scientific reports

Check for updates

OPEN

A lightweight and secure authentication and privacy protection scheme for internet of medical things

Sanjay Kumar[1,5], Kumar Abhishek[1,5] & Shitharth Selvarajan[2,3,4,5]✉

The advent of smart healthcare technology has provided various benefits, including remote patient monitoring, personalized treatments, and early disease detection. However, transmitting sensitive patient data through IoMT devices raises significant security and privacy concerns. To protect patients' data and smart medical devices, authentication is required. We uncovered security flaws in the current healthcare architecture, including impersonation, stolen verifiers, and man-in-the-middle attacks. This encouraged us to propose a security architecture that protects patients' data from attacks and guarantees the security of sensitive healthcare information. Our proposed security scheme, ฿-ED-CRY (Bi Encryption Decryption Crypto), is based on Elliptic Curve Cryptography (ECC). It protects patients' sensitive healthcare information by enhancing privacy-preserving mechanisms and validates the effectiveness of our scheme. We implemented the proposed scheme using GCC 4.9.5 and the pairing-based cryptography (PBC) library. The results demonstrate that our scheme performs better than the existing security schemes in terms of privacy and computational efficiency. The computation cost is around 13.3640 percentage lower than other related schemes. This research explores the revolutionary effects of integrated healthcare systems, with an emphasis on the convergence of digital health technologies and patient treatment in real-world IoMT scenarios.

Keywords Internet of medical things, Healthcare, Lightweight, ECC, Schnorr, Authentication

The IoMT enables smart healthcare through interconnected medical devices, facilitating remote patient monitoring, real-time data exchange, and automated diagnostics. However, the security and privacy of patient data remain critical concerns due to various types of attacks. Traditional authentication mechanisms often impose high computational and communication overhead, making them unsuitable for resource-constrained IoMT devices. Therefore, there is a need for a lightweight and secure authentication and privacy protection scheme that ensures data confidentiality, integrity, and efficient access control while minimizing system overhead[1].

The rapid development of electronic devices and connected gadgets has a considerable impact on the speed at which healthcare applications emerge. Because wearables and smartphones have a range of sensors capable of measuring blood pressure, respiration, and heart rate, continuous remote monitoring is feasible at a cheap cost, allowing healthcare workers to treat patients more efficiently. Cloud computing is a remote data storage and management service. Users can gain access to the service via a network, usually the Internet. It enables the user to save files online, making them accessible from anywhere over the internet. The service provider keeps the uploaded files on an external server, making them available to users online[2,3].

The proliferation of IoMT devices in our digital ecology raises new concerns. These issues involve device authentication while conserving bandwidth and storage. Using identity-based cryptography can solve these problems. The Media Access Control (MAC) address of an Internet of Things (IoT) device is used as the public key in identity-based cryptography. It's necessary to perform resource-intensive cryptographic operations. This approach simplifies and scales IoMT authentication, improving efficiency and scalability. Gateway access control policies and MAC address authentication ensure that only allowed devices can connect to the network

[1]Dept of Computer Science and Engineering, National Institute of Technology, Patna, Bihar 800005, India. [2]CSD, Kebri Dehar University, 001 Kebri Dehar, Somali Regional, Ethiopia. [3] Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, India. [4]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, Rajpura 140401, India. [5]Sanjay Kumar, Kumar Abhishek and Shitharth Selvarajan have contributed equally to this work. ✉email: ShitharthS@kdu.edu.et

and communicate safely with cloud services. The Internet of Things ecosystem's growth enhances security and resource use. At its most basic, identity-based cryptography can solve Internet of Things device authentication challenges. The technique allows safe and efficient communication while managing limited resources[4,5].

The number of individuals who are elderly, people who have chronic diseases, and people who have disabilities has greatly increased, which places a huge burden on the existing healthcare system. This is the case despite the rapid improvement of technology that detects and treats diseases. A great number of countries are experiencing difficulties due to a deficiency of medical resources, particularly in light of the COVID-19 epidemic. Many of the patients have been left alone at home because they have not received proper care. As a consequence of all of these problems, there is an immediate need for a healthcare system that is more efficient and adequate in meeting the medical needs of people who live in distant areas. The IoMT is one possible solution to this problem[6].

The combination of radio frequency identification technology, wireless networks, and medical devices equipped with sensors is used to develop remote healthcare monitoring systems. Medical devices collect the health information of patients who are hospitalized for an extended period of time, persons who have disabilities, and the elderly, and then report it to medical professionals, carers, or healthcare facilities in order to provide fundamental medical services. This results in costs being reduced, medical resources being conserved, and accessibility being improved. In most cases, the capabilities of IoMT end devices are not sufficient to handle the categorization, analysis, transmission, and storage of sensor data. This is because the collection of sensor data requires these activities. As a consequence of this, the Internet of Medical Things design usually makes use of cloud data centres in order to offload resource-intensive computing, networking, and storage tasks from healthcare devices. Cloud computing, on the other hand, has limitations in applications that are extremely mobile or delay-sensitive because of the distance that exists between cloud servers and end devices. Furthermore, the raw data that sensors have gathered must be analyzed to identify only the abnormal health data that has to be detected and then transmitted to cloud servers[7].

Motivation

Ensuring the privacy and security of patient health-related information is a significant concern for remote healthcare systems. Wireless communication technologies frequently transmit sensitive patient information in IoMT. This enables attackers to intercept the communication channel and acquire sensitive information about patients. Furthermore, the rapid adoption of IoMT in the healthcare ecosystem makes it substantially more difficult to establish security measures during pandemics, such as the spread of the COVID-19 virus. F-Secure's analysis reveals that hackers exploited 82 percent of Internet of Things devices in the first half of 2019[8]. The existing schemes are vulnerable to attacks and take more computational cost. This motivates us to design a lightweight security scheme that protects IoMT applications from any attacks and takes less computational cost.

Research objective

The objective of this research is to enhance the security and efficiency of smart healthcare systems while ensuring the protection of patients' health information and the effective functioning of medical devices at various points, such as:

- *Enhance Security and Privacy* Address and mitigate security flaws in the current smart healthcare system.
- *Secure Authentication* Implement an ECC-based lightweight signature scheme for robust authentication.
- *Efficient Implementation* Develop a practical application for the secure and efficient tracking of health status in real time.
- *Performance Benchmarking* Validate the scheme's superior performance in comparison to existing solutions.

Research contributions

- Our proposed scheme and security model are based on an identity-based access control system that protects from new attacks in smart healthcare.
- The Bi-Encryption Decryption scheme secures the patients' information from various attacks, and the scheme ensures patient privacy by employing Schnorr signatures upon registration of medical devices with the hospital.
- Our lightweight scheme is more effective for authentication, boasting strong authenticity and preventing unauthorized IoMT devices from cloud environments.
- The security protocol enables recognizing and destroying any adversarial gateway and IoMT appliances from IoMT healthcare environments.
- Conducted a security analysis of the proposed scheme and compared the results obtained by the proposed scheme with existing schemes.

Paper roadmap

The rest of the paper is structured as follows: We describe some related work and preliminary concepts used in this research in Sect. 2. In Sect. 3, discuss the workings of the proposed methodology. In Sect. 4, the security performance of the proposed scheme. Section 5 calculates the performance results of the proposed scheme as well as security comparisons with related existing schemes. Finally, we conclude the paper and provide future direction for this research in Sect. 6.

Related work

In this section, we examined the working methods, applications, and research limits of current schemes. As a result of the advent of the digital age, numerous industries have been presented with an abundance of

opportunities and innovations, which have been characterized by an ever-increasing dependence on technology. However, these improvements also carry with them several challenges, particularly in the realm of cybersecurity[9]. Insider threats, also known as damaging activities that originate from within an organization, have emerged as a significant worry in recent years, despite the fact that outside threats have traditionally been the primary focus of security measures[10].

The use of a trustworthy server that saves the data is a common feature of the methods now in use. Access control relies on software checks to ensure that a person can access a piece of data only if authorized. From a security perspective, this arrangement is not very desirable. We then encrypt the data using the public key of the intended set and classify it according to the hierarchy. There are some drawbacks to these techniques. If a user of a set needs to provide access to a third party to access data for that set, the user must either provide the third party with their private decryption key so that it may access all entries or act as an intermediary and decode all relevant entries[11].

In contrast to conventional PKI, identity-based public key cryptography (ID-PKC) addresses the issue of key authenticity through various procedures. An entity's public key in ID-PKC is directly obtained from distinct characteristics of its identity, such as an IP address that belongs to a network host or an email address that is connected to a user. The public key generator (PKG) constructs private keys for entities. Before launching an attack, the adversary in a typical PKI must issue a new certificate and persuade entities to accept the new public keys. These factors suggest that applications with low-security requirements or small, closed groups could be the only ones permitted the user ID-PKC[12].

The authors present a brand-new public key cryptography paradigm, referring to it as certificateless public key cryptography (CL-PKC)[13]. The search for public key schemes without requirements for certificates and without ID-PKC's built-in key escrow capability provided developers with the idea of CL-PKC. One of the most important issues with public key infrastructures (PKIs) has always been the efficient revocation of public key certificates. In RSA-type cryptosystems, Boneh presented a technique for getting instantaneous revocation of a user's public key privileges[14].

According to the description, the system known as mediated RSA (mRSA) uses threshold RSA, in which both parties share the private key. The encryption and verification processes in the SEM architecture are identical to those in traditional RSA, making it transparent to both the sender and the verifier of a signature. Additionally, adopting SEM design eliminates the requirement to check a public key's status before using it. Users don't need to worry about any certificate's validity before using another user's key to encrypt a message.

Identity-based cryptosystems are another way to streamline key management. This idea was first presented by Shamir in 1984, with the goal of removing as many public key certificates as feasible by enabling a public key to be uniquely generated from the user's identifying data like email address, phone number, and social security number[15].

Additionally, it makes key management simpler because there's no need to maintain a huge database with a list of public keys and their owners. COVID-19 had a significant impact on the healthcare industry, which was the global pandemic problem. The COVID-19 outbreak resulted in an exponential increase in demand for IoMT devices, which then impacted the global market. The IoMT dramatically reduces patient costs, easing the financial strain on individuals and governments. According to a report published by Fortune Business Insights on August 26, 2024, the IoMT market was estimated to be worth USD 47.32 billion in 2023. During the projection period, the market is expected to increase from USD 60.03 billion in 2024 to USD 814.28 billion in 2032, with a CAGR of 38.5 %[16].

The authors present a sensor cloud architecture that uses virtualized physical sensors and dynamic sensor placement based on patient movement and health to continuously monitor high-risk patients[17]. The research uses a threat model to address wearable payment security. For near-field communication pairs of devices, ECC encrypts messages, and biometrics authenticates safe payments[18].

The authors present an identity-based signature system without key escrow that issues private keys without a secure connection. It employs binding–blinding to avoid key escrow and eliminate the need for a secure connection during private issuance[19]. To ensure the confidentiality of patient information while it is shared and integrated across healthcare providers, they offer a system based on knowledge graphs[20]. Fog computing with private blockchain offers a trustworthy method of storing and transferring patient data while simultaneously improving the identification of security risks and bolstering the privacy and security of medical data[21].

The MD5 hash technique securely stores user passwords for use in authentication procedures. Integrating an MD5 checksum into the original patient record file presents an additional barrier to security and verification[22]. To create a cryptographic method that satisfies the essential requirements of contemporary smart healthcare cyber-physical systems, the research uses ECC, hash functions, and digital signatures[23].

An authentication strategy for IoMT devices is proposed to enhance the security and performance of existing authentication schemes. Through the development of an offline authentication model that directly checks identities, the suggested authentication system successfully authenticates users and IoMT devices within the local area network[24]. A scalable and adaptable distributed group key agreement protocol is used to reduce CPU overhead by running elliptic curve Diffie-Hellman using multiplications instead of exponential calculations to secure data transmissions in WSN[25].

The prospect of IoMT-related attacks poses the most severe threat to the security and privacy of patient medical records. The suggested approach protects the secrecy of IoMT devices linked to the patient's body while communicating. The XOR operator, hash function, and concatenation were used to save processing power[26]. An authenticated key agreement protocol for the IoMT using elliptic curve encryption and zero-knowledge proof methods is used to preserve the privacy of patient's critical information[27].

In order to secure the transfer of medical records, a research uses signcryption with an identity-based authentication system based on elliptic curve cryptography. Based on bilinear pairing, the suggested protocol

covers a number of security characteristics, such as data confidentiality and authentication with efficient key management[28].

iSecureHealth, a lightweight and reliable key exchange mechanism, addresses security, authentication, and privacy issues. To secure communication between IoMT sensors and the gateway node, it adds a security control node. The system uses ECDH for key exchange and HMAC-SHA256-based JSON Web Token for session key creation[29].

Our goal in writing this paper is to add to the increasing quantity of information on insider threat detection by providing theoretical understanding and useful solutions to one of the most important cybersecurity problems of our day. The relation between various existing security models, threat models, and their limitations is discussed in Table 1.

Health monitoring with body sensors

Wireless Sensor Networks are also utilized for in-home patient monitoring. A system for distributed telemonitoring was proposed. It employs the Services Layers over the Physical Devices paradigm. The architecture model is service-oriented. The distribution of resources among several WSNs is the primary goal. This concept can also link several networks with different wireless technologies. The device was placed within the patient's home and gathered motion data and several feature values, such as activity, mobility, and non-response levels. To distinguish between normal and pathological behaviors, the Support Vector Data Description method was applied. An algorithm for categorizing behavior patterns was employed to group the patterns in this instance. There is no evidence to support the expectation that these methods will work in a home setting[30,31].

A Body Sensor Network with several body sensors is developed for the best possible resource allocation. This solution effectively addressed the two main issues facing health monitoring systems: a sustainable power source and quality of service. A survey was conducted on wearable sensor-based health monitoring systems. Evaluation aspects led to the evaluation of several systems[32,33].

The Wireless Patient Portable Unit, which is likewise affixed to the patient's body, received data relating to cardiac monitoring that was continuously recorded in the home module. The Wireless Access Point Unit was then used to transfer it via the Internet to the hospital. If the doctor notices any irregularities in the signals the patient got while in the hospital, they can get in touch with them, offer some guidance, or, in an emergency, send an ambulance to the patient's home. This technology does not provide security or surveillance of the outer environment.

Health monitoring using smart phones

Wearable sensors served as the foundation for the sensor network. The sensors obtained the patient's vital signs, which were then sent to the patient's mobile phone. The data is safely received, stored, and sent to reliable medical specialists by the mobile device. Only the data's accessibility to outside parties is under the patient's control. No PC was utilized in this process; instead, all tasks were completed via mobile device. The handheld gadget transfers only the relevant data after data mining techniques were applied to filter out extraneous data sequences. The expert's equipment and the patient's mobile phone communicated over Bluetooth or WLAN 802.11. When an emergency occurs, the patient's device generates an emergency call, which is then routed to the caregiver's device.

A brand-new Wearable Mobility Monitoring System was unveiled. It recognized a state change and utilized a smartphone to take pictures. A solution for on-demand tracking and placement was suggested. It was designed for vast spaces and was based on devices with Global Positioning enabled. The first communication between the two terminals was done via a smartphone.

First communication takes place during the synchronization phase. In this case, the requested terminal T1 sends the desired terminal T2 a synchronization Short Message Service (SMS). T2 completes the operation if it rejects the message. If not, the terminal's position is sent in one of the following formats: multimedia (MMS) or text (SMS). The graphic that shows the position map of the terminal was present in the multimedia format, but the text format just contained the coordinate values of the terminal. A straightforward Peer-to-peer (P2P) protocol is used to facilitate communication between two terminals.

Health monitoring with security

For health monitoring, various security and privacy protocols were applied[34]. The patient's vital signs were transmitted, stored, and received via a smartphone. A multimedia format was provided between sensors and the central hub encryption scheme, which depicts the location map of the terminal. Peer-to-peer (P2P) protocol is a straightforward means of communication between two terminals.

Cipher text Policy Attribute Based Encryption (CP-ABE) with security enhancement techniques was presented. The two main issues in CPABE were the user revocation and the key escrow problem. In CP-ABE, a set of user attributes is applied to KGC's master secret keys, allowing KGC to produce the users' private keys. Because KGC may decrypt user ciphertext to obtain the original data, it was not considered trustworthy. It is called the "key escrow problem." Users may periodically alter their properties or certain secret keys may be hacked. Regular updates are required for every characteristic to keep the system secure. We refer to this as user revocation. Both of these issues were resolved[35].

Threat model

This subsection covered privacy and security breaches involving patient data. The threat model primarily targets the cybersecurity domains of application-level security, communication-level security, and device-level security. We will discuss the following points related to threat model:

Ref.	Search	Algorithms and Concept	Amalgams	Examination	Limitations
17	To anonymously authenticate high-risk patient data and offer proof of the true role of wireless sensors in data collection, new authentication procedures are suggested.	To demonstrate the effectiveness of the proposed healthcare architecture.	A sensor and cloud.	An innovative sensor cloud architecture that allows for anywhere, anytime, high-risk patient monitoring.	1. No explanation of security measures in place. 2. Proofs of formal security analysis are not provided.
18	The scheme uses an Elliptic Curve Integrated Encryption Scheme (ECIES) and Elliptic Curve Digital Signature Algorithm (ECDSA).	Elliptic Curve Digital Signature Algorithm (ECDSA) and Advanced Encryption Standard (AES).	Real-or-Random oracle model and Scyther's widely accepted model-checking tools.	A comparative analysis of existing systems' security features, communication costs, and computing overhead demonstrates that the proposed framework is secure and efficient for all types of remote and proximity payments.	1. Exclusively suitable for RFID uses. 2. Between the cloud server and mobile devices, the system necessitates greater communication overhead.
11	Privacy-preserving identity-based encryption design.	The scheme is based on q-torsion groups in the supersingular elliptic curve.	The identity-based encryption (IBE) technique of Boneh and Franklin to create an IBE scheme.	Useful for proof-of-concept purposes and for pedagogical purposes.	To reduce trust in the PKG, they have relied on unrealistic assumptions.
13	Original model of CLPKE and propose a new CLPKE scheme that does not depend on the bilinear pairings.	certificates Public Key Cryptography.	Key escrow issue in identity-based cryptography. Certificateless Public Key Encryption was a headache to build.	m-RSA version of certificateless public key cryptography.	Efficient revocation: Prior to encryption or message signing, any domain parity must connect to SEM in order to obtain the ticket.
19	The system is resistant to existential forgery under adaptively determined message and ID assaults in the random oracle model, with the assumption that the Computational Diffie-Hellman Problem (CDHP) is hard.	The key escrow problem is resolved by an identity-based signature scheme that also eliminates the need for a secure channel.	Security in the ROM assumes the intractability of the CDHP against ID attacks and existential forging under adaptively designed messages.	Key escrow is an inexpensive solution that can be used without the need for a secure route to transfer the private key to the user.	1. The public key of a matching user is protected by using the CA's signature on the certificate. 2. Demonstrate its storage inefficiency and computational cost.
20	Framework for secure data sharing and integration among healthcare providers based on a knowledge graph.	Attribute-Based Access Control for unwanted access based on the user attributes.	Cloud-based data transmission.	A significant challenge will be integrating several data sources and subsequently evaluating the system's performance.	Given that data is extremely private and that utility is crucial, methods for anonymizing it could be explored.
21	System security and performance were examined.	TwoFish and Jellyfish algorithms within private blockchain and Fog Computing.	For the purpose of protecting the confidentiality of medical information, the TwoFish encryption algorithm is utilized.	In order to qualify as a solution for health organizations, the proposed scheme offers lightweight operations that are capable of supporting complicated security steps.	There is difficulty involved in keeping medical data from being tampered with, as well as the possibility of hacking and electronic attacks.
22	It has aimed to implement the work in a cloud-based environment and provide strong security and privacy implementations to the medical data at the cloud computing server side.	MD5 Hash Algorithm and checksum	It is possible to append a checksum that was generated by MD5 to the file that contains the original patient record. This improves both the authentication and secrecy of the information.	The goal is to execute the method in a cloud-based environment and ensure robust security and privacy for medical data on the server side.	There are still many issues that need attention, like security of mobile cloud computing and authentication of devices.
23	The research problem with a secure healthcare system for a resource-constrained environment is the cost at which a secure healthcare system is achieved.	ECC, Hash Function and Digital signature	To develop a cryptographic scheme that meets the critical needs of modern smart healthcare cyber-physical systems.	The aim is to balance security and efficiency in IoT-enabled healthcare platforms.	The proposed scheme is vulnerable to various attacks, like offline identity-predicting attacks.
24	In order to protect sensitive patient data, create an authentication system that guarantees a secure connection between IoMT devices.	Elliptic Curve Cryptography (ECC), one-way hash function, and XOR operation.	In this offline authentication architecture, users and IoMT devices are authenticated within the local network by directly verifying identities.	Demonstrated through the application of BAN logic and the Real-Or-Random architecture, which ensures mutual authentication and the security of session keys.	The paper poorly examines the scalability of the system in extensive IoMT implementations involving several devices and users.
25	An efficient key management scheme with lightweight ciphers is essential.	The key agreement uses the hierarchy-based cluster elliptic curve key agreement.	The technique uses elliptic curves instead of logarithmic curves and a shorter key length to achieve security comparable to Diffie-Hellman and RSA cryptosystems.	Using this scheme, group key synchronization is fast, efficient, and dynamic in wireless sensor networks, requiring no reorganization of the system key when members join or leave.	Research offers multiple communication ways to enhance data transmission security. In the same cluster, this study offers an intra-cluster mode to secure data transmission among nodes.
26	The scheme secures IoMT device authentication and user privacy.	ECC-based blind signature.	Provide resistance against common attacks such as man-in-the-middle, replay, impersonation, and chosen ciphertext attacks.	Keep patient data private and user anonymity during authentication.	The protocol has not been fully tested in large-scale IoMT deployments with many devices and gateways.
27	Secure IoMT device communication with an authentication system to protect patient data.	ECC, Zero-Knowledge Proofs, Fog Computing	The scheme is suitable for resource-constrained IoMT devices.	Proposes a novel authentication protocol tailored for the Internet of Medical Things (IoMT), emphasizing both security and efficiency.	The technique allows offline authentication; however, real-time data synchronization and dynamic access control modifications may be difficult.

Continued

[28]	Use identity-based cryptography for authentication to simplify key management and boost security.	Identity-Based Cryptography and ECC	Protocol security is tested using BAN logic, proving its resilience against attacks.	The proposed approach protects EHRs from common security threats by ensuring data confidentiality, integrity, and authentication.	Distributing private keys securely remains a challenge for this scheme.
[29]	Introduced direct authentication for IoMT devices for secure and efficient mutual authentication without internet connectivity.	Elliptic Curve Diffie–Hellman (ECDH), BAN Logic	The proposed iSecureHealth framework reduces IoMT security risks.	It balances security and performance with ECC and HMAC-SHA256, making it appropriate for devices with limited computational resources.	Real-time data synchronization or dynamic access control modifications may be difficult.

Table 1. Relation between various related security schemes and its limitations.

- We analyze a robust adversary model, assuming that, except for the certificate authority, we cannot fully trust any of the entities. Though strange, the hospital and payment gateway are regarded as trustworthy.
- External adversaries could listen in on the conversation and deduce private information about patients as the records are being transmitted.
- To fraudulently accuse lawful patients of overspending, attackers may initiate collision assaults.
- While paying a doctor's charge or ordering medicine online, an eavesdropper may attack the system by providing false information or by pretending to be another real patient, utilizing their hospital account.
- Multiple system attacks may compromise employee privacy when client-server communication stores and forwards private information to several external parties. Via network vulnerabilities or the acquisition of the access point identifier, the attacker, for instance, can seize the patients and examine the network traffic.
- Problems with data communication arise when sensitive data is sent and processed between different detachments participating in the transmission security and privacy problems arise.
- Problems with digital devices and Internet of Things devices, as well as the outcomes for patients using these devices.
- The stakeholders that are considered in the framework are the entities that are a part of this entire procedure (e.g., hospital servers, employees, and patients).
- Digital electronic devices that are incorporated with advanced cryptography tools preserve patient data.

The prevalence of attacks came from the communication and application levels, which we addressed and stopped. The adversary may launch significant assaults and seriously harm financial institutions and other protocol participants if they discover any gaps or vulnerabilities in these areas. We are using the lightweight cryptography techniques provided by ECDSA to create and validate signatures. Similar to this, we have employed the elliptic curve integrated encryption scheme (ECIES) as an asymmetric method of encryption and decryption while employing an encryption/decryption algorithm for symmetric purposes[36].

Secure network model

This subsection discusses the various security models used in data security in the cloud-based system. The The security model provides two-channel digital device connectivity to hospitals, merchants, application providers, and doctors. The main duty of the hospital server, which is a reputable third-party server, is to gather and transmit patients, employees, and doctors' information to merchants. Put differently, this organization determines the information in the patient's database and responds to the hospital employee with an acceptance or rejection of the patient's queries[37,38]. Figure 1 represents the IoMT-based secure netwok model. The information flow in the framework is as follows:

- The hospital receives requests from patients to provide information digitally.
- The staff member's request is sent to the smartphone. Through a wireless connection, the smartphone and the digital devices establish a secure connection.
- Once a link has been made, the application uses password and biometric authentication to verify patients' requests for authentication.
- After the patient's authentication is successful, information is sent from the wireless device to the employee's smartphone through hospital applications that have been loaded.
- Patients initiate and submit requests, such as information portal requests, to any institution.
- The staff member chooses any patient data and submits the request to the appropriate server, like the staff member's server, which manages patient communications records.
- An employee of the hospital verifies the information in their database, validates the patient data, and redirects the exchange of data to the patient's devices.
- The hospital database server uses a secure network to confirm patient information and send data to physicians related to specific medical conditions.
- After completing all verification, the patient's account is credited with the amount of the payment order.
- The server will notify the appropriate entities of the patient's initiator and service provider upon successful validation by the hospital.

Addressing the drawbacks in[17] could considerably improve the effectiveness and security in healthcare architecture. The[18] refers to a lack of research into advanced or emerging security protocols that could improve protection against new types of cyber threats, whereas the[11,13] improves understanding and effectiveness of revocation mechanisms in certificateless public key cryptography, resulting in more robust and practical

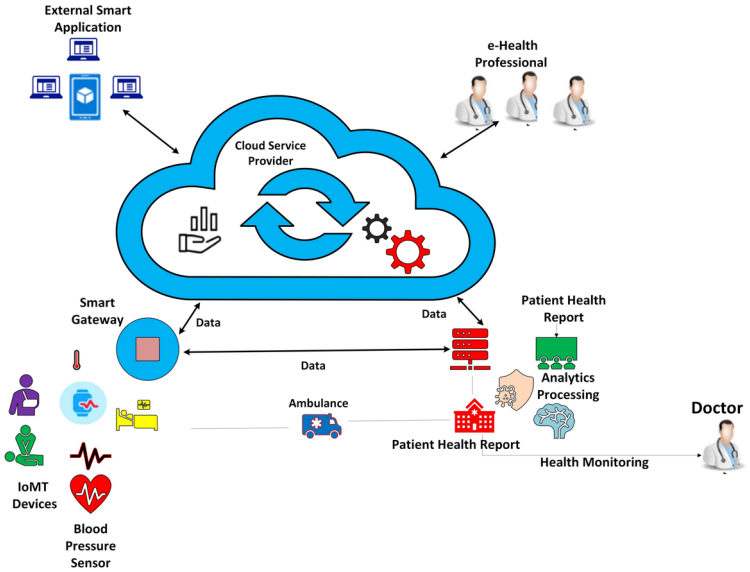


Figure 1. IoMT based secure network model.

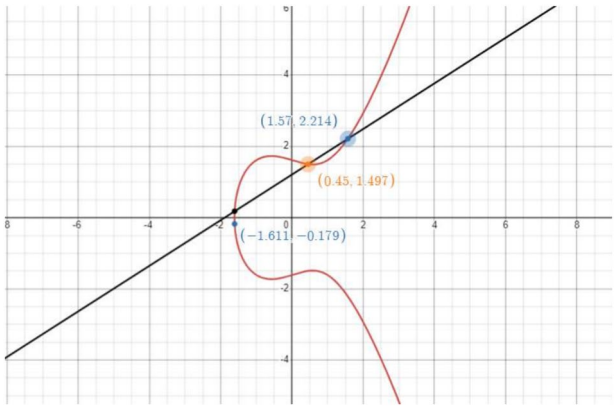


Figure 2. Computation of points by Weierstrass curves.

cryptographic systems. Next,[19] aims to improve the creation and use of identity-based signature schemes, resulting in more secure and practical cryptography solutions based on cloud technologies in healthcare settings.

Proposed methodologies

In this work, we proposed a security scheme ฿-ED-CRY with an identity-based cryptography. Schnorr signature is a digital signature scheme known for its simplicity, efficiency, and ability to generate short signatures. We prove our construction of an encryption-decryption scheme satisfies security by using a signature that shows the identification protocol for an honest verifier zero-knowledge protocol. The next subsections present it with an architecture and encryption-decryption scheme based on elliptic curve cryptography. An elliptic curve generates the secure points, and Fig. 2 depicts the operations.

Our proposed security architecture

This subsection presents the system architecture of an access control system that utilizes identity-based methods and is based on the Internet of Medical Things. The key generation center serves as the trusted authority responsible for issuing user keys that match their public identities. The system utilizes authentication servers to authenticate legitimate users who are trying to access important resources. Similar to traditional public key infrastructure, the system operates under the assumption that a safe and trusted third party exists. The identity-based access system offers a robust authentication mechanism while maintaining low operational overhead needs.

Our proposed IoMT architecture consists of three main components: patients, hospitals, and cloud servers. This design describes the components and procedures that comprise an Internet of Medical Things model. This architecture focuses on interactions between patients, hospitals, and cloud servers, as seen in Fig. 3. Patients use

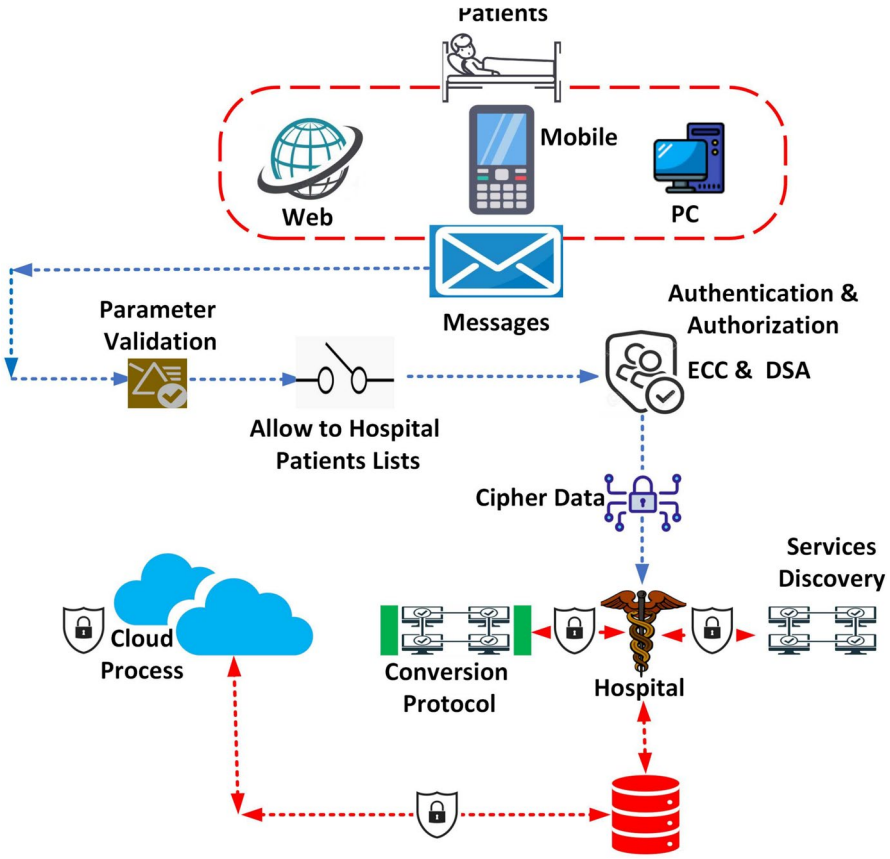


Figure 3. Proposed IoMT Security Model based on identity-based access control system.

IoMT devices to communicate about their present health status. These health records are acquired by hospitals, who process and store them in their own databases. Cloud servers make it easier for medical practitioners and hospital workers to communicate with one another while monitoring and diagnosing patients.

- *Utilization of IoMT Devices* Patients are able to communicate their medical information through the usage of IoMT devices. Wearables, sensors, and other components of medical monitoring devices could be included in this category of gadgets.
- *Wireless Media* It is possible to establish connections between devices connected to the Internet of Things and the web server through the utilization of wireless media. Consequently, there is no longer a requirement for physical connections, which makes it possible for medical information to be transferred smoothly.
- *Validation and Authentication* In order to ensure that the database of the hospital is up to date with the patient's current health condition, it is essential to perform validation on the message that has been received. The integrity of the data as well as its reliability are safeguarded from this perspective. The next step is to authenticate the message using a Digital Signature Algorithm (DSA), which confirms its authenticity. This step comes after the message has been validated.
- *Data Storage* All of the health information that has been verified and encrypted is kept in a safe place within the database of the hospital. Only authorized workers will be able to access important patient information, which will be safeguarded from unauthorized access.
- *Cloud Server Communication* Hospital workers and medical professionals can connect and work together on patient care through the use of the cloud server. According to the information that is provided, they can access patient health data that is recorded in the database of the hospital, which enables remote monitoring and diagnosis.

So, IoMT devices enable patients to transmit their health data to hospitals via wireless connections. The data undergoes validation, authentication, and encryption before being stored in the hospital's database. Cloud servers facilitate communication and collaboration among hospital personnel and doctors for monitoring patient health and making informed diagnoses.

Mathematical preliminaries of ECC

In this section, we will discuss the main mathematical calculations used in elliptic curve cryptography. These include the Elliptic Curve Discrete Logarithm Problem (ECDLP), as well as how signatures are generated and verified. All the acronyms and notations used in this paper are represented in Table 2.

S.No	Notation	Description
1	BS	Base Shift
2	RL	Rotation Left
3	SM	Secret Message
4	MBM	Message Binary Matrix
5	Ma	Matrix
6	RM	Rotated Matrix
7	FM	Final Matrix
8	RC	Rotate column
9	$\Re$	Reshape
10	฿-ED-CRY	Bi Encryption Decryption Crypto
11	Rolt	Rotation

Table 2. Notations and description.

Process of ECC

In this subsection, elliptic curve cryptography (ECC), particularly ECDSA (Elliptic Curve Digital Signature Algorithm), is indeed a pivotal aspect of modern cryptographic systems. Understanding its fundamental operations is crucial for anyone interested in cryptography and cybersecurity. Here's a brief overview of what you'll typically encounter when delving into ECDSA:

Key pair generation of ECC

Key pair generation in elliptic curve cryptography involves creating a public-private key pair that can be used for cryptographic operations such as digital signatures and encryption. Here's an overview of the key pair generation process:

Choose an Elliptic Curve: The first step is to choose an elliptic curve over a finite field. Elliptic curves are typically defined by the equation $y^2 = x^3 + ax + b$, where a and b are constants specific to the curve, and the operations are performed modulo a prime p. Commonly used curves include the NIST curves such as P-256, P-384, and P-521.

Choose one of the generator points, as every elliptic curve has a special point that is referred to as the generator point, which is sometimes represented by the letter G. The number of points on the curve that can be formed by continually adding the generator point to itself is denoted by order n, which is a specific order that this point possesses. When it comes to prime numbers, the order n is often rather large.

The Key Pair Storage of the private key must be securely stored and protected from unauthorized access. The public key can be shared freely with other parties. The key pair usage to generate key pair can now be used for cryptographic operations such as digital signatures, encryption, and decryption.

Schnorr digital signature

Claus-Peter Schnorr invented the Schnorr signature scheme, a well-known digital signature algorithm known for its simplicity, potency, and security assurance it offers. Its implementation takes advantage of the difficulties presented by the discrete logarithm problem (DLP) within finite fields or groups. When adopting ECC for this purpose, while the fundamental principles persist, there is a fundamental shift in the underlying mathematical framework from finite fields to elliptic curves. Here's a high-level summary of how the ECC-based Schnorr signature scheme operates.

The Schnorr signature scheme's security depends on the computational difficulty of solving the DLP, which is a difficult problem even with advances in computing power. The approach preserves the simplicity and effectiveness of the original Schnorr method while leveraging elliptic curves' intrinsic security features.

The basis of Schnorr signature techniques is the ability to digitally sign a message that is verifiable by everyone possessing the signer's public key. This is an interpretation of how its functions work, which are as follows:

1: Choose suitable prime numbers, such as p and q.
2: Select "a" as such that $a^q = 1 \; mod \; p$.
3: (a,p,q) are the global parameters as public for all.
4: Let a User A generate a key.
5: Choose a prime order elliptic curve group $E(F_p)$ with generator point G and prime order n.
6: Select a private key Sec_A randomly from $0 < Sec_A < q$.
7: Compute the public key $Pub_A = a^{Sec_A} \; mod \; p$, where $\cdot$ denotes scalar multiplication.

Algorithm 1. Algorithm for Key Setup

Schnorr Signature Scheme
Let the User sign a message by using different parameters as

- Select random value r from the $0 < r < q$ and compute x = a.r mod p.
- Concatenate message with x and hash result to compute $e = H(M \parallel x)$.
- Compute $y = (r + Sec_A.e)$ mod q.
- Signature is pair σ = (e, y)

So, any other users can verify the σ as follows:

- Compute $x^{'} = a.y.v.e$ mod p.
- Verify that $e = H(M \parallel x^{'})$

So, the signature proof that $x^{'} = a^{y}.Pub_A$ mod p
$=a^{(r+Sec_A e+Z_1 q)}\ a^{(Sec_A+Z_2 p)^e}$ mod p
$=a^(r + Z_3 q)$ mod p
$= a^r$ mod p
= x

Firstly, the message to be signed (m) is hashed using a cryptographic hash function such as SHA-256 to obtain a fixed-size digest: z=Hash(m).

1: Choose a random integer (k) such that $1 < k < n - 1$.
2: Compute the point $k.G = (x_1, y_1)$.
3: Calculate $r = x_1\ mod\ n$. If r = 0, choose a different k.
4: Compute $s = k^1(z + rd)\ mod\ n$. If s=0, choose a different k.
5: The signature is the pair (r,s).

Algorithm 2. Signature Computation

1: Ensure that r and s are integers within the range $1 \leq r, s \leq n - 1$
2: Compute $w = s^{-1} mod\ n$.
3: Calculate $u_1 = zw\ mod\ n$ and $u_2 = zw\ mod\ n$
4: Compute the point $X = u_1.G + u_2.Q$
5: If X is the point of Infinite the signature is Invalid
6: Otherwise, let $v = x\ mod\ n$
7: The signature is valid if v = r; otherwise, it is invalid.

Algorithm 3. Verifying Signatures with ECDSA

Encryption-decryption

This subsection discusses the encryption and decryption mechanism of our security scheme, ฿-ED-CRY to maintain the privacy of patient-related information.

Key Generation

- Let the public key as PK_{key}
  so PK_{key} =(BS, RL)
- The message M with length L = $|M|$, where $|M|$ represents the length of the source message M.
- Convert the Message to Decimal:
  For each character M_i in the source message M
  D_i = ASCII(M_i)**Encryption of Message**

- Convert Message to Binary
  For each character M_i in the source message M:
  B_i=ASCII(M_i)binary
- Convert MBM to BS
  MBM = ℜ(MBM, BS, Col)
- Rotate Each Column RL Times: For each column C_i in the reshaped matrix as: Rotated Col_i = RL(C_i, RL)
- compute the shape Resulting Matrix to 8 Columns Matrix:
  FM = ℜ(RM,8 col)
- Compute the Result to Decimal:
  For every number N in the final matrix D = BinaryTo Decimal(N)

- Compute Decimal to Binary Number as characters
  for every decimal number
  E= (M_i) = ASCII (D)**Decryption of Message**

- Convert Message to Binary (MBM):
  For each character B_i in the source message M:
  B_i=ASCII()binary M_i
- Reshape MBM to BS Columns:
- Reshaped MBM = ℜ(MBM,BS col)
- Compute as a first rotation as Each Column BS-ROTL Times: For each col C_i in the reshaped matrix:
- Next, Rotated Col = RL(C_i, BS-RL)
- Reshape Resulting Matrix to 8 Columns Matrix: FM = ℜ(RM,8 col)
- Convert Result to Decimal:
- For each number N in the final matrix:
  D = BT o D(N)
- Convert Decimal Results to Characters:
  For each decimal number D:
  D=(M_i) =ASCII(E)

Example of encryption process

Let X=A B C D E F G H
CONVERT INTO DECIMAL
65 66 67 68 69 70 71 72
THEN CONVERT IT INTO BINARY FORM
01000001
01000010
01000011
01000100
01000101
01000110
01000111
01001000

Random Reshaped to 64 columns

0000001011110001110101011011011011111011110001000000111101011101

Rolt as 22 digits for change the binary no

0000000000111110000010000100010001011101111111100001111101010101

Adjust in 8 columns as by encryption algorithms
00011101
00100001
00010010
00011010
00101010
00110001
00100010
00001010

Then the values are
29 65 18 26 42 98 34 10

Example of decryption process

29 65 18 26 42 98 34 10

00011101
00100001
00010010
00011010
00101010
00110001
00100010
00001010
Reshaped in 64 columns as

0000000000111110000010000100010001011101111111100001111101010101
Rotate as 64-22 digit by decryption algorithms

0000001011110001110101011011011011111011110001000000111101011101
Reshaped in 8 columns by Algorithms

01000001
01000010
01000011
01000100
01000101
01000110
01000111
01001000
These values are A B C D E F G H

We represent the message as M and convert it into the ASCII values for each input value. We then convert these values into binary form, creating a message binary matrix (MBM) for the message. Next, we manipulate the values of the MBM by using the base shift values and randomly select a point from an elliptic curve as a security parameter. These values serve as the user's private keys for encryption. The user then chooses these values and performs the 8-bit rotation. After these computations, we find the final matrix in matrix D. We store the converted values in E as characters using the ASCII value. For the decryption of the secret message, the algorithm uses the private key of the receiver and follow the steps in as shown in an algorithm.

Figure 3 provides our proposed hospital management system flow of information for the health care protocol using a cloud-based device. Some Initial assumptions and prerequisites used for this proposed secure scheme are as:

1. Using a cloud-based device, the patient requested a health examination and payment. The numerous pieces of technology should be paired or connected with the gadget and smartphone.
2. To access transaction information via a mobile device and pay fees using a digital payment system, the registered patient (hospital and patient) must maintain a current database and account with their respective hospitals.
3. To conduct secure conversations, each patient uses their signed certificates from a certification authority (CA), a reliable third party.
4. Each patient is provisioned with a unique "Wireless Public Key Infrastructure" certificate that is preserved in a Secure Element (SE) within the communication devices.
5. Each party to the suggested protocol owns their digital certificates and public keys.
6. The hospital offers and customizes digital and mobile devices for payment and communication applications through cloud-based technology.

As illustrated in Fig. 4, the client manager and patient data reader are merged to form the data owner. Outdoor environment monitoring was not supported in some of the systems that were already in place. In that instance, it becomes challenging to keep an eye on a patient when they relocate away from their home. However, the GPS-enabled smartphone in the suggested work also allows for outdoor monitoring. Since the patient constantly carries a mobile phone, it continuously gathers bodily parameters even when the patient is not at home. Bluetooth short-range communication is used to communicate between sensors and mobile phones.

The acquired body parameters from the sensors are saved on a personal computer in the majority of current systems. There are several issues that can arise when using a computer. A GPS-enabled mobile phone replaces the requirement for a PC in the proposed task. Data Storing Centre (DSC) and Client Key Manager (KGC) make up the data server. The creation of keys for the safe transfer of medical data falls under the purview of KGC and DSC. The user refers to medical personnel at the hospital side, whereas the data owner represents the patient.

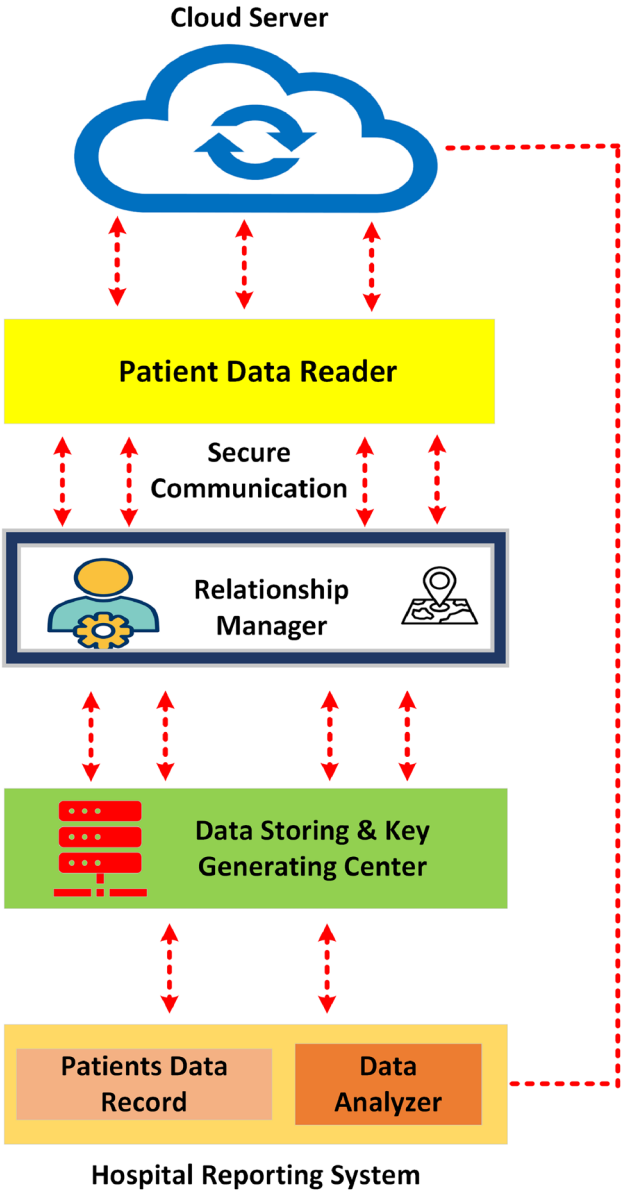


Figure 4. A Secure Relationship between Users and Hospital System.

Figure 5 represents the flowchart to visualize the working of the proposed IoMT model. Using IoMT devices, patients can communicate their current health status to hospitals when seeking treatment from remote locations. To avoid wasting time on fraudulent users, we first verify whether the message is valid or not. If the message is valid, we then perform parameter validation to verify the patient ID and health condition. After parameter validation, we add the patient to the hospital's patient list. The message is then authenticated using a digital signature algorithm, which confirms its authenticity. All verified and encrypted health information is securely stored in the hospital's database. Only authorized personnel can access this important patient health information, ensuring it is protected from unauthorized access. Any incomplete or invalid messages received are temporarily stored without encryption in the hospital database and deleted after a specified period.

Phases of secure communication

This section discusses all the phases for secure communication in a step-by-step manner, as represented in Fig. 6. This figure analyzed stepwise communication between IoMT devices, the cloud gateway, and the cloud server.

Step-1. System Setup In this step, the cloud server provides the server storage and various network resources. The cloud server manages every user and hospital's devices in a centralized. The medical devices are configured with unique identifiers and cryptographic keys. After that secure database is created in the cloud to store device information, user credentials, and cryptographic keys.

Step-2. Device Registration In this phase, the IoMT device sends a registration request to the cloud gateway, including its unique identifier, and forwards the registration request to the cloud server. The server verifies the

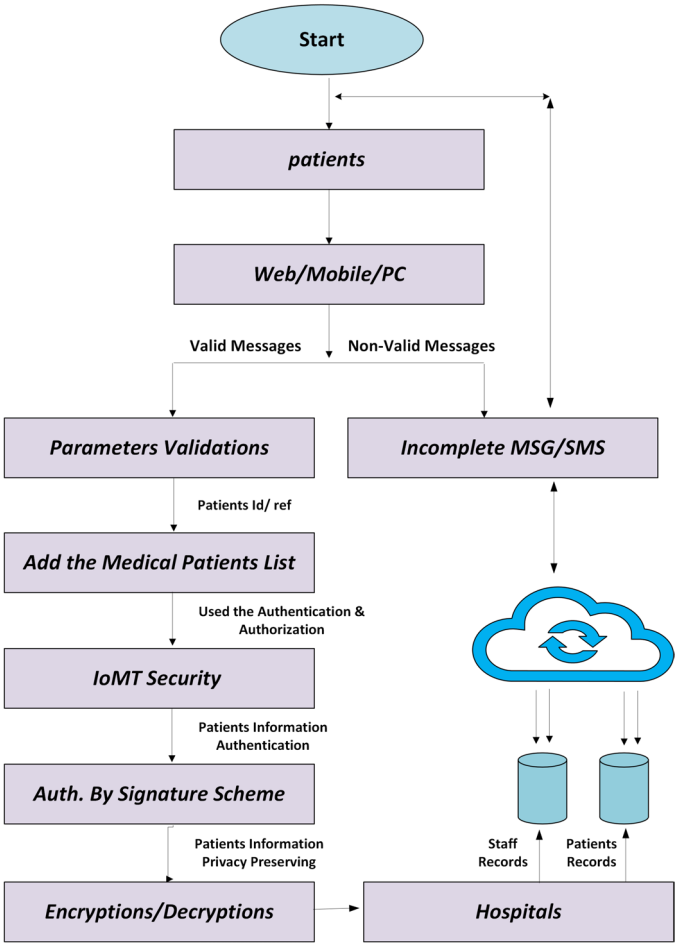


Figure 5. Flowchart to depict the working of the proposed IoMT model.

device identification ID with shared credentials. After that generate the public and private key and pair the devices with updates to the key in the server.

Step-3. Authentication The device sends an authentication request to the cloud gateway including its unique identifier and a digitally signed message. The cloud gateway forwards the authentication request to the cloud server. The cloud server retrieves the device's public key from the database and verifies the digital signature. The cloud server generates a session key for secure communication if the signature is valid.

Step-4. Key Agreement According to Diffie-Hellman and ECC, the cloud server and the IoMT device use a secure key exchange protocol to agree on a shared secret key. All data transmitted between the device and the cloud is encrypted using the shared secret key.

Step-5. Secure communication Any communication network's dependability primarily rests on its ability to flow continuously and securely. The network's autonomous phases, which may function independently to provide a seamless connection, have made this possible.

Step-6. Parameter Update The cloud server sends a parameter update request (e.g., firmware update, configuration changes) to the IoMT. The device decrypts the request, applies the updates, and sends an acknowledgment back to the cloud server. The cloud server updates the device's profile in the database to reflect the new parameters.

Security analysis of the proposed scheme

This section discusses the security analysis of the proposed scheme, including its ability to maintain patients' data confidentiality, integrity, and authentication. We also discuss various potential attacks and provide a security analysis that demonstrates the proposed scheme is resistant to man-in-the-middle (MITM) attacks, based on the Canetti and Krawczyk security model.

Man-in-the-Middle (MITM) Attack This attack is not possible with our framework since it provides robust anonymous authentication. It prevents an attacker from carrying out such an attack. The key values are based on global patient identification. It means that if there is a new wireless sensor network (WSN) visit, an attacker who pretends to be a valid scheme will not be able to guess the key values. In addition, when the same WSN is present in the vicinity, the attacker will not be able to decrypt multiple messages since the cloud server has already encoded them using a session key.

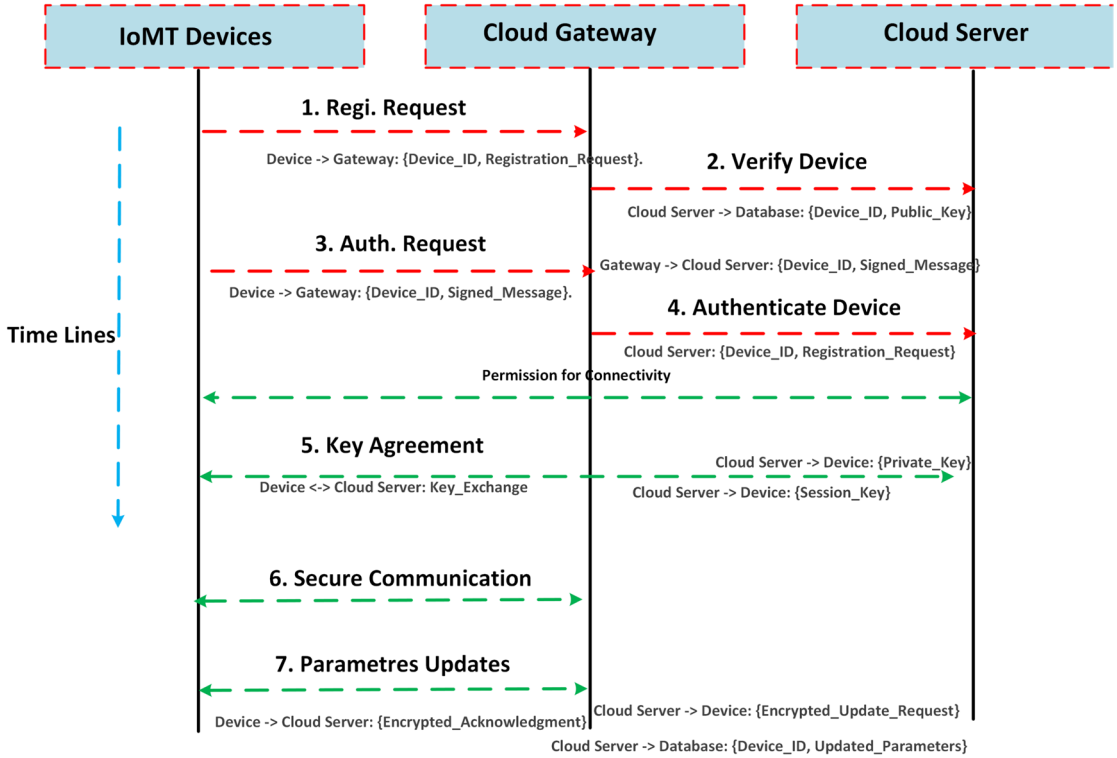


Figure 6. Phases of Secure Communication.

Replay Attack An attacker is capable of replaying previous messages sent and received via the key exchange protocol. Nonetheless, because fresh random numbers are created to ensure the freshness of each session, the provisioning server recognizes the invalidity of the message.

Session Key Disclosure Attack This attack takes place when an adversary is able to intercept and retrieve the session key that is utilized for the purpose of encrypting communication between IoMT devices. In the proposed scheme, session keys are dynamically generated using identity-based cryptography and are never transmitted in plaintext.

Eavesdropping Attack In this, an attacker secretly listens to communication channels to steal sensitive patient data. Our scheme employs a robust encryption technique to ensure all transmitted patient data is encrypted using the session key.

Gateway Impersonation Attack This attack happens when an attacker masquerades as a legitimate gateway to deceive IoMT devices into revealing sensitive data. The proposed scheme uses identity-based authentication and a secure handshake process where both the gateway and devices validate each other's credentials.

Off-line User Identity Predicting Attack This attack involves an adversary attempting to guess a user's identity through offline analysis. The proposed scheme safeguards against this by incorporating identity-based cryptographic techniques where user identities are never exposed in plaintext.

Security Analysis Against MITM Attacks

Security analysis against a man-in-the-middle (MITM) attack based on Canetti and Krawczyk model is represented in Fig. 7.

The Schnorr signature scheme is effective in preventing MITM attacks primarily because of its reliance on the cryptographic hash function and the discrete logarithm problem. This signature scheme involves three main algorithms: key generation, signing, and verification. The scheme uses the discrete logarithm problem in a finite cyclic group for its security.

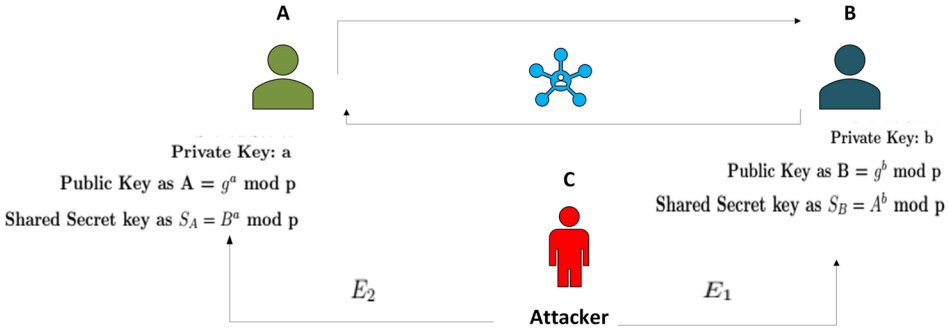
Theorem: The Schnorr signature scheme is secure against MITM attacks, assuming the hardness of the discrete logarithm problem and the security of the hash function.

1. **Non-interactive Signature Generation**

   - There is no communication with any other party during the signing procedure. Sender A can sign any communication on their own without communicating with user B after they have generated their key pair.

2. **Signature Unforgeability**

   - *Assumption* The features of the hash function H and the difficulty of the discrete logarithm problem determine the security of Schnorr signatures.



Attack Steps:

1. **Attacker Intercepts and Modifies Public Keys:**

   User A sends her public key A to User B, Then the User C intercepts it and sends her own public key E1 instead

   User B sends his public key B to User A, User C intercepts it and sends her own public key E2 instead

3. **The Attacker Computes the Final Shared Secret:**
   User C knows both a and b (as she intercepted and modified both keys), so she can compute the shared secrets between User A and User B

   User A's secret: SA,E
   User B's secret: SB,E

2. **Attacker computes Final Shared Secret:**
   Attacker knows both a and b
   User A computes a shared secret with User C's public key

$$E_1 : S_{A,E} = E_2^a \bmod p$$

User B computes a shared secret with User C's public key

$$E_2 : S_{B,E} = E_1^b \bmod p$$

4. **The attacker computes the final shared secret between User A and User B**

$$E_1 : S_{A,E} = E_2^a \bmod p = S_{B,E}$$

$$E_2 : S_{B,E} = E_1^b \bmod p = S_{A,E}$$

Figure 7. Security Analysis against Man-in-the-Middle Attack.

- *Reduction to Discrete Logarithm Problem* An adversary must either solve the discrete logarithm problem or compromise the security of the hash function to forge a signature (r,s) for a message m without knowing the private key a. It is impossible to forge a signature due to the difficulty of these issues.

3. **Authenticity**

- *Hash Function* The hash function H ensures the reliance of the signature on the message m and random integer r. Therefore, an authentic signature used in one message cannot be used in another.
- *No Key Substitution* The signature verification equation $g^s = r \cdot y^e \ mod \ p$ involves the public key y and the hash H, which includes the message. Thus, an attacker cannot substitute User A's public key with their own without failing the verification check.

Because of these features, an attacker can't make a valid signature without the private key or by breaking cryptographic assumptions, even if they are able to read and change messages. Schnorr signatures therefore offer robust defense against Man-in-the-Middle attacks.

Results and simulation

In this section, we have discussed the computational performance of the proposed scheme.We have incorporated patients' sensitive health information in both the encryption and decryption processes. Additionally, we have implemented an authentication mechanism for patients and hospital staff through a digital signing and verification process.

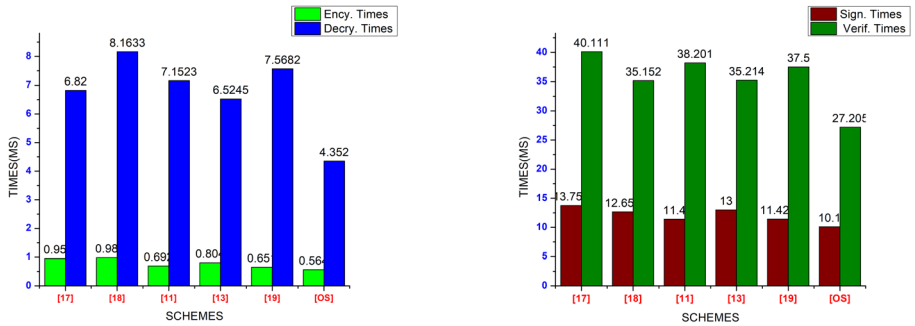
Simulation setup

The proposed security technique is used in a programming language to create the architecture of the suggested in-home patient monitoring system. Every task is completed on a PC running the Linux 18.04 Ubuntu operating system, which calls for a Core i5 processor clocked at 3.4 GHz, 8 GB of RAM, and GCC 4.9.5. C++ is used to code the pairing-based cryptography (PBC) library. In the simulation, we perform 20 iterations in a simulation of the proposed methods to get the desired result.

The relation between various security schemes and their features is presented in Table 3.This table shows different types of security features, such as a digital certificate, key escrow-free (so only the user knows their own private key), denial-of-service, trusted authority (so only a trusted authority can issue a digital certificate), fast revocation (which solves the issue of adding more users), and cryptographic workflow (sender and receiver share encrypted plaintext by a key). In this table, (✓) represents that security features are found, and (×) represents that security features are not found. From this table, we conclude that our proposed scheme provides all security features, while previous schemes lack some features.

S.No	Schemes	Cry Based Scheme	Cert.	Esc-Fre	DoS	TA	F. Rev	Cry Ove
1	[17]	Identity-based Cryptography	✓	×	✓	✓	✓	×
2	[18]	Certificateless PKC	×	✓	✓	✓	×	✓
3	[11]	Traditional PKC	×	×	✓	×	✓	✓
4	[13]	Certificate-based PKC	✓	✓	✓	×	✓	✓
5	[19]	Self-Generated-Certificate PKC	✓	×	✓	×	✓	✓
6	[OS]	Proposed scheme	✓	✓	✓	✓	✓	✓

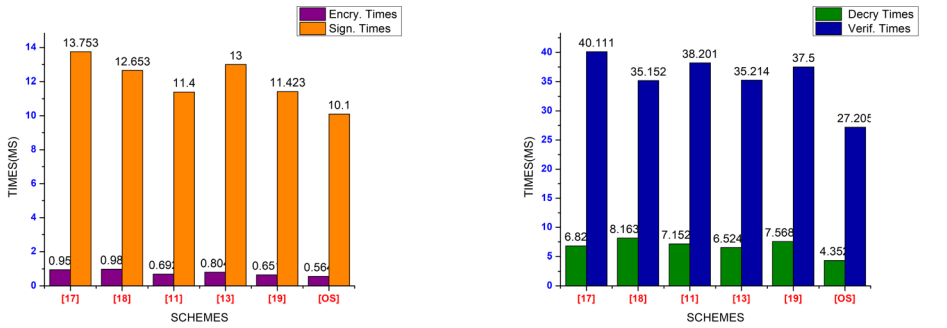
Table 3. Relation between various security schemes along with their security features. ✓: denotes security features found and ×: denotes security features not found



(a) Comparision of time taken in encryption and decryption process

(b) Comparision of time taken in signing and verification process

Figure 8. Comparison of computational time in encryption- decryption and authentication process.



(a) Comparision of time taken in encryption and signing process

(b) Comparision of time taken in decryption and verification process

Figure 9. Comparison of computational time taken by proposed scheme with existing schemes.

Computational comparison

The computational cost is the term used to describe the time needed to execute cryptographic procedures. The primary cryptographic procedures used in this study include pairing, hashing, one-point addition, multiplication, and the exclusive-or (XOR) operation. The time taken for encryption, decryption, signing process, and verification process are shown in Figs. 8 and 9. We find that our proposed scheme takes less time as compared to other related schemes, as shown in Table 4. That means our schemes perform better than other existing schemes.

Conclusion and future research

Protecting patient privacy is an important issue that requires attention in light of recent developments in the Internet of Medical Things. The proposed scheme, ₿-ED-CRY would solve concerns and offer a different perspective on secure communication in the IoMT. The system includes a portable application that securely monitors patients' medical conditions at all times from a remote location. This scheme protects personal information by performing more effective encryption and decryption operations and preserving user identity. We have demonstrated the robustness of the proposed scheme against man-in-the-middle attacks. The results

S. No	Schemes	Enc. Time	Dec. Time	Sign Time	Verif. Time	Attack Prev.
1	[17]	0.9500	6.8200	13.753	40.111	Yes
2	[18]	0.9800	8.1633	12.653	35.152	No
3	[11]	0.6920	7.1523	11.400	38.201	Yes
4	[13]	0.8040	6.5245	13.000	35.214	Yes
5	[19]	0.6510	7.5682	11.423	37.500	No
6	Our Scheme (OS)	0.5640	4.3520	10.100	27.205	Yes

Table 4. Comparison of various security schemes and their execution time. * All schemes tested in the same bit strings and *Time are mentioned in ms

of performance analysis indicate that the proposed scheme provides enhanced security and takes lower computational cost as compared to other related existing schemes.

Even while the proposed scheme works well for existing IoMT configurations, more research is necessary to fully understand its effects on security and performance in large-scale deployments.

Future research might investigate computationally less-intensive, lightweight-based security techniques and add the concept to make the scheme more scalable in the field of smart healthcare.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Received: 12 January 2025; Accepted: 4 June 2025
Published online: 04 July 2025

References

1. Guo, P., Liang, W. & Xu, S. A privacy preserving four-factor authentication protocol for internet of medical things. *Computers & Security* **137**, 103632 (2024).
2. Gupta, C. & Varshney, G. A lightweight and secure puf-based authentication and key-exchange protocol for iot devices. *arXiv preprint* arXiv:2311.04078 (2023).
3. Mondal, A., Chatterjee, P. S. & Ray, N. K. An optimal novel approach for dynamic energy-efficient task offloading in mobile edge-cloud computing networks. *SN Comput Sci* **5**(5), 655 (2024).
4. Gaur, R. et al. A secure and efficient scheme based on unlinkability and anonymous traceable protocol for cloud-assisted iot environment. *J Circuits, Syst Comput* **32**(18), 2350316 (2023).
5. Khajehzadeh, L., Barati, H. & Barati, A. A lightweight authentication and authorization method in iot-based medical care. *Multimedia Tools and Applications*, 1–40 (2024)
6. Yu, S. et al. Efficient ECC-based conditional privacy-preserving aggregation signature scheme in v2v. *IEEE Trans Veh Technol* **72**(11), 15028–15039 (2023).
7. Mondal, A. & Chatterjee, P. S. Cloudsec: a lightweight and agile approach to secure medical image transmission in the cloud computing environment. *SN Comput Sci* **5**(2), 237 (2024).
8. Kumar, S., Abhishek, K., Jhaveri, R., Alabdulatif, A. & Gaur, R. An efficient dual encryption of iomt data using lightweight security scheme for cloud based iot environment. In: *Proceedings of the 38th ACM/SIGAPP symposium on applied computing*, pp. 1782–1788 (2023).
9. Echenim, K.U. & Joshi, K.P. Iot-reg: A comprehensive knowledge graph for real-time iot data privacy compliance. In: *2023 IEEE International conference on big data (BigData)*, pp. 2897–2906 (2023). IEEE.
10. Pooranian, Z., Shojafar, M., Taheri, R. & Tafazolli, R. Pascoinfog/pasfog: Privacy-preserving data deduplication algorithms for fog storage systems. *IEEE Consumer Electronics Magazine* (2023).
11. Bissessar, D. & Adams, C. Construction and implementation of a privacy-preserving identity-based encryption architecture. *J. Inf. Secur.* **14**(4), 304–329 (2023).
12. Das, M. L. A key escrow-free identity-based signature scheme without using secure channel. *Cryptologia* **35**(1), 58–72 (2010).
13. Liu, X., Sun, Y. & Dong, H. A pairing-free certificateless searchable public key encryption scheme for iomt. *J. Syst. Architect.* **139**, 102885 (2023).
14. Boneh, D., Ding, X., Tsudik, G. & Wong, C.M. A method for fast revocation of public key certificates and security capabilities. In: *10th USENIX Security Symposium (USENIX Security 01)* (2001).
15. Shamir, A. Identity-based cryptosystems and signature schemes. *Adv Cryptol: Proc CRYPTO* **84**(4), 47–53 (1985) (**Springer**).
16. Methodology - Internet of Medical Things (IoMT) Market | Fortune Business Insights — fortunebusinessinsights.com. https://www.fortunebusinessinsights.com/industry-reports/methodology/internet-of-medical-things-iomt-market-101844. [Accessed 12-09-2024]
17. Guezguez, M. J., Rekhis, S. & Boudriga, N. A sensor cloud for the provision of secure and qos-aware healthcare services. *Arab. J. Sci. Eng.* **43**(12), 7059–7082 (2018).
18. Bojjagani, S. et al. The use of iot-based wearable devices to ensure secure lightweight payments in fintech applications. *J King Saud Univ-Comput Inf Sci* **35**(9), 101785 (2023).
19. Sahana, S. C., Das, M. L. & Bhuyan, B. A provable secure key-escrow-free identity-based signature scheme without using secure channel at the phase of private key issuance. *Sādhanā* **44**, 1–9 (2019).
20. Walid, R., Joshi, K.P., Elluri, L., et al. Secure and privacy-compliant data sharing: An essential framework for healthcare organizations. In: *10th International conference on mathematics and computing ICMC* 2024 (2024).
21. Al-Zubaidie, M.H. & Razzaq, R.H. Maintaining security of patient data by employing private blockchain and fog computing technologies based on internet of medical things. *Informatica***48**(12) (2024).
22. Patil, A., Ashwini, D., TP, R.R. & Srinivas, T. A mobile cloud based approach for secure medical data management. *International Journal of Computer Applications***119**(5) (2015).
23. Kumar, M. & Chand, S. A provable secure and lightweight smart healthcare cyber-physical system with public verifiability. *IEEE Syst. J.* **16**(4), 5501–5508 (2021).

24. Maarouf, A., Sakr, R., & Elmougy, S. An offline direct authentication scheme for the internet of medical things based on elliptic curve cryptography. *IEEe Access* (2024).
25. Lin, H. Y. Integrate the hierarchical cluster elliptic curve key agreement with multiple secure data transfer modes into wireless sensor networks. *Connect. Sci.* **34**(1), 274–300 (2022).
26. Samal, K., Sunanda, S. K., Jena, D. & Patnaik, S. A lightweight privacy preservation authentication protocol for iomt using ECC based blind signature. *Int J Eng Bus Manag* **17**, 18479790251318536 (2025).
27. Misra, G., Hazela, B., & Chaurasia, B.K. A user-adaptive privacy-preserving authentication of iomt using zero knowledge proofs with ecc. *Multimedia Tools and Applications*, 1–32 (2025).
28. Patil, R. Y., Karati, A. & Patil, Y. H. A signcryption with identity-based authentication for secure EHR sharing in iomt utilizing ECC. *Int. J. Inf. Technol.* **16**(8), 5133–5148 (2024).
29. Dhar, C. K. & Majumder, A. isecurehealth: an efficient and secure technique to exchange health data using iomt devices. *Smart Health* **33**, 100504 (2024).
30. Cano, C.A.G., Castillo, V.S., Castillo-Gonzalez, W., Vitón-Castillo, A.A., & Gonzalez-Argote, J. Internet of things and wearable devices: a mixed literature review. *EAI Endorsed Transactions on Internet of Things***9**(4) (2023).
31. Chen, C.-M., Liu, S., Li, X., Islam, S. H. & Das, A. K. A provably-secure authenticated key agreement protocol for remote patient monitoring iomt. *J. Syst. Architect.* **136**, 102831 (2023).
32. Ouiazzane, S., Addou, M. & Barramou, F. A zero-trust model for intrusion detection in drone networks. *Int. J. Adv. Comput. Sci. Appl***14**(11) (2023).
33. Liu, S., Wang, Z., Kumari, S., Lv, J. & Chen, C.-M. Provably secure anti-phishing scheme for medical information in smart healthcare. *IEEE Internet of Things Journal* (2024).
34. Gaur, R. & Prakash, S. Privacy prevention and nodes optimization, detection of iout based on artificial intelligence. *Wirel Personal Commun* **138**(1), 67–97 (2024).
35. Li, X., Wang, H., Ma, S., Xiao, M. & Huang, Q. Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud. *Cybersecurity* **7**(1), 1–19 (2024).
36. Gaur, R. et al. A machine-learning-blockchain-based authentication using smart contracts for an ioht system. *Sensors* **22**(23), 9074 (2022).
37. Khan, N. et al. An ECC-based mutual data access control protocol for next-generation public cloud. *J Cloud Comput* **12**(1), 101 (2023).
38. Mondal, A. & Chatterjee, P.S. A systematic literature survey on data security techniques in a cloud environment. In: *2022 OITS International conference on information technology (OCIT)*, pp. 451–456 (2022). IEEE.

Author contributions

Mr. Sanjay Kumar designed the idea of framework of the research. He created and tested the proposed algorithm. Sanjay also prepared the first draft of the manuscript. Kumar Abhishek played a role in the final model's development, testing, and verification. Throughout the duration of the endeavor, Sitharth Selvrajan provided guidance and supervision. Managed all correspondence with the journal and served as the corresponding author, overseeing the submission process.

Declarations

Competing Interest

No

Dual Publication

No

Additional information

Correspondence and requests for materials should be addressed to S.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.