International Journal of Mathematical, Engineering and Management Sciences
Vol. 8, No. 5, 1006-1023, 2023
https://doi.org/10.33889/IJMEMS.2023.8.5.058

Secure Authentication and Data Transmission for Patients Healthcare Data in Internet of Medical Things

Anup Patnaik
Institute of Computer Science & Information Sciences,
Srinivas University, Mangalore, Karnataka, India.
Corresponding author: patnaik.a@hotmail.com

Krishna K. Prasad
Institute of Computer Science & Information Sciences,
Srinivas University, Mangalore, Karnataka, India.
Email: krishnaprasadkcci@srinivasuniversity.edu.in

(Receive on April 26, 2023; Accepted on July 2, 2023)

Abstract
Currently, data transmission is an expanding area in healthcare, enabling health practitioners to examine, assess, and manage patients using mobile communication technologies. To identify and analyze a patient, healthcare providers need to access the physician's Electronic Medical Record (EMR), which may contain extensive audiovisual big data such as MRIs, CT scans, PET scans, X-rays, and more. To ensure accessibility and scalability for healthcare workers and consumers, the EMR needs to be stored in large data repositories on cloud servers. However, due to the sensitive nature of medical information stored in the cloud, the healthcare profession faces numerous security challenges, with data theft attacks being one of the most critical vulnerabilities. This research focuses on protecting medically sensitive data in the cloud by leveraging cloud computing facilities. The upgraded AES approach ensures that confidential data is securely accessible and stored. In addition, improved Elliptic Curve Cryptography (ECC) is utilized for key generation and validation. A hybrid optimization approach, combining robust optimization and genetic algorithms, is employed to select unique and distinct keys. Decryption is performed using deep neural networks, and Convolutional Neural Networks (CNN) enable batch encryption of multiple documents. The comparison between old methods and the proposed approach is based on encryption time, decryption time, and security strength.

Keywords- Telemedicine, Internet of medical things, Convolutional neural networks, ECC technique, and AES approach.

1. Introduction

One of the emerging fields of research in e-health is communications. When remote doctors request EMRs within the outpatient clinic that include MBD, photos, and multimodal medical information, they are instantly delivered through an unprotected internet connection (Li et al., 2017; Jan et al., 2021a). The medical cloud architecture would make it much easier to gather all of a person's different health data when they move between institutions; as a result, the knowledge of the caregivers can be easily monitored and regulated. As shown in Figure 1, the hospital internet is a cloud-based storage architecture where all patients and healthcare customers may connect during cloud storage. By providing online services, medical cloud computing offers advantages over both software and hardware (Pirbhulal et al., 2019; Lone et al., 2020). According to the NIST (2009) definition of cloud computing, it is "a prototype for having convenient, on-demand network access to a common pool of configurable things (e.g., connections, server farms, collection, software, and assistance) that can be right at the right time and published with little effort in managing or service provider engagement". The Internet of Things (IoT) is changing the healthcare industry because it enables significant connectivity between physicians, medical equipment, clinicians and medical technicians, and patients to make real-time monitoring easier. Due to the size and variety of the internet, there are benefits and drawbacks to gathering and transmitting information. To ensure safety and privacy, patient data, including medical conditions and medical equipment used by such customers, must be protected. Professionals in the healthcare industry discreetly communicate information to research health and provide customers with treatment on time (Vandanna and Venkateshwarlu, 2020; Chang et al., 2023). Deep learning (DL) techniques are commonly used in combination with cryptosystems and fingerprint systems to authenticate, detect anomalies, and demonstrate resistance to medical systems. The most important issue to be addressed when building a protection system based on subterranean algorithms is harmonizing protection and efficacy since sensing in networks is accomplished by electrical devices. The Internet of Medical Things (IoMT) is providing a range of opportunities for our personal lives and healthcare. A healthcare expert may remotely operate these technologies and obtain patient data via sophisticated sensors that are connected to them. Privacy regulations and cybersecurity in healthcare institutions are becoming important factors as a result of this trend. A common practice to ensure information security is to perform authentication before beginning a data transmission. The privacy and quality of health data have become major problems for apps that provide healthcare services as a result of the Internet of Things (IoT) enormous rise in the healthcare industry.

This study offers a hybrid security strategy for defending text data diagnostics. These advanced algorithms are also used to safeguard private data from implanted devices, provide availability and secrecy, and improve the quality of services provided by healthcare systems. The present paradigm for smart healthcare is thought to include IoMT as a crucial component. The source-of-energy nature of IoMT devices, their diversity, and the sheer number of IoMT users, on the other hand, make IoMT systems vulnerable to a variety of threats. As a result, IoMT security presents a significant and challenging barrier for IoMT systems (Saif and Biswas, 2020). Essential security requirements include access control, resource availability, and data privacy and confidentiality (Das et al., 2015; Adeli et al., 2021; Jan et al., 2021b). User and device authentication, which is essential for directly or indirectly satisfying security requirements, is the first barrier to entry for IoMT systems. The researchers of this study were inspired to evaluate IoMT authentication approaches to get relevant insights from the IoMT authenticating literature. To provide academics with a broad grasp of IoMT authentication, the publication also develops a detailed taxonomy (Guo et al., 2020; Lai et al., 2021).

The suggested technique is shown to be safer against many common threats, such as loss of service, router assault, and sensor assaults, by extensive empirical analysis and simulated results. The recommended method has enhanced patient health assessment processes in terms of resistance (Kumar et al., 2018; Annane et al., 2022; Kore and Patil, 2022). We present a safe downlink and identification based on the encryption-based Simulated Annealing and Convolution. The important aspects and accomplishments of this paper are summarized as follows:

- We provide a safe solution for the medical data acquired from the Internet of Things in current medical systems.
- An Optimization-based Elliptic Curve Cryptography (Optimized-ECC) is given for the authentication of users and also Improved Advanced Encryption Standard (I-AES) is used for increasing medical data security during the data transmission phase.
- To improve the encryption and decryption processes, a Convolutional Neural Network (CNN) is used for encryption and decryption using a secret key of the AES algorithm.
- The suggested technique beats current illness prediction systems based on confidentiality and security, based on the outcomes of the testing.

The article is as follows: Section 2 discusses the background of the IoT in medicine, safety and privacy challenges, and the importance of transfer learning in the security business. In Section 3, the research on documented privacy protection approaches in medical IoT is evaluated. Section 4 outlines the suggested privacy protection strategy by developing a prototype system. In Section 5, Analysis is done with graphs by evaluating three typical procedures. Lastly, Section 6 gives the findings and future directions for research.

2. Background

2.1 IoMT Architecture

- To get the healthcare data to the third tier, the network layer sends it from the data collection layer across a wired or wireless network (i.e., the data management layer). This layer transfers data and links all of the network's medical devices.
- The compatibility here between diverse entities being used is assured in the data management layer by utilizing the middle-ware apps and services required by IoMT applications and users. This layer also offers other crucial functions, including handling, analyzing, and storing the gathered medical data.
- Intelligent communication between such a user and the IoMT system is supported at the application level. Here, the user can simply connect medical devices, manage them, and view medical data.
- By addressing various aspects such as security, interoperability, data privacy, implementation complexity, data analytics, real-time monitoring, system resilience, and cost in the design and implementation of IoT architecture, healthcare organizations can facilitate a secure, interoperable, privacy-aware, and efficient ecosystem. This will leverage the potential of IoT technologies to improve patient care and healthcare outcomes.

2.2 Healthcare Applications

- Pervasive computing is used by monitoring applications to remotely monitor a patient's health for preventative measures. This list includes common uses such as blood pressure, glucose, electrocardiogram (ECG), asthmatic, and oxygenation level monitoring.
- To identify disorders, diagnostic applications mostly leverage the semantics described in electronic medical records. The caliber of the data gathered by the IoMT devices, as well as the predetermined observations in the electronic medical record, heavily influences how effective these applications are.
- Therapeutic applications involve remote interventions that can pose various challenges depending on the level of intensity required. Remote surgery is an example of such usage. Implementing therapeutic Internet of Medical Things (IoMT) solutions does not impact the workflow as it requires advanced technologies and specialists from multiple domains.
- Applications for rehabilitation are primarily used to pinpoint patients' issues and aid in their recovery of everyday functioning. The treatment and rehabilitation system is an illustration of a rehabilitation application.
- An Optimization-based Elliptic Curve Cryptography (ECC) is a cryptographic algorithm used for secure authentication of users. It provides strong security with smaller key sizes compared to other encryption algorithms because of its mathematical properties of elliptic curves. In addition to ECC, the Improved Advanced Encryption Standard (I-AES) is an enhancement or modification of the Advanced Encryption Standard (AES), which is widely used for its security and efficiency. I-AES is employed during the transmission phase of medical data to encrypt the data and protect it from unauthorized access. This helps maintain the confidentiality and integrity of sensitive medical information. Combining ECC for user authentication and I-AES for data transmission security creates a robust security framework. It ensures that only authorized users can access the system and that medical data remains confidential and secure during transit (Table 1).

Table 1. Leveraging security measures for healthcare applications.

Healthcare Application	Leveraging Advanced Models
Secure Data Transmission	• Secure key exchange and authentication • Encryption of data for confidentiality and integrity during transmission
Patient Data Privacy	• Secure authentication and access control Encryption of data to prevent unauthorized access
Telehealth and Remote Monitoring	• Authentication of remote devices • Encryption of data during transmission between devices and healthcare providers
Medical Device Security	• Secure authentication and communication Encryption of data transmitted by medical devices
Health Information Exchange	• Secure connections and authentication • Encryption of exchanged data for confidentiality and integrity

2.3 IoMT Devices

Implanted cardiac devices are put into patients' bodies to aid doctors in performing surgical and diagnostic procedures. Some of these gadgets include an implanted heart sensor and a camera capsule tiny enough to be eaten.

- Different types of sensors are incorporated into wearable accessories to create wearable devices. Necklaces, wristbands, shoes, and watches are a few examples of these accessories.
- Patients' PCs are outfitted with usable gadgets for particular functions. These frequently assist people in obtaining various services in daily life. An acceptable device that can be connected to an asthmatic person's smartphone or tablet is an air quality meter.
- Anchors for nearby gadgets can be found on beds, desks, and doors. These devices don't need to be carried by patients. When using sensors like those for doors, motion, pressure, or temperature, interaction with all these devices is intuitive. When unusual indicators are observed, they are expected to notify patients, their family members, or healthcare professionals. To assist patients in tracking daily activities, such as the quantity and quality of restroom trips, these gadgets are aware of the patient's context.

3. Related Work

Concerning to the Internet of Things, several researchers have studied authentication systems. Some IoMT system authentication difficulties have only been partly solved by this study. Scientists claim that their solution is secure against typical vulnerabilities in the context of RFID access control (Adeli et al., 2021) and have proposed a small, precise fingerprint method for digital health settings. However, in this paper, we give a more thorough examination of this method and show that their protocol is weak to a man-in-the-middle attack. Furthermore, we demonstrate that other security requirements like forwarding transparency, isolation, and unlinkability aren't fully met by their protocols. To address these issues, we propose a novel strategy and demonstrate that it can withstand typical attacks while using 23% fewer CPU resources and 50% less network bandwidth than existing methods. We also specifically test the recommended protocol's security using the Haunter tool, a commonly used computational tool for this purpose.

For network-enabled healthcare devices (IoMT), authors (Jan et al., 2021b) created a lightweight and reliable authentication technique that addresses all the issues raised in the existing research. Technically, BAN logic and ProVerif2.02 have been used to investigate the recommended system's safety, and intuitively, a practical explanation has been used to assess the safety. In a similar vein, the data visualization outcome at the end of the research shows a careful balance of safety with efficiency that is frequently lacking in the current techniques. Today, there are more and more patients every day in many parts of the world. A wide range of changes take place in a clinical environment. Undoubtedly, the body sensor network, which is used for IoT research purposes, is a crucial technology in the health industry. A lot of health monitoring may be found in operational hazards rather than in the atmosphere. Patient data cannot provide complete assurance for this kind of device. Various current plan prices are affordable when considering energy use, delay, and connection expenses. In this work, a safe method for Trust Attribute-based

Lightweight Authentication (TALA) for IoT Health Care was provided. This method provides IoT security. The recommended technique achieves precision, minimizes transmission overhead, and limits latency (Vijayakumar et al., 2019).

Cyber-Physical Systems (CPS) based on the Internet of Medical Things (IoMT) are essential in the era of smart healthcare because they can access, monitor, assess, and prescribe to patients anywhere. For these platforms to continue to be trusted by users, healthcare professionals, researchers, and other affiliated organizations, efficient authentication and private file transmission must be overcome. In this paper, we propose a compact hybrid deep-learning protocol to integrate security and privacy to address the key exchange protection concerns in the healthcare industry. By using an MPPT algorithm to posit and transmit the verification qualities of physician wearables to the next concerned central source, when it started shifting from one area to another region, we helped to facilitate the federated confirmation of legitimate physician wearable technologies to minimize computation complexity, verification time, and interaction overhead cost. When compared to previous research, simulations of quick shots of the ML technique demonstrated remarkable security mechanisms with the cost-effective verification of legal client wearables and practical communication features. However, it would have been very difficult to employ IoT- based implanted implants and run such a big, complicated medical IoT system on standard single-Cloud Platforms (CP). For a fifth-generation IoMT platform, we provide a scalable FC with a cryptocurrency design. This research proposes a safe cryptocurrency fog BMIoMT exchange of information to function on an FC architecture with flowing effects, little overhead cost, and secure storage (SS) (Almaiah et al., 2022). We have recommended an updated and improved recuperation-based digitally signed approach with batch communications validation that boosts the computation performance of the basic algorithm for the identification of the most recent report in WBAN. For digitally signed creation using the suggested method, one-way hash calculation is not necessary. To confirm the security and confidentiality of communications against various attacks, an evaluation of the recommended work has been provided. The results show that the digitally signed validation approach has improved performance (Kumar et al., 2018). However, significant research has been done on data encryption at the HetNet physical layer, and as a result, the number of hardware devices has increased. In addition to being costlier, the increasing hardware needs also use more energy. Therefore, our work suggests an alternative method for HetNet protocol stack-level communication security.

Nevertheless, addressing security flaws at the network level increases processing complexity. However, several encryption techniques have been used in the past to protect data, including identity-based encryption (IBE), symmetric key encryption (SKE), and public-key encryption (PKE). This research utilizes attribute-based encryption (ABE) identification to protect health data for clinical purposes due to its inherent drawbacks. This tactic prevents the attackers from entering, which reduces the amount of communication required. This authentication mechanism aids in protecting sensitive data from attacks by attackers. A third-party website is included in it to validate and save patient data. A tool called AVISPA (automatic verification of online security protocols and applications) is used to analyze the outputs once the whole security strategy has been specified in the form of HLPSL (high-level protocol specification language) coding. Telecare Medical Information System (TMIS), a typical e-health application, may assist patients and medical personnel in monitoring and connecting for medical assistance. However, since TMIS often uses unreliable mainstream networks, it must provide a secure authentication mechanism to fulfill its strict privacy, data security, and authentication requirements. Lone et al. (2020) presented a biometric-based remote authentication method with reliable transmission and client privacy and security. Nevertheless, to see whether it is vulnerable to identity fraud assaults, user account hijacking, active attacks, and key compromised spoofing. To address these issues, we will update the original system, offer supporting evidence, and subject it to a rigorous analysis. To demonstrate that our method can withstand likely assaults and provide special security features, we also give a thorough heuristic safety study. Finally, a statistical analysis shows that the altered technique has improved integrity without significantly increasing computation costs (Guo et al., 2020). Downloads and image exchanges between medical practitioners for diagnostic purposes are among them. The category represented in telehealth applications and systems must be safeguarded since the electronic notice communication between doctors and patients contains important data. Integrity and message integrity, two key components of security, are closely tied to encryption. The message authentication code may have provided integrity and ensured that the receiver could verify that the information came from the source. The purpose of this research is to construct a secure message identification code for a telemedicine proposal as well as to verify, investigate, and expose data security and authentication as data security objectives in healthcare services. We enhanced the Java versions of the SHA2 MAC generation process. Using two similar MAC tags, the patient may be sure that the communication came from the doctor (authorization) and that the data was not changed or updated while en route (message integrity). We concluded that integrity and message integrity are essential components of digital doctor-patient communication (Lim et al., 2018). Deep learning (DL) methods are often used in cryptosystem, and fingerprint systems to detect irregularities and ensure healthcare procedures are secure. When developing a protective system that is based on deep-learning algorithms, safety, and efficacy must be matched since sensing in networks is power equipment. This is the most important factor to be handled. To protect data with an overhead rate of 67.08%, an encryption time of 58.72 ms, and a decryption time of 62.72 ms (Padinjappurathu et al., 2022). Further, the IoMT model can be strengthened through the use of Blockchain technology (Ghubaish et al., 2020) and Electronic medical reports (EMRs) primarily consist of patient-related clinical data that is provided by the patient to the medical practitioner or healthcare provider (Dilawar et al., 2019). These EMRs are confidential and crucial for providing optimal treatment to the patient. Diagnostic labs can also generate electronic medical reports (EMRs). The Cloud-Based Medical Healthcare (CBMH) system is a standardized platform that provides support to patients seeking emergency treatment through Internet communication from medical experts. Given the sensitivity of medical records, ensuring security protection is essential. Additionally, patient anonymity needs to be well preserved (Farahat et al., 2018; Parah et al., 2020). Secure and Energy-Efficient Framework for IoMT (SEF-IoMT) employs cipher block chaining to forward data in the form of chains, increasing the security level of e-healthcare data against malicious traffic (Saba et al., 2020; Nagarajan et al., 2021).

4. Proposed Work

The IoT innovations usage in the healthcare application domain creates convenience for primary and specialty care as they connect to the healthcare field. Several illnesses could be lowered by doing a proactive check of one’s wellness. Yet privacy problems are enhanced by employing service users’ illness details and medical data. The scientific data’s confidentiality and safety difficulties might occur due to a delay in clinical performance, which may potentially risk the patient's health.

4.1 System Model

To facilitate accurate illness forecasting in an enhanced Healthcare System (HCS), this paper presents an efficient approach that ensures excellent privacy protection for doctors' IoT data, preserving the confidentiality of service users' healthcare data and maintaining the design's trustworthiness.

The described system consists of two main components: verification and private data transfer. Various IoT sensors are installed on the physician's body, and the patient can connect with the corresponding institution through an inpatient smartphone app or website. Once the connection is established using an appropriate suggested signature scheme, the sensor data is securely detected and transferred to the HCS through the Fog layer. Simultaneously, on the healthcare side, the authorized doctor can securely access the physician's data and analyze it using an established system. The proposed architectural design of the Private

Information Healthcare Model is presented in Figure 1.

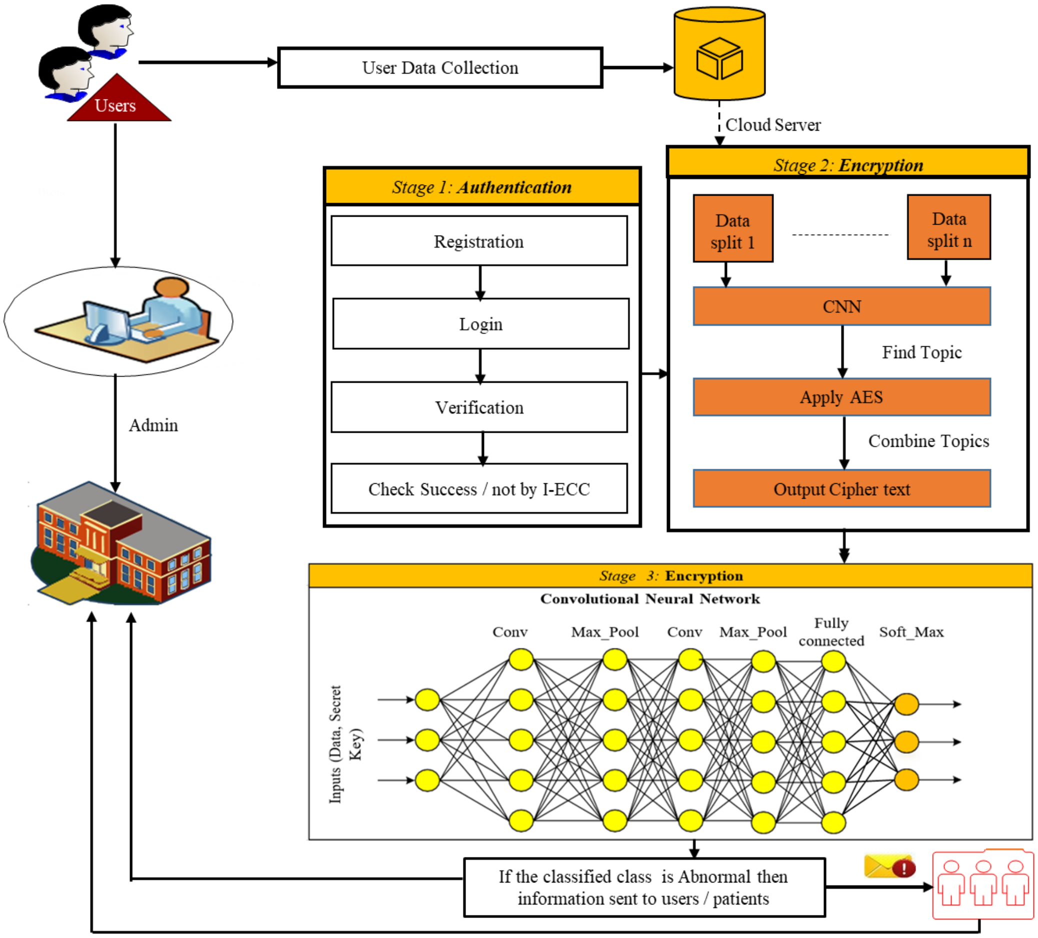

Figure1. System architecture.

4.2 Authentication

Authentication is the process of validating a user identity to prevent the network from unauthorized user access. This authentication mechanism is majorly associated with incoming requests with a set of identifying credentials. The authentication process provides access control for the network by verifying user credentials. Typically, authentication is performed based on two-factor (such as user ID, and password), or multifactor (such as user ID, password, secret key, OTP, and so on). Biometrics are also involved in authentication, which is considered a more secure way of authentication. To increase the privacy of the system and the delivery of data, verification is obtained among physicians, caregivers and the Cloud Server (CS), consumers and the CS, and the medical center and the CS. This level is the initial step in the present scheme. This is a crucial step in enabling access to certified IoT wearable sensors. The verification technique contains 3 phases:

- Registration
- Login
- Verification

4.2.1 Registration

The superintendent's permission is necessary before the information may be viewed on numerous IoT devices linked to health care. After confirmation, the administration gives the data to the IoT system for certification. The four parts included in this signup process are depicted below. Essentially, patient data is supplied by the customer in the registration step. The patient information includes a User, Patient Name, Gender, Birthday, Location, Login, Customer Identification, Vein, MAC, IP Address, Healthcare Card, Doctors Identifier, and so on that are input by the added benefits and maintained on the computer. Patient information may be quantitatively expressed in Equation (1).

$$\tilde{P}_{pd} = \{\tilde{p}_1, \tilde{p}_2, \tilde{p}_3, \dots \dots . \tilde{p}_k\} \tag{1}$$

In basic authentication, the characteristics used to identify an entity are the same ones that are employed to authenticate it. How many factors are necessary to carry out the authentication procedure will determine how accurate and effective the authentication techniques are. Basic authentication typically uses two factors; for entities to access the IoMT system, they must submit both identifying information and biometric information. By developing a shared key between the information exchanged to guarantee secure communication, IoMT authentication can be accomplished. IoMT authentication systems are primarily used to make sure that only authorized users and devices can access system services and features. The authentication processes should therefore be tested against attacks that are successful in gaining access to unauthorized IoMT systems. Here, $\tilde{P}_{pd}$ denotes the patient's detail set and $\tilde{p}_k$ symbolizes the users' characteristics such as gender, name, birth, patient ID, etc. The first process is involved user authentication which is performed based on the vein pattern of the human, MAC address, IP address, and elliptic curve cryptography (ECC) key. The authentication is supported by the cloud server (CS) presented in the second tier i.e., the users involved in the first tier are authenticated in the second tier. The involvement of an effective authentication process ensures that the network is protected from unauthorized users. Further, unnecessary network traffic from unauthorized users is also blocked by authenticating users.in authentication, the vein pattern of a human is considered since the vein pattern of humans is completely different from each other and it is possible to identify the user by comparing vein patterns. The key features presented in vein patterns are the main vein length and the angle at the bifurcation points. These are utilized in user authentication. The proposed authentication scheme is comprised of two phases as follows: (i) setup phase, and (ii) authentication phase. The setup phase is included with following steps,

Step 1: The first step in the setup phase is initiated by CS to identify an elliptic curve (Equation (2)) as follows,

$$E\ (F_2^n) : y^2 + xy = \ x^3 + ax^2 + b \tag{2}$$

where, $a, b\ \in\ F_2^m$ and a generator point $P \in E\ (F_2^n)$with order m.

Step 2: Then, the CS chooses a random number S, which keeps as a private key and computes the public key from a curve point $Spub = SP$.

Step 3: For each user, the CS chooses a random number r and verifier as = r.

Step 4: Each user MUi corresponding values $\{R, r\}$ are keep stored in the database and also kept $Spub$ in memory.

The above four sequential steps are executed to perform the setup phase. After completion of the setup phase, the authentication phase is initiated to allow authorized users into the network. The overall process of user authentication is depicted in Figure 2.

Similar to the setup phase, the authentication phase is involved with following four sequential steps,

Step 1: The authentication process is initiated by TA in order to authenticate the users connected with the network. Thus, TA generates a random number S_1 and computes $S_{pub\,(1)} = S_1 P$. Then it forwards the Query_Message the user as <$Query_{Authentication}, S_{pub(1)}$>.

Step 2: Upon receiving Query Message, the user chooses a random number as S_2 and computes an Elliptic Curve point $S_{pub(2)} = S_2 P$. Then, TA computes $G1 = S_2 S_{pub(1)} S_{pub}$ and an authentication parameter is computed as $a_1 = R \oplus G_1$. After the completion of authentication parameter computation, the user sends response message to TA in order to process the authentication by <$a_1, S_{pub(2)}$>.

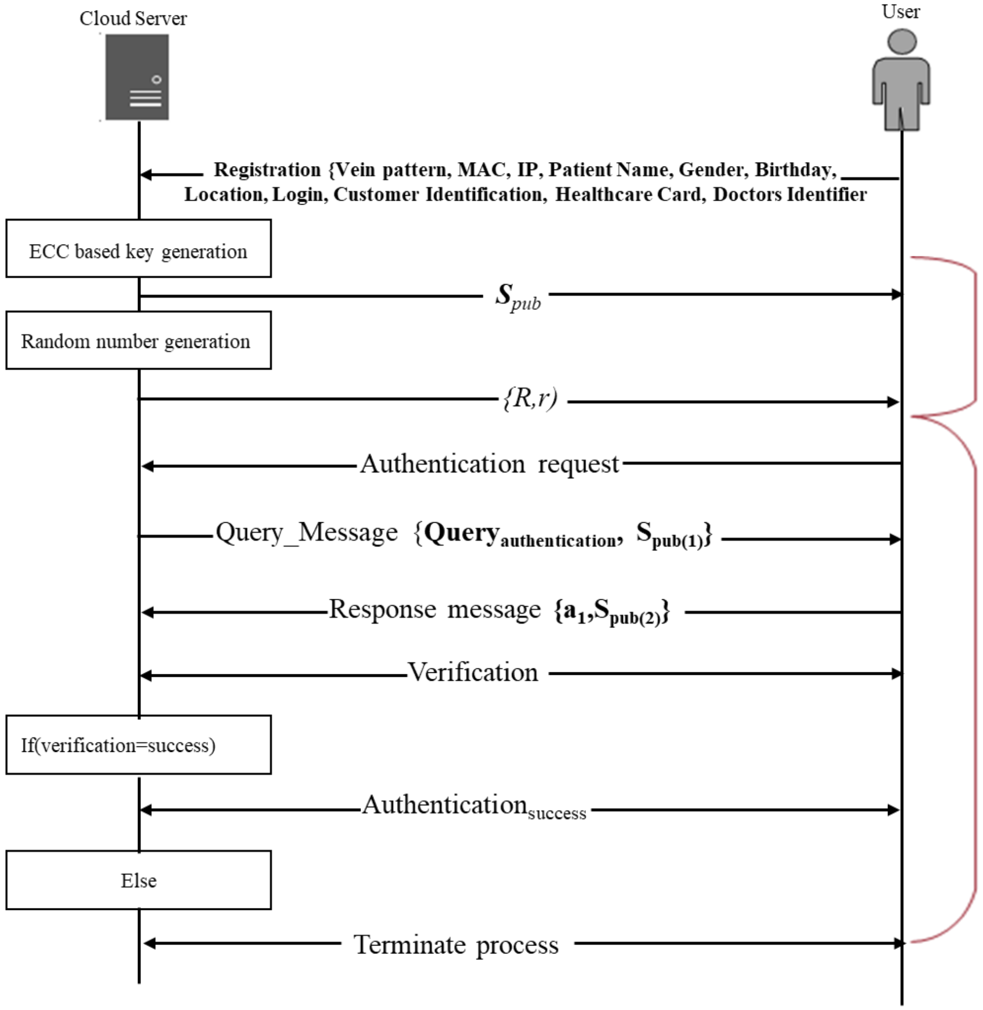
Cloud Server
User
Registration {Vein pattern, MAC, IP, Patient Name, Gender, Birthday, Location, Login, Customer Identification, Healthcare Card, Doctors Identifier
ECC based key generation
S_{pub}
Random number generation
{R,r)
Authentication request
Query_Message {$\mathbf{Query}_{\mathbf{authentication}}$, $\mathbf{S}_{\mathbf{pub(1)}}$}
Response message {$\mathbf{a_1}$,$\mathbf{S}_{\mathbf{pub(2)}}$}
Verification
If(verification=success)
$\text{Authentication}_{\text{success}}$
Else
Terminate process

Figure 2. Authentication process.

Step 3: After receiving response message, the TA determines the R' value as follows in Equation (3),

$$R' = a_1 \oplus S_1 S_{pub(2)} S_{pub} \tag{3}$$

The computation of R' value is performed to verify this value to the database, to find whether it matched the user or not. If the value is matched, then TA computes $G2 = S_1R$ and authentication parameter 2 = $R \oplus G2$ and the authentication parameter is sent to the user.

Step 4: By receiving the authentication parameter, the user computes $S' = a2 \oplus rS1$. If the authentication is completed then the user sends an authentication message to the TA or else the process for a particular user is terminated. The authentication success message is sent to TA as follows < $Authenticationsu$, $Spub(D)$ >.

4.2.2 Login

There, the Cloud will generate the decryption key along with the secret address. The access policy has been supplied; nevertheless, the secret key is delivered to the person's address that is given at the time of enrolment; this signifies that cryptography is completed, and the credentials are created. Cloud hosting will query the secret key as fast as the user wishes to see the files. If the user supplies the right secret keys, the decrypt of the Word document is conducted through the hosting company and shown to the user. It shows just encrypts structure, not the real file when the password save is wrong. The mathematical formulation shown in Equation 4 of the key pair, coupled with the secret information generated by the internet, is:

$$\text{CS} \xrightarrow{(\overleftrightarrow{K}''_{pu},\ \overleftrightarrow{K}''_{pr})} \text{User} \tag{4}$$

Thus, K ┴ ↔ pu^" symbolizes the decryption key in addition to K ┴ ↔ pr^" symbolizes the secret key. The encryption key has been calculated to boost the alert status. The password was computed by examining the round log number of the K┴↔ pu^" together with the K┴↔ pr^", which itself is theoretically expressed as (Equation (5)):

$$\overleftrightarrow{K}''_{se} = \log\,(\overleftrightarrow{K}''_{pu} \oplus \overleftrightarrow{K}''_{pr}) \tag{5}$$

Thus, K ┴ ↔ se^" represents the private keys and ⊕ represents the complete logs quantity of the K┴↔ pu^" along with the K┴↔ pr^".

Registration is an information set used for verifying a user. Usually, these include the login as well as the passwords. The login section permits a user for acquiring admittance to an application by submitting their password and username. The sufferers have to enter the identification details given for identification utilizing the administration when signing in to the website. The patient should input the user-id, passwords, and crypto-system when checking in.

4.2.3 Validation

The confirmation process has been carried out when the system has signed in. The program would compare this section's customer, user, passcode, and cryptosystem. The software finalizes that the individual is already identified with the particular Healthcare Cloud Server if all the information is matched. Or otherwise, the system responds to the enrollment step.

4.3 Encryption and Decryption

The proposed system of CNN integrates two features Splitting and Merging. The CNN has 4 layers which are the input layer, hidden layer, full-connection layer, and output layer. In hidden layer also have three sub-layers such as convolution layer, pooling layer, and multilayer which includes the convolution layer and max pooling layer. The input layer performed input splitting operations. The convolution layer denotes the confidential features of the input text. Each convolution function creates a local feature vector. CNN includes 2 methods used to catch the relationship between the data. The pooling layer is used to select the number of features concerning the hidden layer. The output layer has a softmax function, which converts the output value into possibilities of the input data that is subjective or objective. The possible value is calculated as follows (Equation (6)),

$$P\ (i|t,\ \Theta) = \frac{\exp\ (y_i\ )}{\sum_{k=1}^{n} exp(y_k)} \tag{6}$$

where, yi is the input secret key, and yk is the split data Evolutionary methods and simulation annealed have evolved as the dominant techniques for finding and optimizing issues in large dimensional areas. DGA with SA is a revolutionary worldwide optimizer that is capable of preventing the routing loops of GAs and near-optimal solutions. Well at the start of the procedure, startup settings would include the current population, quantity of variables, lower and higher ranges of each variable, mutations, and crossovers rates, selecting technique, annealed and heating factors are specified. Then GA is done and halted within a given amount of generations, which yields the semi-answer for the encoding process. Further, SA uses individual sub-solution from the GA, which creates the global optimum for encoding. Optimizer is a probability search method, which is founded on the selection procedure and genetics. Optimizer is launched with a set of answers referred to as a population. Here the solutions are renowned as "chromatids". For each creation, the populace is retained and at each new gene genetic optimal solution is assessed. An optimization algorithm is used to distinguish between fit and unsuitable alternatives. The efficiency function is a scientific formula that provides differentiated signal agreement with the genetic method. The optimization algorithm of GA is framed using PSNR and NCC variables. It provides a guideline for the progression via a series of work-around toward the final remedy. The chromosomal for the following generations are picked depending on the viability likelihood value. Chosen chromatin must have a larger chance value than the preceding ones. This procedure is repeated till the conclusion of the need is met. Optimizer is handled utilizing the necessary stages:

- *Initialization populations*: Assemble a random number of chromosomal at randomly or with previous information into a weight matrix.
- *Health Analysis*: Analyze the wellness of all chromosomes in matrix M. The health assessment is done by applying optimization techniques that were created.
- *Classification*: Select a group of worthy prospects from array M. Select pairs of chromatids using a random sample graded by wellness.
- *Crossovers*: Conduct collab on the chromatin pairing concerning information, from matrix M to create a set of children 0.
- *Modification*: Employ mutant on the progeny genomes set 0 to get its altered combinations set 0, with a sufficiently low chance.
- *Successor*: Replacing the present demographic M by sets of descendants 0.
- *Terminating*: Verify the cessation, criterion, if not fulfilled, and then go to step 2. Then, end the procedure.

The search algorithm is a clustering version of the approach for estimating the optimal path of a specified sub-optimal function. It is a method of determining optimal solutions from all conceivable possibilities. The key feature given by SA above other techniques is its capacity to prevent global minimums by managing the adoption of expense neighbors by methods of likelihood, which reduces solutions containing a rise in the minimization problem. SA is a storage-less method, this method does not utilize any data obtained during the scan.

- Enter a randomized Ri (starting answer), pick initial conceptual temperatures, and define the warming timetable.
- Calculate this simulated component 〖$E(R$〗 (i).
- Discompose R, the index i to analyze the surrounding layout vectors (R (i+1)).
- Calculate 〖$E(R$〗 $(i + 1)$) utilizing simulated module.
- If 〖$E(R$〗 $(i + 1)) <$ 〖$E(R$〗 i), then, 〖$E(R$〗 $(i + 1)) -$ innovative answer.
- If 〖$E(R$〗 $(i + 1)) >$ 〖$E(R$〗 i), then R (i+1)is novel answer having chance e^(-Δ/T).
- Reduce the temperature, according to the heating time-table.
- Discontinue this program.

The corresponding doctor on the hospital side can download patient data securely and test these data with the already trained system.

5. Results and Discussion

The proposed work was evaluated by using Netbeans 8.2 Integrated Development Environment (IDE). It is an open-source software platform that is proposed for Java applications. Netbeans IDE supports a Java virtual machine which is performed on any operating system. This platform provides many facilities, which are,

- Storage.
- Processing.
- Transmission.
- Analysis.

To assess the performance of Twitter sentiment analysis, data is collected from the online registry. The proposed system's dataset consists of 10,000 instances of various diseases. These processes are executed on machines with a configuration of 2GB of RAM and a 64-bit Windows 10 operating system (Table 2). It is an open-source software platform designed for Java applications, with support from the Netbeans IDE for Java virtual machines. Three performance metrics, namely encryption time, decryption time, and security strength are the primary focus of evaluating authentication algorithms for IoMT. The evaluation of these characteristics depends on the time efficiency of authentication and data transmission in IoMT scenarios with limited resources. Efficient authentication and data transmission processes result in lower costs and a lighter authentication method.

- Encrypted time: It is the disparity between decryption beginning and finishing timings and the time required by the encryption process to generate a cipher text from simple text.
- Decrypted time: The disparity here between encrypted starting and completion timings is utilized to compute it.
- Security Strength: How the proposed security algorithm encrypts the data and how it could be a strong and secure data transfer are mentioned.

Therefore, in terms of security level thinking, encrypted duration, and block cipher, the efficiency of the novel LR-ECC technique is contrasted to that of the current Fully Homographic Encryption (FHE), ECC, RSA, and Diffie Hellman (DH) techniques. The performance indicators comparison is clarified in Figures 3, 4, and 5.

Table 2. Hardware and software requirements.

Software Requirements	Operating system	Window 10
	Language	Java
	IDE	Netbeans 8.2
	Package	XAMPP
	Development Kit	JDK 1.8
	Processor	Intel core
Hardware Requirements	RAM	2GB
	Hard disk drive	256 GB

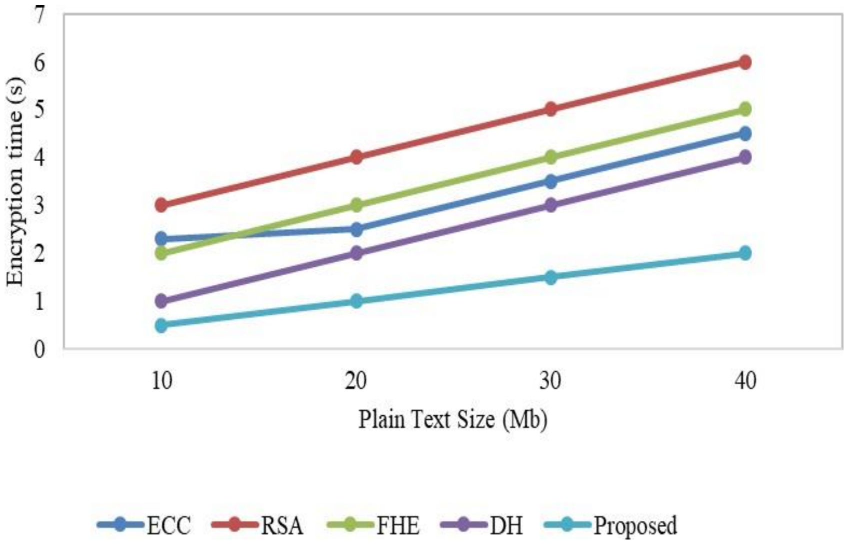

Figure 3. Encryption time.

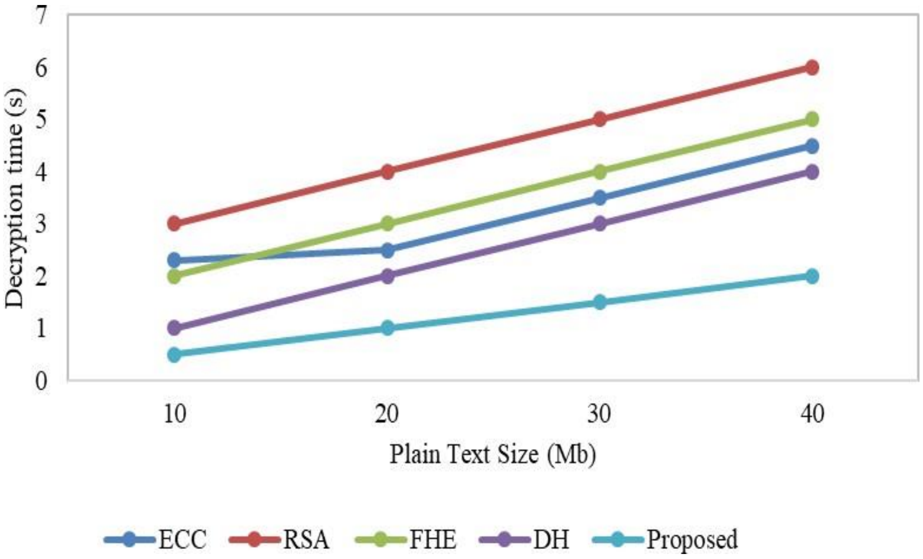

Figure 4. Decryption time.

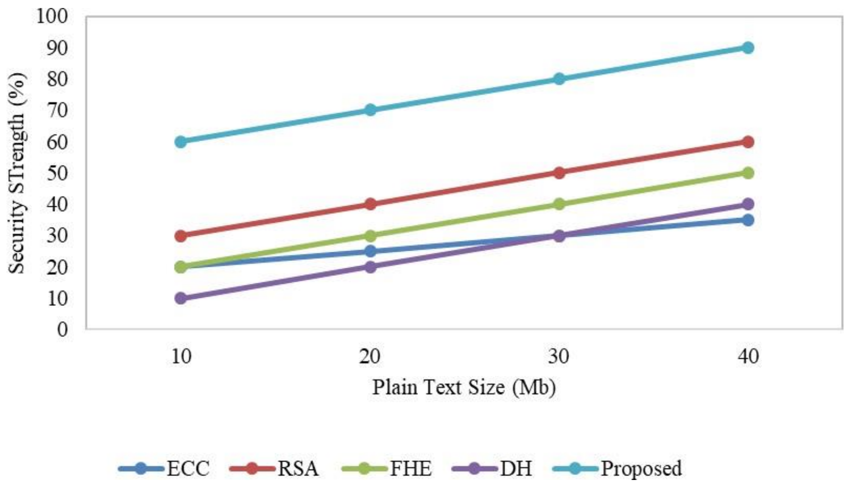

Figure 5. Security strength.

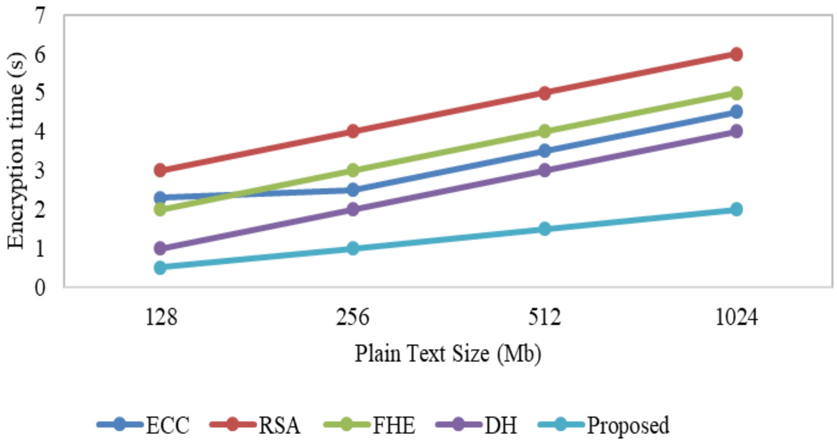

Figure 6. Encryption time.

Considering the process of encryption and decryption, Figure 6 elucidates the suggested proposed work when the earlier data relationship implies the traditional ECC, RSA, FHE, and DH techniques. The file sizes vary from 128 to 1024 bits of plaintext. Figure 7 indicates that the suggested technique requires 20 seconds to encode a 10 kb file. In comparison, the current DH, ECC, FHE, and ECC techniques take 34s, and 52s to encode the data. Conversely, the suggested approach yields superior results for the 128 to 1024-bit range. The ongoing debate consistently showcases the exceptional performance of the suggested method when following standard procedures. The higher security evaluation of the suggested program is highlighted in Figure 8 and Figure 9, which demonstrate the recommended proposed work using standard ECC, RSA, FHE, and DH techniques. The traditional DH algorithm provides 78% security, which is significantly lower. Additionally, the current ECC, RSA, and FHE algorithms offer 25%, 35%, and 60% security, respectively, all of which are also lower than the suggested approach. In contrast, the proposed work achieves a robust security strength of 99.87%. Therefore, the discussion demonstrates that the suggested approach performs exceptionally well when dealing with data relationships using the current approaches.

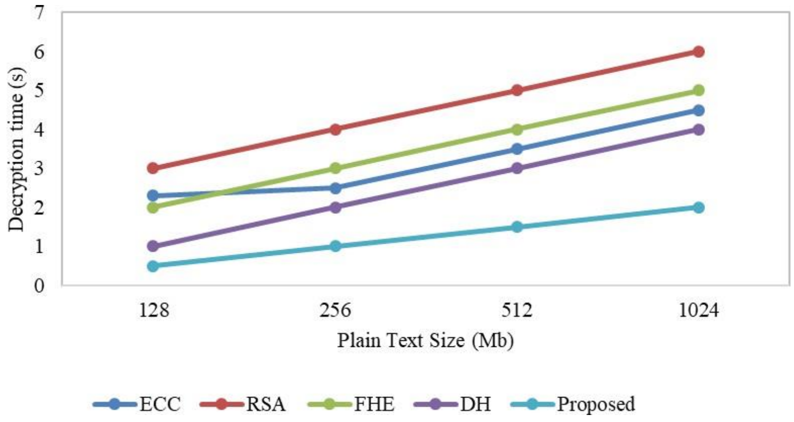

Figure 7. Decryption time.

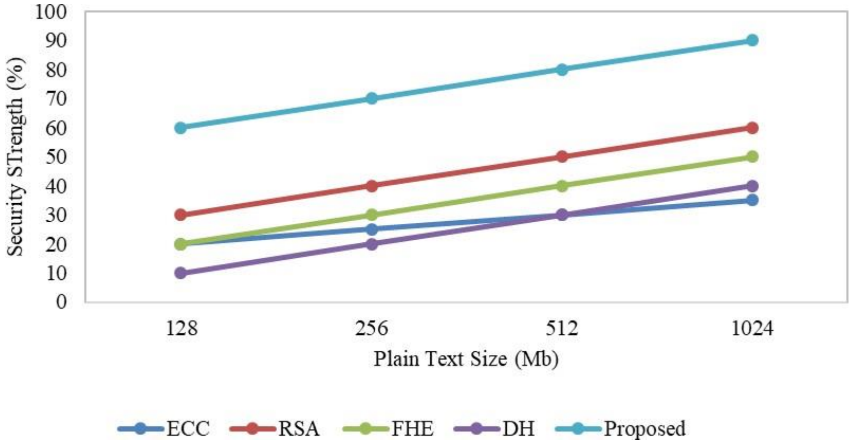

Figure 8. Security strength.

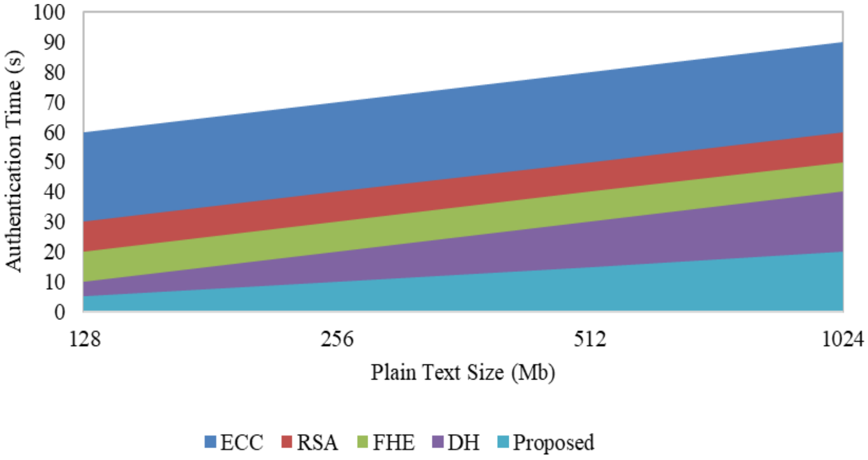

Figure 9. Security strength.

Healthcare organization decision-makers can adopt this model to enhance data transmission and authentication practices, ensuring that all relevant stakeholders are aware of their roles and responsibilities in maintaining the security and privacy of patient information. Depending on the sensitivity of the data and the potential risks involved, it is important to prioritize stronger encryption algorithms with high security strength to effectively mitigate potential risks and vulnerabilities. However, it is crucial to consider the impact of encryption and decryption times on data access and user experience. Striking a balance between security and user experience is essential, considering the needs and expectations of end-users, especially in critical cases. By carefully considering these factors, decision-makers can make informed decisions and implement effective measures to safeguard data while maintaining optimal user satisfaction.

6. Conclusion

IoMT devices are devices are utilized to capture various physiological data, such as skin temperature, pulse rate, breathing rates, electroencephalogram (EEG), electrocardiogram (ECG), and hypertension. These measurements are transmitted using Wireless Medical Sensor Network (WMSN) to remotely evaluate individuals through IoMT. However, transmitting sensitive information over an unencrypted connection in WMSN exposes it to potential risks and necessitates proper safeguards against attackers. To ensure the safety of all involved parties, including healthcare providers monitoring patients or guaranteeing the authenticity, permission, and integrity of data over the network, a robust authentication method is indispensable. This study primarily focuses on securing medically sensitive data in the cloud by leveraging cloud computing facilities. An enhanced Advanced Encryption Standard (AES) technique is employed for retrievable and secure storage of confidential information. Prior to that, an advanced Elliptic Curve Cryptography (ECC) method is used for key generation and validation. A hybrid optimization technique, incorporating robust optimization and genetic algorithms, is utilized to select unique and distinct keys. Deep neural networks are employed for decryption, and Convolutional Neural Networks (CNN) enable batch encryption of multiple documents. Comparisons between new and old methods are made based on encryption time, decryption time, and security strength. Additionally, future advancements may involve the integration of blockchain technology.

Conflict of interest

The authors declare that they have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor-in-chief, guest editors and anonymous reviewers for their comments that help improve the quality of this work.

References

Adeli, M., Bagheri, N., & Meimani, H.R. (2021). On the designing a secure biometric-based remote patient authentication scheme for mobile healthcare environments. *Journal of Ambient Intelligence and Humanized Computing*, *12*, 3075-3089.

Almaiah, M.A., Hajjej, F., Ali, A., Pasha, M.F., & Almomani, O. (2022). An ai-enabled hybrid lightweight authentication model for digital healthcare using industrial internet of things cyber-physical systems. *Sensors*, *22*, 1448. https:// doi.org/10.3390/s22041448.

Annane, B., Alti, A., Laouamer, L., & Reffad, H. (2022). Cx-CP-ABE: Context-aware attribute-based access control schema and blockchain technology to ensure scalable and efficient health data privacy. *Security and Privacy*, *5*(5), e249. https://doi.org/10.1002/spy2.249.

Chang, S.H., Hsia, C.H., & Hong, W.Z. (2023). A secured internet of robotic things (IORT) for long-term care services in a smart building. *The Journal of Supercomputing*, *79*(5), 5276-5290.

Das, A.K., Odelu, V., & Goswami, A. (2015). A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS. *Journal of Medical Systems*, *39*, 1-24.

Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: Securing internet of medical things (IoMT). *International Journal of Advanced Computer Science and Applications*, *10*(1), 82-89.

Farahat, I.S., Tolba, A.S., Elhoseny, M., & Eladrosy, W. (2018). A secure real-time internet of medical smart things (IOMST). *Computers & Electrical Engineering*, *72*, 455-467.

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal*, *8*(11), 8707-8718.

Guo, J., Lu, S., Gu, C., Chen, X., & Wei, F. (2020). Security analysis and design of authentication key agreement protocol in medical internet of things. In *2020 International Conference on Networking and Network Applications* (pp. 233-240). IEEE. Haikou City, China.

Jan, M.A., Khan, F., Mastorakis, S., Adil, M., Akbar, A., & Stergiou, N. (2021a). LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. *IEEE Transactions on Green Communications and Networking*, *5*(3), 1202-1211.

Jan, S.U., Ali, S., Abbasi, I.A., Mosleh, M.A., Alsanad, A., & Khattak, H. (2021b). Secure patient authentication framework in the healthcare system using wireless medical sensor networks. *Journal of Healthcare Engineering*, *2021*, Article ID 9954089. https://doi.org/10.1155/2021/9954089.

Kore, A., & Patil, S. (2022). Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. *Wireless Networks*, *28*, 287-301.

Kumar, S., Tomar, A.S., & Chaurasiya, S.K. (2018). Enhanced secure transmission of data in wireless body area network for health care applications. In *Smart and Innovative Trends in Next Generation Computing Technologies: Third International Conference* (pp. 138-145). Springer, Singapore.

Lai, L., Zhou, T., Cai, Z., Yu, J., Bai, H., & Cui, J. (2021). Leveraging blockchain for cross-institution data sharing and authentication in mobile healthcare. In *2021 17th International Conference on Mobility, Sensing and Networking* (pp. 311-318). IEEE. Exeter, United Kingdom.

Li, C.T., Wu, T.Y., Chen, C.L., Lee, C.C., & Chen, C.M. (2017). An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. *Sensors*, *17*(7), 1482. https://doi.org/10.3390/s17071482.

Lim, C.K., Iipinge, V.J., Tan, K.L., & Hambira, N. (2018). Design and development of message authentication process for telemedicine application. In *2018 IEEE Conference on Wireless Sensors* (pp. 23-28). IEEE. Langkawi, Malaysia.

Lone, T.A., Rashid, A., Gupta, S., Gupta, S.K., Rao, D.S., Najim, M., Srivastava, A., Kumar, A., Umrao, L.S., & Singhal, A. (2020). Securing communication by attribute-based authentication in HetNet used for medical applications. *EURASIP Journal on Wireless Communications and Networking*, *2020*, 1-21.

Nagarajan, S.M., Deverajan, G.G., Kumaran, U., Thirunavukkarasan, M., Alshehri, M.D., & Alkhalaf, S. (2021). Secure data transmission in internet of medical things using RES-256 algorithm. *IEEE Transactions on Industrial Informatics*, *18*(12), 8876-8884.

Padinjappurathu, S.G., Chowdhary, C.L., Iwendi, C., Farid, M.A., & Ramasamy, L.K. (2022). An efficient and privacy-preserving scheme for disease prediction in modern healthcare systems. *Sensors*, *22*(15), 5574.

Parah, S.A., Kaw, J.A., Bellavista, P., Loan, N.A., Bhat, G.M., Muhammad, K., & de Albuquerque, V.H.C. (2020). Efficient security and authentication for edge-based internet of medical things. *IEEE Internet of Things Journal*, *8*(21), 15652-15662.

Pirbhulal, S., Pombo, N., Felizardo, V., Garcia, N., Sodhro, A.H., & Mukhopadhyay, S.C. (2019). Towards machine learning enabled security framework for IoT-based healthcare. In *2019 13th International Conference on Sensing Technology* (pp. 1-6). IEEE. Sydney, NSW, Australia.

Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *Journal of Infection and Public Health*, *13*(10), 1567-1575.

Saif, S., & Biswas, S. (2020). On the implementation and performance evaluation of security algorithms for healthcare. In *Proceedings of the 2nd International Conference on Communication, Devices and Computing: ICCDC 2019* (pp. 629-640). Springer, Singapore.

Vandanna, T.S., & Venkateshwarlu, S. (2020). A secure cloud-assisted Wban health care system using biometric keys and or pattern analyze. *International Journal of Scientific & Technology Research*, *9*(2), 631- 634.

Vijayakumar, K., & Bhanu, V.S. (2019). A secure scheme for trust attribute basedlightweight authentication (TALA) in IOT healthcare environment. *International Journal of Innovative Technology and Exploring Engineering*, *8*(2), 4553-4558.

Publisher's Note- Ram Arti Publishers remains neutral regarding jurisdictional claims in published maps and institutional affiliations.