International Journal of Applied Engineering and Technology

An IoT-Based Secure Healthcare Framework

Hesham A. El Zouka

Computer Eng. Dept., College of Engineering and Technology Arab Academy for Science, Technology, and Maritime Transport, Alexandria, Egypt

helzouka@aast.edu, helzouka@gmail.com

Date of Submission: 15th November 2023 Revised: 27th December 2023 Accepted: 18th January 2024

How to Cite: **Hesham A. El Zouka (2024). An IoT-Based Secure Healthcare Framework. International Journal of Applied Engineering Research 6(1), pp. 53-62.**

***Abstract* - Undeniably, IoT-clouds are liable to attacks and intrusions due to its formation of a huge number of sensors that are mainly used in producing data. When it comes to healthcare data being secured in IoT clouds, then this would be a real challenge. In this case, Artificial Intelligence technology will represent the best way out of this trouble through adopting AI-based methodologies to secure healthcare data, in IoT-cloud framework, from any violations that may affect its privacy and security. Yet, this solution has also got its drawbacks like inefficient data handling, being unable to tackle unstructured data, being more complex in terms of algorithm design and time consumption. Therefore, this paper presents a security-based methodology which aims at reducing IoT sensors cost and providing conversational AI experience to healthcare data available in IoT-cloud framework using probabilistic hash function mechanism. Adopting this new mechanism will also help in detecting attacks at an early stage, along with analyzing and studying their main features and characteristics. Moreover, this mechanism will help in securing data through standard Elliptic Curve Cryptography technique and the secure key produced from the data output hash value. Consequently, data cryptography processes will be used by the, previously mentioned, randomly generated hash key along with the updated ECC-HF technique. Performance indicators are used to evaluate, compare, and validate the results of applying both suggested and already existing mechanisms.**

***Index Terms* – Internet of Thing (IoT); Healthcare, Encryption; Network; Privacy.**

INTRODUCTION

It is undeniable how the Internet of Things (IoT) has become an important medium for storing and transmitting info through a variety of means. IoT networks are mainly built upon connectivity, user interface, sensor devices and data processing. It has become extremely useful in many fields like healthcare where it is responsible for collecting the patient's crucial data from the devices attached to his body [1]. Then, it sends it to the cloud network through radioaccess points in order to be processed via the used application and be ready to be displayed and sent to the targeted receiver/doctor with the help of the user interface.

It has become quite urgent, then, for the healthcare field to be more updated and flexible to rely on cloud networking for healthcare services to be more accurate, credential, and efficient. On one hand, Artificial Intelligence (AI) technology is highly recommended to be used in real time application of health systems to deal with complex data, guarantee data security, identify unknown threats and reduce duplicates [2]. IoT technology, on the other hand, is frequently adopted and recommended for its autonomous characteristics, robust efficiency and ability to connect enormous number of sensors and devices to securely transmit data to the cloud using wireless links. However, securing the data transmitted from the sensor devices to the nearest radio access point is not totally achieved and the whole process of connecting both ends is at stake [3]. This process is liable to system failure, human error, network failure, natural phenomena, and malicious intent. However, this paper only tackles privacy threats/risks intrigued by malicious factors such as collusion attacks, malicious code, man-in-the-middle attack, data leakage and destruction, DOS/DDOS and malware like ransomware [4]. Therefore, it has become quite urgent to have a security algorithm that would guarantee using IoT devices on every single scale without being concerned with security issues.

As being a main pillar in transmitting data in the healthcare field, IoT has successfully high lightened the vulnerabilities that the patient's personal transmitted info are liable to in the process of remote treatment [5]. However,as it has been mentioned earlier, IoT technology faces serious security issues which need to be handled to maintain a completely secure data transmission process. Hence, AI technology is the best mechanism to be used in enhancing healthcare applications adopted in IoT cloud frameworks due to its efficiency in securing healthcare data transmitted between both ends, the patient and the doctor. Actually, AI technology has different types that are widely used in many systems coming under the different classifications of rule-based methodologies, deep learning model, and machine learning techniques [6]. The general architecture of IoT with AI System for health care security is representedin Figure 1.

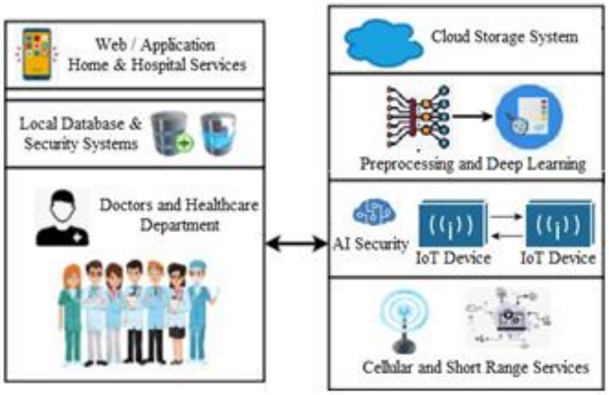

Figure 1: AI Network Security System for healthcare IoT

I. Motivation and Achievement

An AI-based learning methodology is meant to be developed here in order to predict attacks at an early stage after testing the features of user data which to be encrypted and decrypted as well due to the application of the Elliptic Curve Cryptography (ECC) technology along with the randomly generated hash value [7]. Unlike other researches, this paper focuses on the transmission of data from the IoT sensor-devices attached to the patient's body to the doctor through network providers and introduces an encrypted security algorithm which processes from the IoT sensors in order to keep this info covered and unexposed to any interfering party [8]. This solution works on encrypting the data packets right from the sensor devices and before being sent to the doctor [9]. As an end-to-end health data transmission security system in IoT, this algorithm has proven its success as a two-level encrypting solution at the patient's end, and a two- level decrypting solution at the doctor's end.

II. Problem Statement

For data storage and security services in the cloud framework, different encryption techniques like Elliptic ECC, AES (Advanced Encryption Standard, and Secure Hash Algorithm (SHA) have been utilized in different security systems as shown in Figure 2. These encryption and classification techniques can securely decrypt data at an early stage before storage and retrieval procedures and limit inefficient prediction results, high error rate and process delay, which affects the performance of the whole system, respectively [10].The proposed system is developing a hybrid AI- based intelligent algorithm that is based on both IoT sensors and random hash function to secure healthcare data and solving all the previously mentioned problems.

III. Contribution and Assumption

The contributions of the suggested scheme are presented as follows:

- Encrypting and decrypting data are carried out using Random Hashing or RH generated hash keys [11] to secure stored healthcare data in IoT-cloud.
- Applying user query input processing to ensure secure-reliable transmission and attack detection [12].
- Utilizing AI-based Probabilistic hash function mechanism (PHF) [13] to ensure the reliability of data retrieval with feature learning models for attack analysis and reporting.

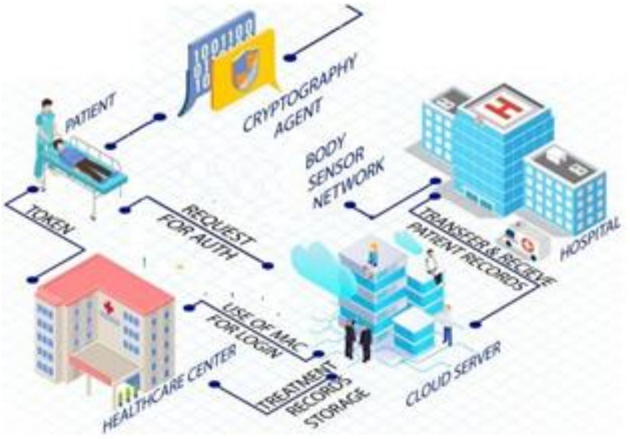

Figure 2: Secure IoT-based Healthcare System with Cloud

The PHF mechanism performance is mainly evaluated in terms of encryption/decryption time, key generation time, recall, accuracy and precision with the assumption that all data is initially stored unsecured in the cloud.

The remaining of the paper is presented as follows: Section II presents the importance of IoT security including the pros and the cons of the currently used data security and attack detection techniques in IoT-cloud framework. The related work is also discussed in this section. Section III presents the suggested encryption/decryption model in detail through algorithmic illustrations, description and clear flow. It also explains how the data is processed throughout its journey from the sender to the receiver. Section IV represents how the proposed system is tested and analyses its results. Ultimately, section V summarizes the whole paper and presents the suggested future work.

LITERATURE REVIEW AND RELATED WORK

The issue of securing data transmitted with the help of IoT has been of great interest to many researchers and several contributions have been presented for this end. For example, the SaaS security system which employs Virtual Local Area Network (VLAN) through a three-layer IT-based system consisting of private layer, fog layer and extreme layer [14]. This system is responsible for connecting the network's different devices, considering the possible risks ofthe system, and providing the involved devices with numerical values after carrying out different security tests on them.

Another security solution is the use of AI technology to prioritize and identify risk, instantly spot any intrusionon the network, detect any malware on the network, and guide to incident response [15]. The currently used AI-basedschemes to secure data in IoT frameworks are presented in detail in this section along with their advantages, disadvantages, characteristics, and processing manner.

As it is getting more important these days, IoT devices are utilized on a wider scale and the issue of its ability to secure data and other devices they're connected to is becoming urgent. To maintain the security of the medical environment from which the whole process starts, Vaibhav et al. [16] have introduced a smart IoT algorithm to which all AI-technique features and policies are integrated like transparency, interoperability, data privacy, accountability, sustainability, accountability, and security. This algorithm has also been targeting the detection of information disruption, network properties and other different host-property types of attacks. However, system adopting this algorithm have proven not to perform perfectly due to the lack of adopting specific methodologies to detect different attacks on the network. Wei et al. [17] have introduced a study tackling healthcare IoT systems in terms of the machine-learning techniques used in them.

In this study, each technique has been thoroughly discussed and its constraints and applications have been introduced in terms of reliability, privacy, security, interoperability, reliability and bounded latency which must be achieved to maintain a secure and efficient IoT algorithm. Upon this study, different similarity-matching techniques along with their operating features and applications have been tackled like: K-means, linear regression, dimensionality reduction methods discriminant analysis and logistic regression. In this respect, it has been proven that linear regression is considered the best technique to evaluate the dependent/ independent relationship variables. Gopalan [18] has introduced an AI-based IoT algorithm to continuously monitor, measure, and maintain the security of healthcare networks, including patient records, medical devices, databases, vulnerable legacy systems, and cloud services. For this end, a Deep Conventional Neural Network (DCNN) or DCNN-based malware detection algorithm has been applied to limit access to the data and, hence, block any violations. In conclusion, this framework has proved to be beneficial in terms of increasing minimal delay and delivery packs and decreasing response time.

As for Hayyolalam et al.[19], they have introduced a three-tier smart healthcare system that aimed at designing Internet of Medical Things in which basic features like field sensor networks, cloud services and WBSN were included. Baoyuan et al [20], have introduced a system that aimed at authenticating the patients to provide access to the application data stored on the cloud. It is a lightweight authentication system that mainly works on authenticating user/server registration and securing the cloud environment IoT devices.

This algorithm was not highly efficient in terms of providing high attack detection, misclassification rate and reliability. However, it is extremely beneficial when it comes to computational and storage cost reduction. Siam et al. [21] have also worked on securing IoT-cloud environment by using homomorphic encryption algorithms and bilinear maps to encrypt data. In the same respect, Chang and Junho [22] have introduced a context ontology model to secure the system through detecting vulnerabilities and intrusions.

According to the pattern of attacks including software attacks, memory dump, port access and data sniffing, inference rules have been created. Those rules are responsible for detecting and analyzing vulnerabilities, and, hence, they would be extremely helpful in understanding such a complex model.

Hodo et al. [23] have focused on securing IoT networks by presenting a survey that is covering different AI mechanisms. Main security challenges in IoT networks like source authentication, availability and confidentiality have been tackled in this proposal. Adopting an improved Ant Colony Optimization technique has been suggested byChang et al. [24] to secure data by setting optimized completion time for load balancing strategy to be improved.

In this case, data storage in an encrypted form on IT cloud is maintained by adopting full homomorphic encryption and decryption mechanisms. Utilizing encryption mechanisms like Advanced Encryption Standards (AES-128) to secure data in IoT cloud, mainly result in generating secret keys so that the ciphertext would have several transformation rounds. Such a security model could be evaluated in terms of latency, QoS, consistency and accuracy.

Elzouka and Hosni [25] have discussed the main factors for securing data in sensor networks via dynamic support, authorization code, reduced overhead, fine-grained control, access efficiency and integrity verification. The security of cloud environments is ensured through confidentiality parameters using a fine-grained access control mechanism. This mechanism could be evaluated in terms of calculating storage overhead, throughput and encryption/decryption time. Muhtadi et al. [26] have introduced a new cyber security system adopting a machine learning approach to reduce computational overhead. An Optimal Homomorphic Encryption scheme has been presented by Kalyani and Chaudharito increase data sensitivity in IoT cloud . For this model, the Deep Conventional Neural Network (DCNN) technique and the optimization technique have been adopted to identify optimal feature-based attacks and to authenticate the key generated during data encryption, respectively. A detailed study of AI-based mechanisms utilized for securing IoT cloud environment, AI technologies like shallow machine learning, rule-based learning and deep learning and layer- wise security threats has been presented by El Zouka et al [27]. AI and machine learning techniques have proven their ability to initiate all the operations that would help in elevating the security systems and block IoT threats.

However,these techniques are facing some challenges in terms of handling increased delay time, data scarcity and large dimensional data [28]. An advanced AI technique is, hence, proposed in this paper to guarantee secure retrieval of healthcare systems and data storage.

PROPOSED METHODOLOGY AND FRAMEWORK

The proposed algorithm, as mentioned earlier, works on encrypting data collected from the attached devices, having them sent to the cloud network via radio access points and getting them delivered to the receiver/doctor to be decrypted. The whole process is quite vulnerable, especially when sending this crucial data to the cloud network where it could be extremely liable to violations [29]. At this point, the suggested cryptography system will be applied, where the data, already taken from the attached medical devices, is gathered in a matrix form, and multiplied using a key that is different and unique for each patient. The proposed methodology mainly uses an advanced AI technique to securely handle, retain and store data from IoT-cloud computing system. The AI techniqueadopted here is the PHF or the Probabilistic hash function technique to analyze the main features of the retrieved data from IoT devices and to secure data transmission. PHF AI-based technique is supposed to instantly detect/learn features of attacks or other normal procedures taking place during the process of data storage and data retrieval whichcould also be guaranteed by the Elliptic Curve Cryptography (ECC) model which uses Random Weight Hashing (RWH) algorithm for the same end. The AI-based security system proposed in this paper is presented in details and its architecture and flow illustrations and presented in Figures 3 and respectively.

According to the system's choice, the multiplied data will be turned into an ASCII/binary and then it will be multiplied again using a different key in the ASCII/binary and the resulting outcome will present the encrypted codefor the suggested system. The used formula is:

$$Y = h_{256}(X) + XOR(X, E, C) + k \qquad (1)$$

Where Y, K and X represent the encrypted data, the applied key, and the patient's information, respectively and ***h*** represent the signature pattern. The encrypted data is mainly made up of two keys: E and C. The first one is applied as the process starts and the second one is responsible for enhancing the system's security.

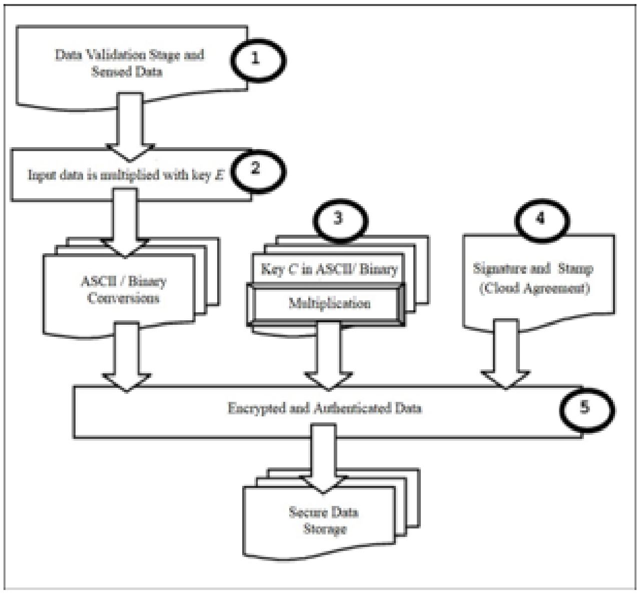
Data Validation Stage and Sensed Data
1
Input data is multiplied with key E
2
ASCII / Binary Conversions
3
Key C in ASCII/ Binary
Multiplication
4
Signature and Stamp (Cloud Agreement)
Encrypted and Authenticated Data
5
Secure Data Storage

Figure 3. Block Diagram of Encryption Process

A predefined inverse ASCII/ binary ruleis adopted by an IoT sender, and is also applied at the receiver end, to generate both keys; key E and key C which can be easily changed after the key change request go through all the required security checks [30].

The above diagram shows how key E, which is set as a default key by the proposed algorithm, is multiplying the collected data. As mentioned before, this key, which could be changed, if necessary, will be ready for multiplication again by key C when changed into ASCII for more security. This step will make any violation to the data extremely difficult, making the suggested algorithm unique and special. Then, the encrypted and authenticated data will be securely sent to the receiver/the doctor to be decrypted and analyzed without any intrusion.

$$X = h_{256}(Y) + XOR(Y, E, C) + k \qquad (2)$$

The decryption process will depend on the following formula as the receiver is aware of the used keys in the encryption process.

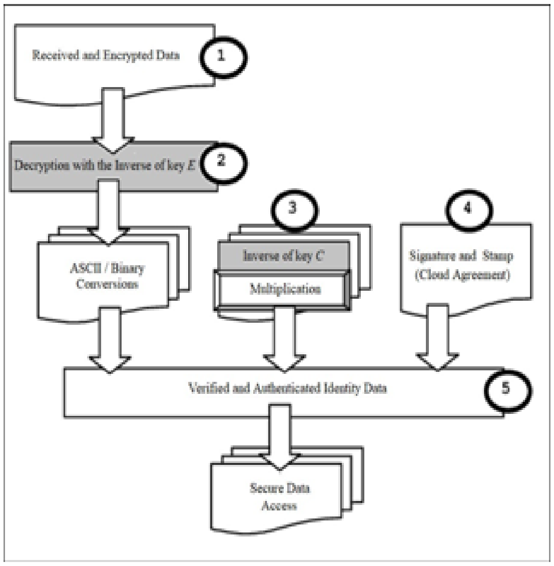
Received and Encrypted Data
1
Decryption with the Inverse of key *E*
2
ASCII / Binary Conversions
3
Inverse of key *C*
Multiplication
4
Signature and Stamp (Cloud Agreement)
Verified and Authenticated Identity Data
5
Secure Data Access

Figure 4: Block Diagram of Decryption Process

The encrypted data (Y) will be decoded by multiplying key E inverse matrix and turning it into ASCII/Binary, then using key C to multiply it again in order to get the patient's original data (X), so that this 2-phase process could be completed safely. Frequently, the Media Access Control layer or MAC witnesses the addition of keys as headers and the concatenated hash being sent with messages to recognize the man in the middle using bits [31].

According tothe suggested algorithm, keys E and C will delve into the original data along with the hash, which is added at the endin a form of a single bit, to help in decoding the data at the receiver's end and to make it more difficult to any intruderto get access to the original info. The procedures / stages performed by the proposed technique could summarized as follows:

- Transmission of data to the cloud servers
- Processing the input of user-defined functions.
- Feature extraction and attack detection.
- Retrieving secured data from the cloud.

Firstly, the RWH algorithm is used to encrypt/decrypt data after hash 256 projection matrix generation and before this data is moved into the cloud as shown in Equation 3 and Equation 4. Where k is a randomly generated value and less than the value N, which is the possible hash value, and N-1 is the remaining values. Then, the proposed AI-based method will be used to analyze whether this hash is normal or represents an attack. If it is proved to be normal, data arrangement process into the cloud will be proceeded, otherwise the routing system or the firewall will be instantly informed to block this attack at its initial stage.

$$\frac{N-1}{N} * \frac{N-2}{N} * \dots * \frac{N-(k-2)}{N} * \frac{N-(k-1)}{N} \qquad (3)$$

$$h_{256}(T) = e^{\frac{-k(k-1)}{2N}} \qquad (4)$$

The destination IoT device level and sender only witnesses the encryption and the decryption processes in the suggested system due to personal privacy rules, man-in-the-middle problem termination, IoT limitations, characters and security which make it more of an end device level and, finally, delay avoidance when processing at every level. Moreover, it should be mentioned that in the same sender and destination IoT devices only three hops are used between both ends, bearing in mind that changing the number of hops will not make any difference due to limiting this process to this level only. For this end, the PHF mechanism has been adopted to update the training model with the features and the properties of the reported attacks. Then, comes the role of AI-PHF mechanism in detecting the query input of the user, to access data, and deciding whether it is normal or malicious. If it is proved to be normal, the process of retrieving data will be proceeded by decrypting this data and generating a signature matching pattern using the RH-based decryption [32]. Finally, the user will have access to the data and will be able to see it with all security measures being considered.

I. IoT Security based on ECC Random Hashing Algorithm

Undeniably, ensuring data security represents a real challenge in different IoT security system because of the complex format of data-feature learning and arrangement and the size of data transferred. Therefore, the original data should be initially encrypted using RWH technique. The processes of encrypting and decrypting data have proven to be quite vital, then, when carried out before data storage and data retrieval, respectively, along with checking the query input of the user to maintain a totally secure process. In this respect, many conventional models like IDEA, RC4and AES have adopted different encryption and decryption mechanisms. But using encrypting and decrypting mechanisms has some drawbacks like computational overhead, key generation and encryption increased time consumption and complexity implementation. To avoid these disadvantages, the proposed algorithm is using ECC-RWH mechanism or the Elliptic Curve Cryptography with Random Hashing key generation to ensure data security in IoT cloud domains relying on encryption and decryption processes. As for the RWH technique used in this mechanism, it depends on the input data to generate a random key that is responsible for encrypting and decrypting data in IoT cloud. As mentioned earlier, IoT could be useful in the healthcare field when collecting data packets and transmitting them through radio access points, like a near cell tower or wireless LAN, to be sent and processed at the cloud network and be finally targeted to the doctor's device. The distance between both ends or the actual locations of them is totally unimportant. To increase data security, the proposed mechanism follows different computations in order to create the hash function, but as yet, it has several advantages like: small generated keys , reduced time consumption, using optimal bandwidth and fast encryption processes.

Finally, the ECC-based encryption system is considered one of the security systems that has been working on securing data sent from sensor devices to the doctor’s office through fog computing and cloud computing security layers. However, the security systems mentioned above were not able to provide total security to the transmitted data, as the methods used to encode this data were easily violated by malicious intruders. The proposed system adds cryptographic security in order to guarantee information security from the very beginning. The whole process starts by embedding the sensor devices with cryptographic algorithms so that the crucial health info will be encoded even before being sent/transmitted to the targeted receiver. The cryptography mechanism could be made clear by multiplying the data collected from the sensors using a cryptography key-code matrix and hash function, so that the encrypted data could be encoded. Then, this encoded data will go on with its journey to the nearest radio access point, then to the cloud and, finally, to the receiver, to be decrypted by multiplication using the cryptography key-code to be decoded. What makes the suggested solution special and efficient is the encryption process through which the flow of data from the sensor devices to the doctor’s office will be totally secured. This aim is achieved by multiplying the messages and the key added to encode the info and make it totally unavailable for any intruder. This makes the output message totally different from the already encrypted one at the beginning of the process, making it more complicated and less liable to violations. Unlike the previously mentioned security solutions, which just add a message and a key to encrypt the data while being sent to the nearest access point making it more liable to violation and interference. only the security of transmitted data in healthcare field from devices attached to the patient to the doctor is the main concern of this paper, but also the routing of such info between both parties. Aiming to present a sensor-driven solution that could add an identifier at the sensor level to tackle data routing in bust IoT networks.

II. The PHF Algorithm

Upon the features in the matrix, the features learning technique will carry out its mission in detecting attacks features in the training model [33]. The PHF algorithm here represents the feature learning model which will detect the attacks by comparing and matching feature attributes with the features database. To detect any attacking attempts to the data in the IoT, either during data storage or the retrieval process, the features of the IoT device will be matched with those of the training model. As mentioned earlier, if any attempt to access data is proved to be normal, the ordinary sequence of processes will take place, otherwise the routing device will be informed to initially block those attempts and maintain data security. Learning and detecting all attacks features will, consequently, help in updating and arranging new attacks features in the training model.

This will automatically help this model to instantly detect and attack malicious intrusions. A better prediction process is, then, maintained after identifying several parameter combinations to be grouped and set in the cluster. Therefore, using AI-based mechanism that relays on probabilistic features, will result in many advantages like : ensuring data privacy , reducing complexity and time consumption , increasing detection accuracy and high security .Within this algorithm, input data matrix NID and the predicted clustered results Aij, Rij and Cid represent the input of processing and the output, respectively .According to the size of matrices Sj and Si, matrices of responsibility and availability will be set up to compute Rij relevant factor.

PERFORMANCE ANALYSIS

All the devices used in testing the proposed algorithm were chosen due to possessing the same protocols as other regular commonly used sensors, being originally designed for testing IoT protocols and being able to behave like nodes used in the middle or IoT end devices. First, the base standard for the applications used in this test is IEEE-802.15.4 TI standard. Secondly, CC1310 Launch Pad development kits are used for data transmission testing. For creating sample sensor devices like those attached to the access points and patient’s body at the receiver’s end, twenty of the previously mentioned launchpads have been used due to their ability to obtain data, create packets and send data, respectively. Moreover, those launchpads are adopted here for their efficiency in data collection, long-range connectivity and external sensors interface providence. Ultimately, it should be mentioned that the whole process has been tested and developed using C programming code composer studio version.

For being able to be easily applied at source/ destination node level and to avoid extra delay in the middle hop sensor nodes, the suggested end-to-end IoT security model is more privileged and more unique than any other algorithm. Table 1 has made it clear that the range of executing the suggested IoT security scheme is 80-120M, where its nodes can communicate with the cloud in the approved channel by 60 kbps data rate and the packet arrival rate for each nodeis 0.22 seconds.

To carry out this experiment / test, one collecting unit for router and another one for the doctor are used along with eight sensors. One of the, previously mentioned, Launch Pad [34] will be used in collecting the patient’s data from the sensor devices attached to his body to be multiplied by key E and, then, received by another launchpad at the doctor’s end to be decrypted. Hence, licensed users could access the same channel if star topology non-beacon IoT communication is carried out.

TABLE I
NETWORK SETUP PARAMETERS

Parameters	*Values*
Identifier	7-10 Bits
Number of Applications	10
Frame Type	2-4 Bits
Transmission range	80-120M
Number of Packets Sent	150
Time Delay of Health Data (ms)	33.53
Data rate of the channel	60kbps
Size of medical data packet	80 bytes
Running Time	24 hours
Frequency	950 GHz

The end devices used in this experiment will altogether help the suggested IoT algorithm in encrypting and decrypting data depending on sensed data.

Test Results And Analysis

The suggested algorithm has been tested using different examples to check its success in encrypting and decrypting data on both ends; sender and receiver. It has also been tested and assessed in terms of key size, processing time, overhead communication, flexibility to be applied to variant IoT types, cost, liability to attacks and memory usage. Regarding energy consumption, memory usage and processing time, the proposed system's results are better than other security systems. In this respect, two different inputs have been added to test the system's ability to encrypt and send them via access points to the targeted destination.

The first input to be encrypted, multiplied by key E and converted to ASCII upon user's request, which was then multiplied again by key C to have more secure and trust connections. The result achieved, as it is already clear, is totally different from the original message and the possibility for any intruder to violate it is null . Therefore, no one will be able to read and understand the sent messages rather than the licensed users because of their previous knowledge to the keys used in this process. After receiving messages at the other end (receiver), they will be decryptedto successfully obtain the original messages. This result was achieved by multiplying the encrypted messages using key C inverse, then followed by key E inverse to be obtained again from ASCII and get it in its original format.

Using built-in keys could easily expose data to violation by intruders, which is a matter/issue that is not done at all by the proposed IoT security system. On the other hand, it uses different self-created keys with each case and performs character by character encryption to make it impossible for an intruder to decipher and understand the transmitted messages [35]. All characteristics mentioned above show how efficient the suggested system is in terms of securing data using complicated steps to prevent any intrusions or violations.

This section is comparing and assessing the performance of both suggested and existing security mechanisms in terms of Matthews Correlation Coefficient (MCC), F1-score, delay, throughput, encryption/decryption time, precision, accuracy, recall , computational time and packet delivery rate.

I. Performance Analysis of Proposed and Existing AI System

With respect to the throughput of both mechanisms in many IoT devices, it should be first mentioned that a system's output is evaluated in terms of bytes and the packet delivery ratio of the connected devices has a great influence on it. Therefore, the total number of packets made up by the nodes as well as the total number of received packets will help in estimating the throughput as shown in Figure 5. Due to its increased throughput value after allowing reliable data transmission between both ends and using a set of features for detecting and analyzing any possible attacks, the proposed AI mechanism has overpowered other existing security systems such as IoT Artificial Intelligence System, Securing Things in the Healthcare Internet (ST-H-IoT), Navigation System and Intelligent Face Recognition, and Intrusion Detection System (IDS).

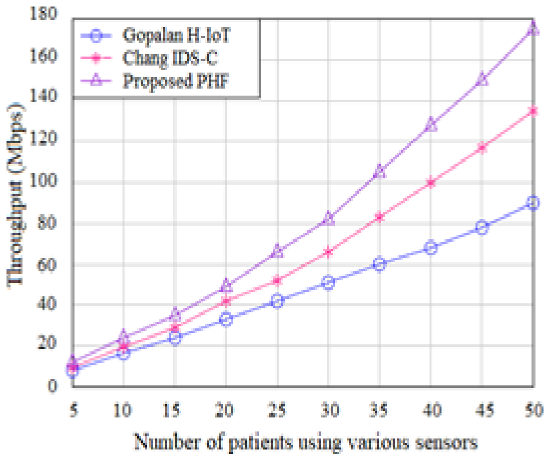

Figure 5: Throughput vs. Number of Patient Sensors

Considering the delay issue, it should be mentioned that delay in any network is calculated by the maximum duration spent by the data rate resulting from the maximum flows to reach its destination and how they are separated due to the delay and, ultimately, by estimating the latency between the sent request and cloud server received response. As mentioned earlier, the proposed technique PHF initially checks and analyses the features of user's query input and, hence, both input data transmission and retrieval processes are carried out in a shorter spanof time and a minimum delay is consumed when compared to the existing techniques.

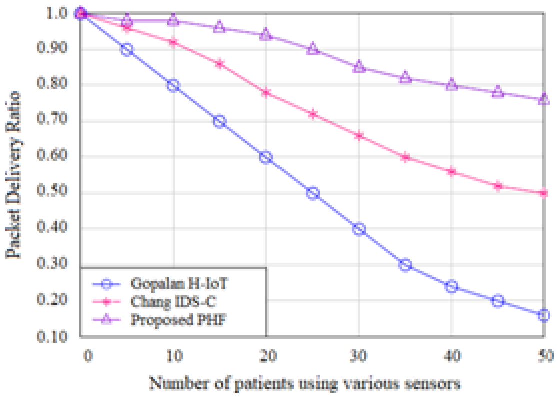

Figure 6: Transmission Rate vs. Number of Patient Sensors

To evaluate the packet delivery ratio of the proposed PHF and the existing IoT-AIS techniques, it should be made clear first that the message delivery ratio is evaluated according to the flow of data between IoT device and the cloud on one hand, and the received data from the cloud to the user, on the other hand. As a matter of fact, identifying and, hence, blocking attacks will definitely result in an increased data transmission rate, which is the case for the proposedtechnique as illustrated in Figure 6.

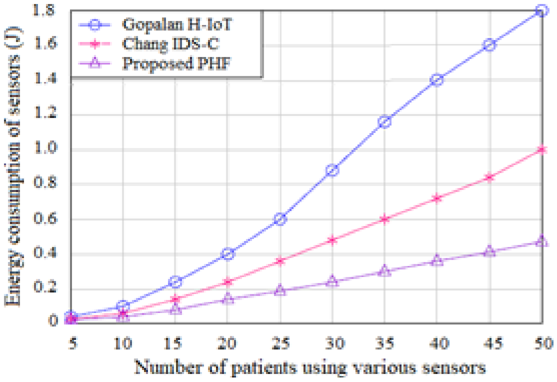

Figure 7: Average Energy Consumption of Sensors

As for energy consumption, it is mainly calculated according to communication delay of the IoT devices. The proposed algorithm has given better results than the existing ones in terms of energy consumption as it has only required / consumed minimal energy to accomplish its mission. The average energy consumption of sensors in the proposed PHF model compared with other competitive models is illustrated in Figure 7.

The overall performance of a security system must be computed in order to evaluate both its effectiveness, suitability, precision, and accuracy. These measures are also utilized in calculating and predicting the actual estimations at the time of attacks prediction and identification. This kind of analysis is vital for permitting attack detection regardless the variety of thresholds. Hence, the proposed technique has given an increased true positive ratewhen compared to other existing ones.

As for information entropy, it is calculated in different security systems according to the calculations of ciphertext average uncertainty levels. As being able to generate random hash while generating keys, the proposed technique has proven to be more efficient than the existing ones in this respect.

II. Performance of Existing and Proposed Security Models

As for calculating the encryption time, this mainly depends on the time taken to encrypt data, using a generatedkey, into a ciphertext.

On the other hand, calculating the decryption time depends on the time taken to decrypt ciphertext into the original form. Both encryption and decryption times are calculated for the proposed technique andthe existing ones, and, hence, the proposed technique has provided reduced encryption and decryption time.

Actually,both processes are carried out in a considerably short time because of the signature pattern and the data matrix hash value which work together in creating the random key which detects the input data stream.

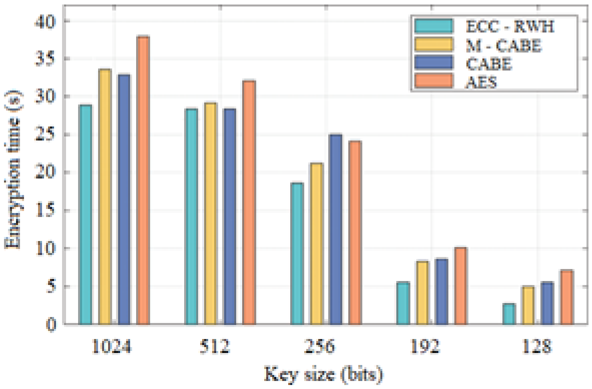

Figure 8: Comparison of Average Encryption Time

According to Figure 8, comparing encryption/decryption time of the proposed PHF technique with ECC and the existing ciphertext attribute-based encryption (CABE), Modified CABE (M-CABE) and Advanced Encryption Standard (AES) techniques have shown how the proposed technique has given shorter time for both processes and, hence, has outperformed the existing techniques.

TABLE 2
ENCRYPTION TIME OF THE PROPOSED SCHEME.

Key size (bits)	*CABE*	*M-CABE*	*AES*	*ECC-RWA*
128	*7.2*	*6*	*5*	*2.3*
192	*8*	*7*	*6.2*	*5*
256	*12*	*9*	*7.4*	*6.2*
512	*15.3*	*11*	*9*	*7.8*
1024	*17*	*13*	*11.3*	*9.3*

Regarding the average of computation time calculation, the retrieval process is finally done as illustrated in Figure 9.

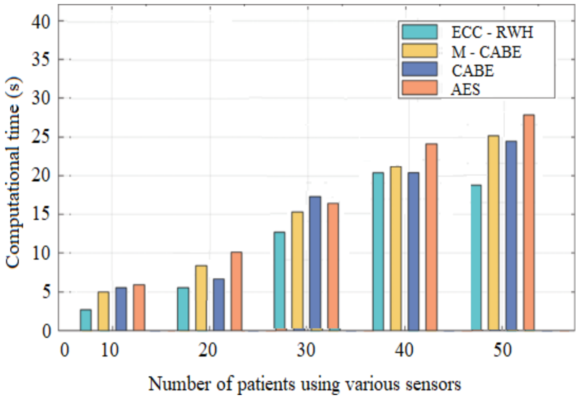

Figure 9: Computational Time Complexity

The average computation time is mainly calculated by computing the time consumed starting from handling the user's request until the retrieval process is finally done as shown in the figure.

Comparing computation time calculations of the proposed technique and the already existing ones has proven the former's abilityto store and retrieve data in a comparably shorter computational time while maintaining security and considerably high speed as well.

CONCLUSION AND RECOMMENDATION

Maintaining privacy security of healthcare applications in IoT cloud environment has been recently a matter of great interest to many researchers, and, hence, the proposed AI-based security has been presented. Its main purpose was to store and retrieve data efficiently taking into consideration all the challenges that the existing systems are already facing. Attempting to secure the patient's data right from the packet transmission initiation point by applying complicated encrypting methods to the IoT sensor devices, made the proposed system quite unique in terms of achieving total security for the sent data. The PHF technique along with the RH key generating processes have worked together in detecting attacks instantly and ensuring data storage and retrieval using the ECC mechanism as well.

The Proposed AI-based security system presents a training model with a set of attack features that can instantly detect potential attacks and inform the routing device to block it right away. This technique will guarantee data security before even reaching the cloud network and, hence, prevent any intruder/hacker from violating this data. Moreover, this system guarantees that the receiver end will not be able to decipher the message unless he knows the newly created keys used in the encryption process from the very beginning. This system has managed to carry out better encryption and decryption processes utilizing the security pattern and data matrix's hash value to generate a random key that ensures data storage and retrieval in IoT cloud environment and, hence, resulting in more efficient encryption and decryption processes, respectively.

Various evaluation measures have been used to evaluate and compare the performance of the existing ones to the proposed technique. Finally, this system has shown promising results in terms of securing critical data transmission through access points to reach its destination safely without any intrusions. Moreover, IoT sensor driven security will be tackled and studied on a wider scale in the future. This AI-based security system could be applied to other real time application systems and random key generation and trust agreement processes could be used on a wider scale in the future to maintain healthcare IoT data security.

REFERENCES

[1] Kashani, Mostafa Haghi, et al. "A systematic review of IoT in healthcare: Applications, techniques, and trends." Journal of Network and Computer Applications, vol 192, no. 2, pp.103-164, 2021.

[2] Greco, Luca, et al. "Trends in IoT based solutions for health care: Moving AI to the edge." Pattern recognition letters, vol.135, no. 11, pp. 346-353, 2020.

[3] Gopalan, Subiksha Srinivasa, Ali Raza, and Wesam Almobaideen. "IoT security in healthcare using AI: A survey." 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA). IEEE, 2021.

[4] Khatkar, Monika, Kaushal Kumar, and Brijesh Kumar. "An overview of distributed denial of service and internet of things in healthcare devices." 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH), pp. 44- 48, 2020.

[5] Rasool, Raihan Ur, et al. "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML." Journal of Network and Computer Applications, pp. 103-132, 2022.

[6] Ghaffarian, Seyed Mohammad, and Hamid Reza Shahriari. "Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey." ACM Computing Surveys (CSUR), vol. 50, no. 4, pp. 1-36, 2017

[7] Elhoseny, Mohamed, et al. "Hybrid optimization with cryptography encryption for medical image security in Internet of Things." Neural computing and applications, vol. 32, no.9, pp. 10979-10993, 2020.

[8] El Zouka, Hesham A., and Mustafa M. Hosni. "Secure IoT communications for smart healthcare monitoring system." Internet of Things, vol. 13, pp. 1-14, 2019.

[9] Das, Sangjukta, and Suyel Namasudra. "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure." Computers and Electrical Engineering, vol. 101, pp. 107-119, 2022.

[10] Challa, Sravani, et al. "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks." Computers & Electrical Engineering, vol. 69, pp. 534-554, 2018.

[11] Khadidos, Adil O., et al. "Healthcare data security using IoT sensors based on random hashing mechanism." Journal of Sensors, pp. 1-17, 2022.

[12] Desnitsky, Vasily, Andrey Chechulin, and Igor Kotenko. "Multi-Aspect Based Approach to Attack Detection in IoT Clouds." Sensors, vol. 22, no.5, 2022.

[13] Yao, Xuanxia, et al. "A lightweight multicast authentication mechanism for small scale IoT applications." IEEE Sensors Journal vol. 13, no. 10, pp. 3693-3701, 2013.

[14] Basi, Mahmoud Norain Mahmoud. Enhancement of Security for Electronic Record using Virtual Local Area Networks Techniques. Diss. Sudan University of Science and Technology, 2019.

[15] Joudar, Shahad Sabbar, A. S. Albahri, and Rula A. Hamid. "Triage and priority-based healthcare diagnosis using artificial intelligence for autism spectrum disorder and gene contribution: a systematic review." Computers in Biology and Medicine, 2021.

[16] Thakare, Vaibhav, Gauri Khire, and Manisha Kumbhar. "Artificial Intelligence (AI) And Internet of Things (IoT) In Healthcare: Opportunities And Challenges." ECS Transactions vol. 107, issue no. 1, pp. 7941-7956, 2022.

[17] Li, Wei, Chai, Y., Khan, F., Jan, S. R. U., Verma, S., Menon, V. G., & Li, X.,"A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system." Mobile networks and applications vol. 26, pp. 234-252, 2021.

[18] Gopalan, Subiksha Srinivasa, Ali Raza, and Wesam Almobaideen. "IoT security in healthcare using AI: A survey." 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2021.

[19] Hayyolalam, V., Aloqaily, M., Özkasap, Ö., & Guizani, M., "Edge intelligence for empowering IoT-based healthcare systems." IEEE Wireless Communications, vol. 28, no. 3, pp. 6-14, 2021.

[20] Kang, Baoyuan, Han, Y., Qian, K., & Du, J., "Analysis and improvement on an authentication protocol for IoT-enabled devices in distributed cloud computing environment." Mathematical Problems in Engineering, 2020.

[21] Siam, Ali I., Mohammed Amin Almaiah, Ali Al-Zahrani, Atef Abou Elazm, Ghada M. El Banby, Walid El-Shafai, Fathi E. Abd El-Samie, and Nirmeen A. El-Bahnasawy., "Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications." Computational Intelligence and Neuroscience, 2021.

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

[23] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R., "Threat analysis of IoT networks using artificial neural network intrusion detection system." 2016 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6, 2016.

[24] Chang, D., Li, L., Chang, Y., & Qiao, Z., "Cloud computing storage backup and recovery strategy based on secure IoT and spark." Mobile Information Systems, pp. 1-13, 2021.

[25] El Zouka, Hesham A., and Mustafa M. Hosni. "Secure Authentication and Session Key Management Scheme for Distributed Sensor Networks." 2022 International Conference on Computing, Electronics & Communications Engineering (iCCECE). University of Essex, Southend, UK, IEEE, 2022.

[26] Al-Muhtadi, Jalal, et al. "Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment." Health informatics journal, vol. 25, issue no. 2, pp. 315-329, 2019.

[27] El Zouka, Hesham and Hosni, Mustafa, "Time Granularity-based Privacy Protection for Cloud Metering Systems. ", Advances in Science, Technology and Engineering Systems Journal (ASTESJ), vol. 5, issue no 6, pp. 1278-1285, 2020.

[28] Lee, Choong Ho, and Hyung-Jin Yoon. "Medical big data: promise and challenges." Kidney research and clinical practice vol. 36, no.1, pp. 3-17, 2017.

[29] Raghuvanshi, Abhishek, Umesh Kumar Singh, and Chirag Joshi. "A review of various security and privacy innovations for IoT applications in healthcare." Advanced Healthcare Systems: Empowering Physicians with IoT- Enabled Technologies, pp. 43-58, 2022.

[30] Das, Sangjukta, and Suyel Namasudra. "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure." Computers and Electrical Engineering, pp. 101-112, 2022.

[31] Rashid, Mamoon, et al. "Securing E-Health IoT data on cloud systems using novel extended role based access control model." Internet of Things (IoT) Concepts and Applications, pp. 473-489, 2020.

[32] Gopalan, Subiksha Srinivasa, Ali Raza, and Wesam Almobaideen. "IoT security in healthcare using AI: A survey." 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), IEEE, 2021.

[33] Newaz, AKM Iqtidar, et al. "Adversarial attacks to machine learning-based smart healthcare systems." GLOBECOM 2020, 2020 IEEE Global Communications Conference, 2020.

[34] Habibzadeh, Hadi, et al. "A survey of healthcare Internet of Things (HIoT): A clinical perspective." IEEE Internet of Things Journal vo. 7, no. 1, pp. 53-71, 2019.

[35] Sadek, Ibrahim, et al. "Privacy and security of IoT based healthcare systems: concerns, solutions, and recommendations." How AI Impacts Urban Living and Public Health: 17th International Conference, ICOST 2019, New York City, NY, USA, October, 2019, Proceedings 17. Springer International Publishing, 2019.