewall will immediately block a projected clustered label that constitutes an attack, and feature learning will proceed with the updating of attacking features in the training model. The assaults are then further classified using the updated model to guarantee secure data storage and retrieval procedures. The proposed PSL methodology's architecture model is shown in Figure 4.

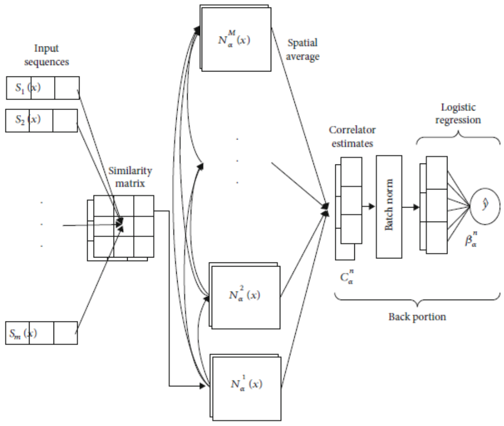


FIGURE 4: Architecture model of PSL methodology.

The following are the specific algorithmic stages for the proposed PSL-based feature learning model as shown in Algorithm 2:

```
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's consider, $S_i$ and $S_j$ to be the size of the matrix ($M_{NID}$)
        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 $\mathrm{temp}_{Rij} = 0$;
                For $m = 1$ to $S_i$
                        $\mathrm{temp}_{Rij} = \mathrm{temp}_{Rij} + R_{im}$;
                  End for $m$;
                Compute $\mathrm{temp}_{Rij}$ 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 $\mathrm{Expm}_{ij}$ and the average $A_{ij}$ of relevant vector $R_{ij}$    based on the
estimated list index $\mathrm{avg}_{idx}$ and update $\mathrm{avg}_{list}$ 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 $\mathrm{dis}_{ls}$ between the average list $\mathrm{avg}^2_{\mathrm{List}}$ and the related    parameter
        $\mathrm{avg}^2_{\mathrm{R}}$ by using equation (16);
          Update $C_{id}$ with the minimum of $\mathrm{dis}_{ls}$ as shown in equation (17);
        End for $y$;
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 their characteristics are updated in the training model as
        shown below:
        UF = append ($A_F$); //AF–attacking
        features in the trained model;
End if;
```

based secure environment that is protected by powerful firewalls and under the supervision of the organization’s IT department. The private cloud offers bigger opportunities that help meet specific organization requirements in customization.

4. Results and Discussion

This section evaluates the accuracy, precision, recall, and Matthews Correlation Coefficients (MCC) performance of existing and planned security methods, as well as the encryption and decryption times, delays, throughput, packet delivery rates, and processing time.

4.1. Performance Analysis of AI Techniques

Figure 5 (and Table 2) illustrate throughput rates for both proposed and existing AI security methods. Typically, a system's output can be expressed in terms of bytes. The output of the network is significantly influenced by the transmission rate of linked devices. The ratio of the total number of messages created by all nodes to the total number of messages successfully received is used to calculate the throughput of the network. These include the Internet of Things Artificial Intelligence System, Intelligent Face Recognition and Navigation System, Intrusion Detection System, and Securing Things in Healthcare (IoT-AIS). According to the findings, the PSL-RH methodology performs better than the other methods with a higher throughput value. The suggested framework accurately detects assaults based on the predetermined criteria, enabling dependable data flow between users/devices.

Figure 7 compares the proposed PSL RH approaches with existing IoT AIS transmission rates for various devices.

Licensed Under Creative Commons Attribution CC BY

Table 4. The difference between the data flow from an IoT device to a cloud and the data obtained from that cloud and delivered to the user is the data transmission rate. This makes assault detection possible. The PSL-RH model achieved a quicker data transmission rate while maintaining good security compared to the present model. Attacks can be recognized and stopped early on thanks to the feature model's training. This enhances the proposed system's data transfer rates.

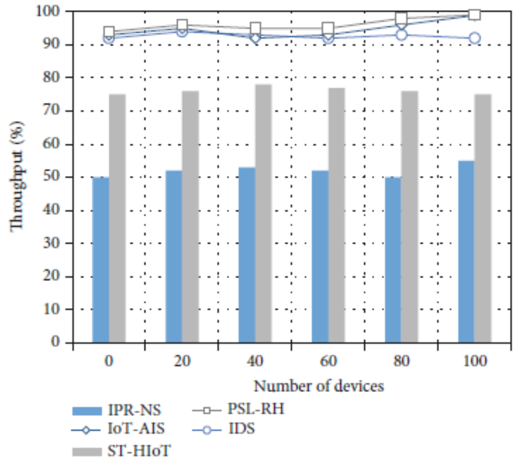


Figure 5: Throughput vs. number of devices.

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

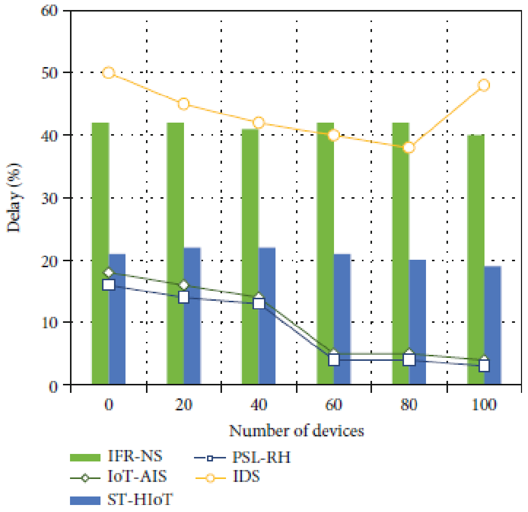


Figure 6: Delay vs. number of devices.

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

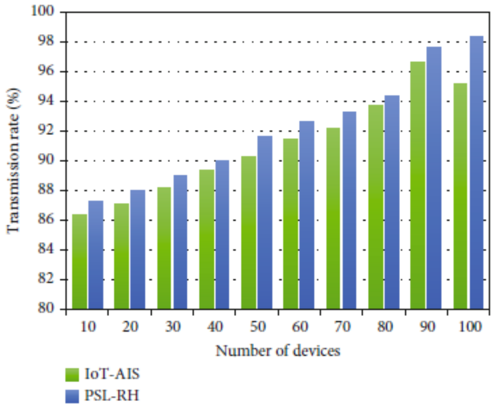


Figure 7: Transmission rate vs. number of devices.

Based on measurements of accuracy, precision, recall, F1-score, and MCC, Figure 9 and Table 6 compare the overall performance analysis of existing [37] and suggested attack detection systems. Typically, the accuracy, precision, and recall metrics have a significant impact on how effective the overall security system is. Additionally, these measurements are primarily computed to see how the security plan could forecast the precise values at the time of attack identification and prediction and are calculated as follows:

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

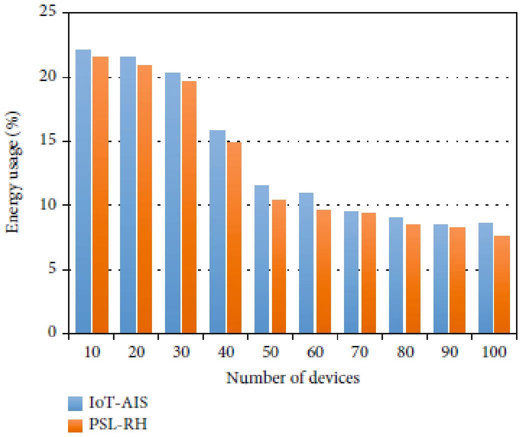


Figure 8: Energy usage vs. number of devices.

A comparison of the energy requirements of various security measures, both current and proposed, is shown in Table 5. Energy utilization is computed based on the IoT device's communication latency. These findings also demonstrate that the suggested plan uses less energy than alternative methods.

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

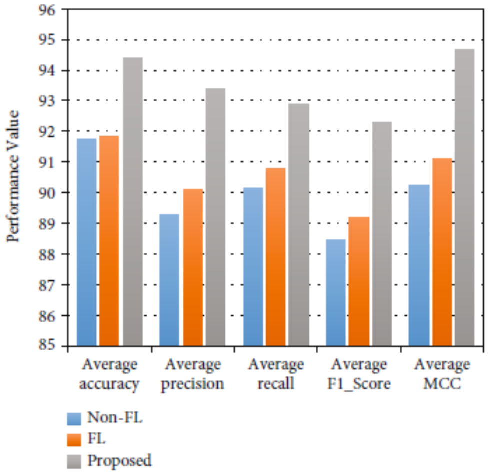


Figure 9: Overall comparative analysis of the existing and proposed techniques.

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 stands for "true positive, " TN for "true negative, " FP for "false positive, " and FN for "false negative. " These findings make it clear that the proposed PSL-RH technique, which accurately detects and blocks attacks based on the trained model of the feature set, outperforms alternative learning strategies in terms of performance.

Figure 10 shows the Receiver Operating Characteristics (ROC) analysis of both current and suggested methodologies with regard to altering True Positive Rate (TPR) and False Positive Rate (FPR). The performance of the attack detection procedure under various thresholds is validated here by computing the ROC of the learning models. This analysis makes it clear that, when compared to the other learning models, the suggested PSL-RH approach offers a higher TPR.

The information entropy analysis of both the current [19] and new approaches for various samples is shown in Figure 11 and Table 7. Typically, the information entropy has been calculated based on the information's randomness, which is primarily assessed for calculating the average level of ciphertext uncertainty. This investigation demonstrates that by producing random hash points during key generation, the RH combined with the PSL technique could effectively increase the information entropy.

The maximum, minimum, and mean values of the Number of Data Unit Change Range (NPCR) and Unified Average Changing Rate (UACI) are assessed for both the current and suggested security techniques in Figure 12 and Table 8. This is how these measurements are calculated:

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

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

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

where $\boldsymbol{A_1}$ **(i, j)** and $\boldsymbol{A_2}$ **(i, j)** are described as two ciphertext data's gray values at two places (i, j). According to the evaluation, the proposed PSL-RH technique offers better theoretical NPCR and UPCI values when compared to the existing techniques.

Licensed Under Creative Commons Attribution CC BY

4.2. Performance Analysis of Existing and Proposed Data Security Techniques

For the various IoT devices, including ECC, RSA, IECC, and suggested ECC-RH, Figure 13 and Table 9 display the encryption times of both existing [38] and new data security solutions. In most cases, the encryption time is determined by how long it takes to use the produced key to encrypt the original data into ciphertext. As illustrated in Figure 14 and Table 10, the decryption time is determined by the time required to convert the cipher data back into its original format, and it is evaluated for both existing and new algorithms. These comparisons lead to the conclusion that the suggested RH approach when used in conjunction with the ECC data security mechanism, takes less time for both data encryption and decryption. The random key is created for the input data stream in the proposed data security technique based on the random hash value and signature pattern of the data matrix. As a result, it aids in accelerating the time-intensive procedures of data encryption and decryption.

5. Summary, Conclusions and Recommendations

In order to safeguard the privacy and confidentiality of healthcare applications in an IoT environment, this study provides an AI-based security framework. With the help of cutting-edge AI technology, this article aims to enable secure data storage and retrieval. PSL is an AI method that foresees attacks before they happen. By employing the features that were learned to train the model, the security of the healthcare system is increased. In order to save sensitive data securely, the RH-based key-generating method is created and integrated into the ECC mechanism. The distinctive feature of this AI technology is that it maintains a trained model of data with the normal and attack features that aid in early-stage attack detection. Additionally, it notifies the user of the firewall assault and updates the trained model with the details of the identified attacks. The signature pattern and hash values of the data matrix could be used to generate a random key. This will enhance the method for protecting data. In IoT-cloud contexts, this arbitrary key can be used to protect data storage and retrieval.

Reduced computing complexity, speed, low time consumption, and precise attack detection are some of the main benefits of the suggested AI security method. A performance analysis of the suggested AI security mechanism is conducted to verify the findings. It was evaluated using a variety of criteria and contrasted with the existing feature-learning, classification, and data security models. The PSLRH technique is superior to other procedures with better performance results, it was concluded based on the findings.

5.2 Further research

This work can be extended in the future by integrating the AI-based security framework into various more real-time application systems. Additionally, based on the random key generation and trust agreement procedures, compact security models may be created to guarantee the security of IoT data used in the healthcare industry. The heterogeneity seen in 5G necessitates dispersed security solutions. A distributed cyber security system that can be applied to stop DDoS attacks is [60]. For dependable and effective data delivery, the trusted routing strategy in [61] can be used to support 5G-enabled IoT apps. [62] was able to improve the dependability of data routing while defending the network layer for 5G-enabled IoT against various routing attacks independently. The cyber-physical system aspect of cyberattacks, which is important for 5Gen-enabled IoT apps, is investigated and addressed in [63]. The network layer for 5 G-enabled IoT apps still has other flaws that need more analysis.

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 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

Licensed Under Creative Commons Attribution CC BY

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 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.

Licensed Under Creative Commons Attribution CC BY