Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

A Secure Framework based on Sensor-Cloud architecture for Healthcare data using enhanced Elliptic Curve Encryption

[1]*Munish Saran, [2]Rajan Kumar Yadav, [3]Pranjal Maurya, [4]Sangeeta Devi, [5]Upendra Nath Tripathi

[1]Assistant Professor, [2,3,4]Research Scholar, [5]Associate Professor

[1]Department of Computer Science and Engineering, IET DDU Gorakhpur University, Gorakhpur, India

[2,3,4,5]Department of Computer Science, DDU Gorakhpur University, Gorakhpur, India

Article History:

Received: *11-11-2024*

Revised:*24-12-2024*

Accepted:*09-01-2025*

Abstract:

Healthcare data security is of utmost importance in today's era due to the several reasons such as Privacy Protection, Legal and Regulatory Compliance, Protection against Data Breaches and Cyber Attacks, Patient's Safety and Continuity of Care, Research and Innovation, Trust and Patient's Confidence. There must be a security authority deployed that can provide efficient as well as transparent defence mechanism. Traditional technique makes use of access control lists which allows the provision for coarse-grained access to data. Whereas the proposed approach makes use of Attribute-Based Encryption (ABE) which provides fine-grained access control of data. Fine-grained access mechanism provides detailed level of authorization as compared to coarse-grained access mechanism. Ciphertext Policy Attribute Based Encryption (CP-ABE) provides fine-grained access mechanism but involves some complex computations due to which there is computational delay involved. Our proposed approach makes use of enhanced ECC encryption algorithm based on user defined attributes on the sensor-cloud architecture, in order to provide an efficient as well as transparent security mechanism through which data owner can have complete control over their data by specifying the role based access control rules. The proposed fine grained access control approach guarantees the confidentiality and integrity and at the same time reducing the overall computational overhead and in turns makes the system more efficient as well as robust. The results clearly depicts that the proposed approach achieves faster encryption, decryption and key generation along with the more complex ECC keys as compared with traditional CP-ABE.

Keywords: Data security, Sensor-Cloud, Elliptic Curve Encryption, Ciphertext-Policy Attribute-Based Encryption.

1. Introduction

In recent years, the emergence of the Internet of Things (IoT) has revolutionized various industries by connecting physical devices to the internet, enabling data collection, analysis, and automation. One of the key components that has played a pivotal role in the IoT ecosystem is sensor technology. Sensors have the ability to detect and measure physical phenomena, such as temperature, humidity, light, and motion. However, with the proliferation of sensors and the exponential growth of data generated by these devices, there arises a need for efficient data management and processing. This is where the concept of Sensor-Cloud comes into play.

Sensor-Cloud represents the integration of sensor networks with cloud computing technologies to enhance the capabilities and efficiency of data collection, storage, processing, and analysis. It combines the power of sensors, which capture real-time information from the physical world, with the scalability, flexibility, and computational resources offered by cloud computing platforms. [1, 2] The fundamental idea behind Sensor-Cloud is to leverage the advantages of cloud computing to overcome the limitations of traditional sensor networks. In traditional setups, sensors are usually connected through a local network and have limited storage and processing capabilities. As a result, the data collected by these sensors is often restricted to a local environment and cannot be easily shared or accessed by other applications or users. Sensor-Cloud, on the other hand, enables sensors to connect to the cloud infrastructure, where they can seamlessly transmit data, store it in remote servers, and perform complex analytics. By harnessing the power of the cloud, Sensor-Cloud provides a scalable and cost-effective solution for managing massive amounts of sensor data. It eliminates the need for local storage and computational resources, as the cloud infrastructure can handle the processing and storage requirements of the sensor network. Sensor-Cloud finds its utility in variety of applications such as Smart Agriculture, Industrial IoT, Environmental Monitoring, Smart Cities, Healthcare etc. [3, 4]

The benefits of Sensor-Cloud are manifold. Firstly, it allows for centralized data management, where data from multiple sensors can be aggregated, processed, and stored in a unified manner. This facilitates real-time monitoring, analysis, and decision-making, enabling businesses and organizations to derive valuable insights from the collected data. Secondly, Sensor-Cloud provides a platform for collaboration and data sharing among different stakeholders. Moreover, Sensor-Cloud offers enhanced scalability and flexibility. As the number of sensors and the volume of data grow, the cloud infrastructure can easily accommodate the increasing demands without requiring significant hardware upgrades or infrastructure changes. [5, 6] Additionally, Sensor-Cloud enables remote access to sensor data, allowing users to monitor and control sensor networks from anywhere at any time. However, along with the advantages, Sensor-Cloud also presents certain challenges and considerations. Issues such as data security, privacy, network connectivity, and interoperability need to be addressed to ensure the successful implementation and adoption of Sensor-Cloud solutions. [8, 9, 10]

2. Preliminaries

This section describes the background details about the architecture of the "Sensor-Cloud" and Elliptic Curve Encryption thereby giving a brief idea about both of them.

2.1 Architecture of "Sensor-Cloud"

The architecture of Sensor-Cloud typically consists of the following components:

1. Sensors: These are physical devices equipped with various sensors to capture real-world data, such as temperature, humidity, motion, or light. The sensors are responsible for collecting the data from the environment.

2. Sensor Nodes: Sensor nodes act as intermediaries between the sensors and the cloud infrastructure. They receive data from the sensors, process and package it, and transmit it to the cloud for further processing and storage. Sensor nodes often include microcontrollers or microprocessors, communication modules, and memory for data buffering. [11, 13]

3. Communication Network: The communication network connects the sensor nodes to the cloud infrastructure. It can be wired or wireless, depending on the deployment scenario and requirements. Wireless communication protocols such as Wi-Fi, Bluetooth, or cellular networks are commonly used to transmit sensor data to the cloud.

4. Cloud Infrastructure: The cloud infrastructure consists of servers, storage systems, and networking components hosted in data centers. It provides the computational resources, storage capacity, and scalability required to handle the large volumes of data generated by the sensors. The cloud infrastructure can be public, private, or hybrid, depending on the specific needs of the application. [16, 17, 18]

5. Cloud Services: Within the cloud infrastructure, various cloud services are utilized to process and manage the sensor data. These services can include data storage, data processing, analytics, machine learning algorithms, and APIs for data access and integration with other applications.

6. Data Processing and Analytics: The cloud services perform data processing and analytics on the sensor data. This can involve tasks such as filtering, aggregation, normalization, and applying advanced analytics techniques to derive meaningful insights from the data. The processed data can be stored in databases or data warehouses for further analysis and visualization.

7. Applications and Services: The output of the data processing and analytics phase is made available to applications and services that can utilize the sensor data for specific purposes. These applications can range from real-time monitoring and control systems to predictive maintenance, resource optimization, or decision support systems. The applications can be accessed by end-users through web interfaces, mobile apps, or APIs.

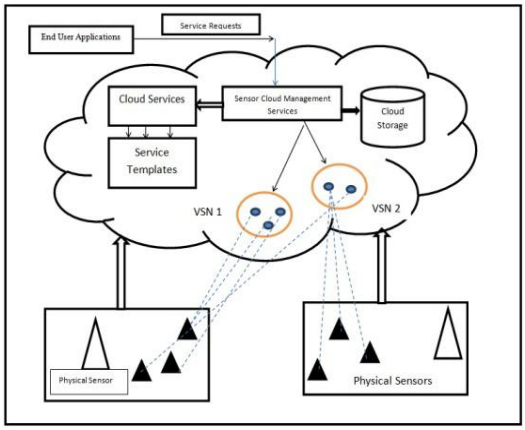

Figure 1. Architecture of "Sensor-Cloud"

2.2 Elliptic Curve Encryption

ECC, or Elliptic Curve Cryptography, is a modern encryption technique widely used in various cryptographic systems to ensure secure communication and data protection. It is based on the mathematical properties of elliptic curves over finite fields. ECC offers strong security with relatively shorter key lengths compared to other encryption algorithms like RSA. The strength of ECC lies in the computational difficulty of reversing the scalar multiplication process without knowledge of the private key. The large size of the elliptic curve and the complexity of the mathematical operations involved make it computationally infeasible to determine the private key from the public key or the ciphertext. The four phases of ECC are described below. [20, 21, 22]

1. Key Generation: In ECC, the first step is key generation. A user selects a specific elliptic curve defined over a finite field, and a base point (also known as a generator point) on that curve. The base point is a fixed point on the curve with special properties. Using the base point, the user generates their private key, a random number within a certain range. The private key remains secret and must be kept confidential.

2. Public Key Calculation: The user then calculates their public key by performing a mathematical operation called scalar multiplication. Scalar multiplication involves multiplying the private key with the base point on the elliptic curve. The result is a new point on the curve, which becomes the user's public key. The public key is shared with others and does not need to be kept secret.

3. Encryption: Suppose User A wants to send an encrypted message to User B. User A obtains User B's public key, which is used in the encryption process. The encryption process involves the following steps: a. User A converts the message into a numerical value. b. User A generates a random value called the ephemeral key, which is used only for this specific encryption. c. User A performs scalar multiplication of the ephemeral key with User B's public key on the elliptic curve. This generates a new point on the curve. d. User A takes the x-coordinate of the generated point and uses it as the ciphertext.

4. Decryption: User B receives the ciphertext from User A and wants to decrypt it. The decryption process involves the following steps: a. User B performs scalar multiplication of their private key with the received ciphertext (x-coordinate) on the elliptic curve. This generates a new point on the curve. b. User B takes the x-coordinate of the generated point and converts it back into the original numerical value. c. User B converts the numerical value into the original message.

3. Literature Review

This section gives an overview about some of the latest and authentic research work that have been carried out for providing secure frameworks for Sensor-Cloud based healthcare applications.

Mehmood et al. [22] proposed a framework that provides enhanced privacy mechanism based on Elliptic curve cryptography (ECC) for cloud based healthcare applications. In order to provide enhanced anonymity to the sensitive healthcare data, this approach utilizes the TOR at the network layer which in turns restricts the network eavesdroppers from penetrating in the network. Evaluation features such as, traceability, anonymity, defence against modification attacks, mutual authentication and forward unlink ability were compared with the other state of art methodologies and the simulation results clearly depicts that the proposed security mechanism provides strong defence against these parameters. Hema et al. [23] suggested the importance of secure sharing the patient's critical data in the cloud based environment. The sensitive data is encrypted via ECC (Elliptic curve cryptography). TTP-CS (Trusted Third Party-Cryptographic Server) which is responsible for the computation of Elliptic curve cryptography (ECC) mathematics, HC (Health Cloud) is maintains the sensitive healthcare records in the cloud environment and the last component includes CU (Cloud Users) who are the primary consumers of the healthcare data (such as patient, doctors, insurance agents etc). The above three modules which comprises of the architecture of the proposed system. For performance evaluation the parameters such as turn-around time, file-upload time, key-generation time, file-uploading speed, encryption time and download time were considered and the results clearly depicts the supremacy of the proposed approach over the traditional approaches.

Humayun et al. [24] proposed a framework that could provide enhanced security as well as manages the energy efficiently so that the IoT (sensor-cloud) based healthcare devices can transmit the data over cloud securely. The Cooja Contiki simulator is utilized for performing the simulation and the results clearly depicts that the proposed approach outperform the traditional methodologies. Primarily there are four layers that works in collaboration with each other in order to constitute the working of the proposed framework. Wearable IoT devices, smart devices (tablet etc), the cloud environment for healthcare applications, actual application for the end users comprises the layer 1, layer 2, layer 3 and layer 4 respectively.

Sowjanya et al. [25] secures the risk of information leakage during the transmission of the medical data from the IoT sensors to the cloud environment. An authentication protocol based on light weighted ECC (Elliptic curve cryptography) is employed by the proposed approach. In order to analyze the security of the proposed approach the parameters such as defence against DoS, impersonation, insider and replay attacks, clock synchronization and user anonymity were considered by the proposed approach and the result clearly depicts that the proposed approach outperforms the traditional approaches.

ZHANG et al. [26] proposed a fine grained based cipher text policy attribute based encryption (CP-ABE) scheme that overcomes the limitations of size of the user attributes as well as decryption key cost. The attributes created by the end users are transferred to the cloud servers in the traditional approaches, is removed in the proposed approach. The proposed cipher text policy attribute based encryption (CP-ABE) shows a remarkable decrease in the decryption time. Access structure, fast decryption and data authenticity are three primary components of this approach. The access structure is responsible for

transferring the cipher text along with the access matrix. ECC decryption is time is reduced with the reduction in bilinear pairing. FH-CP-ABE (File Hierarchy cipher text policy attribute based encryption) is given by Chandrasekaran et al. [22] in order to provide an enhanced WBANs and cloud servers communications. FH-CP-ABE supports the transfer of multiple files of hierarchical structure. The performance evaluation is performed on various parameters such as energy consumption, cost for computation as well as size of the message transferred.

4. Proposed Framework For Security Over Sensor Cloud Based Healthcare Applications

For the purpose of continuous monitoring of the health status of a patient, various body sensors are used by the patients. These body sensors are wearable devices worn by patients that can collect various body data such as heart beat rate, blood pressure, body temperature etc. There are many medical cases in which the continuous monitoring of health conditions are required which allows doctors to monitor the health status of the patients regularly or when required in the case of emergency. This minimizes the healthcare treatment cost and allowing the mobility of patients. The data collected by these sensors are forwarded to gateways such as mobile phones via wireless communication medium and from gateways finally transferred to the cloud for storage and processing.

The proposed framework involves primarily three entities for functioning namely, data owner i.e. the patient who is the prime owner of the data which is collected from the various sensors connected to the patient's body some of which are described in table 1, healthcare security authority (HSA) whose major responsibility is to create security policies as well as to store the patient's medical record in its cloud storage servers and the data consumers who are the entities requiring the patient's medical record some of which are described in table 2.

Table 1. Medical Sensors for connected body

S. No.	Medical Sensors	Sensor Category	Description
1	BioHarness 3	Performance Monitoring	Captures and transmits comprehensive physiological data
2	Lumafit Sensor	Wearable Activity Tracker	Monitors exercise as well as heart rate during workout sessions
3	Wireless Blood Pressure Wrist Monitor	Blood Pressure Wrist Monitor	Monitors Blood Pressure
4	Dexcom G4	Continuous Glucose Monitor	Monitors glucose and gives information on managing the diabetes
5	Google Glass	Wearable Technology	Provides Augmented Reality experience

6	Fitbit Flex	Wearable Technology	Tracks sleep, activity, diet etc
7	Heart Monitor	Heart Monitor	Tracks ECG heart rate
8	Helius	Ingestible Sensors	Tracks real time information about rest patterns, medications and activity
9	t:slim Insulin Pump	Insulin Pump	Provides regular flow of insulin as per requirement
10	BodyMedia Fit	On-Body Monitoring System	Gathers information regarding moisture, movement and temperature

In the initial step, the patient gets registered with the Healthcare Security Authority (HSA). The HSA inquires about the lists of attributes from the registered patient and saves in its cloud database. HSA issues all the authentic attributes so as to create the access policy rules and avoid the unauthorized access to the patient's (data owner) data. The patient has complete control in specifying the access rules (role-based policy) separately for each end user (data consumer) with the help of conjunction or disjunction. HSA creates a unique encryption key (EK) as well as decryption key (DK) using the specified access rule for each data consumer. The data owner (patient) uploads the sensitive medical records to the HSA's cloud servers. HSA encrypts the sensitive medical records with the ECC encryption key with the EK and the ECC encryption keys (EK + EK_ECC). The encrypted medical record is uploaded to the HSA's cloud storage servers. Upon the request of the specific medical record from data consumer (end user), the HSA first whether the data consumer is allowed to have the access rights to the medical record against the access rule created by the data owner (patient). If the HSA finds the data consumer as the authorized personnel then the requested medical file id decrypted using the DK and ECC decryption keys (DK + DK_ECC). Figure 2 and figure 3 describe the architecture and workflow model of the proposed framework.

Table 2. Healthcare data consumers

S. No.	**Healthcare data consumers**	**Description**
1	Healthcare Providers	Healthcare providers, including hospitals, clinics, and physicians, rely on healthcare data to deliver quality care and improve patient outcomes. By accessing and analyzing this data, healthcare providers can make informed decisions, personalize treatment plans, track patient progress, and enhance coordination among care teams.
2	Medical Research and Clinical Trials	Researchers and scientists use large datasets, including clinical data, genetic information, and population health data, to study diseases, identify risk factors, and explore potential treatment options. Clinical trials heavily rely on healthcare data to evaluate the safety and effectiveness of new drugs or interventions.

3	Public Health	Public health organizations and agencies utilize healthcare data to monitor and manage public health concerns. Data on disease prevalence, outbreaks, vaccination rates, and environmental factors are analyzed to identify patterns, track the spread of diseases, and implement preventive measures.
4	Health Insurance and Payers	Health insurance companies and payers rely on healthcare data to assess risks, determine premiums, and manage claims. Claims data provides insights into treatment costs, healthcare utilization patterns, and effectiveness of interventions.
5	Health Tech and Digital Health Companies	Health tech and digital health companies leverage healthcare data to develop innovative technologies, tools, and applications that improve healthcare delivery and empower patients. Analyzing this data enables health tech companies to provide personalized insights, preventive care recommendations, and remote patient monitoring.
6	Government and Policy Makers	Governments and policy makers rely on healthcare data to develop public health policies, allocate resources, and make evidence-based decisions. Data on healthcare utilization, disease prevalence, healthcare disparities, and population health outcomes help shape policies to improve healthcare access, quality, and affordability.

Proposed ECC Encryption Algorithm

Step 1: Key Generation

- Select an elliptic curve defined over a finite field, represented as E(Fp), where p is a prime number.
- Choose a base point G on the elliptic curve.
- Generate a private key, d, which is a random number in the range [1, n-1], where n is the order of the base point G.
- Calculate the public key by performing scalar multiplication: Q = d * G.
- Identify the User Attributes
- Apply the key derivation algorithm PBKDF2 (Password-Based Key Derivation Function 2) on the identified user attributes EK
- Key=Q+EK

Step 2: Encryption

- Convert the plaintext message M into a numerical value.
- Choose a random number k in the range [1, n-1] as the ephemeral key.

- Compute the ephemeral point P = k * G on the elliptic curve.
- Compute the shared secret point S = k * Key = k * (d * G) on the elliptic curve.
- Take the x-coordinate of the shared secret point S and use it as the ciphertext C.

ECC Decryption Algorithm:

Step 1: Key Generation

- Generate a private key, d, within the same range used for the encryption process.
- Calculate the corresponding public key, Q = d * G.

Step 2: Decryption

- Retrieve the ciphertext C.
- Perform scalar multiplication to recover the shared secret point S = d * P = d * (k * G).
- Take the x-coordinate of the shared secret point S and convert it back into the original numerical value.

Convert the numerical value back into the original plaintext message M.

5. Performance Evaluation

5.1 Implementation Setup

The proposed framework is implemented using .NET framework version 5 with Visual Studio 2019 as the IDE. The web application is created for the data owner in order to get registered with the HSA and be able to upload the medical record data, whose overflow model is depicted in figure 3. The technologies involved in the development of the applications are C#, ASP.NET, ADO.NET, JQuery. For cloud storage our application uses Microsoft Azure SQL database. Microsoft Azure SQL Database is a cloud-based relational database service that offers high-performance, scalable, and secure storage for structured data. It provides organizations with the flexibility to manage their databases efficiently while benefiting from Azure's robust infrastructure and advanced data management capabilities.

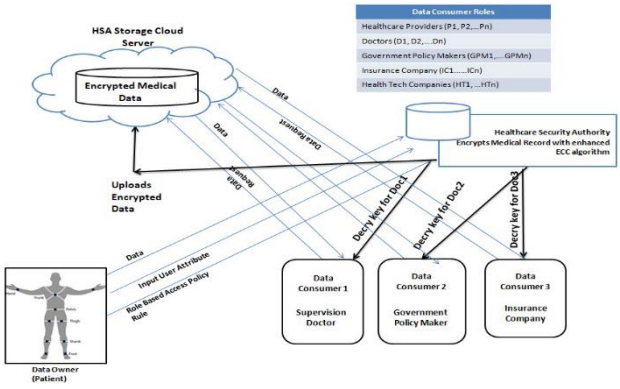

Figure 2. Proposed Framework

MHEALTH Dataset is utilized for the performance testing of our proposed approach which contains the data captured from the body sensors and is downloaded from UC Irvine Machine

Learning Repository []. MHEALTH (Mobile HEALTH) dataset includes records from ten volunteers' body motion and vital signs as they engaged in a variety of physical activities. Each individual left ankle, chest and right wrist are fitted with sensors that record the magnetic field orientation, acceleration and rate of turn. The sensor, which is placed on the chest, also generates 2-lead ECG readings, which are utilized for routine cardiac monitoring, screening for different arrhythmias, or examining affects of ECG.

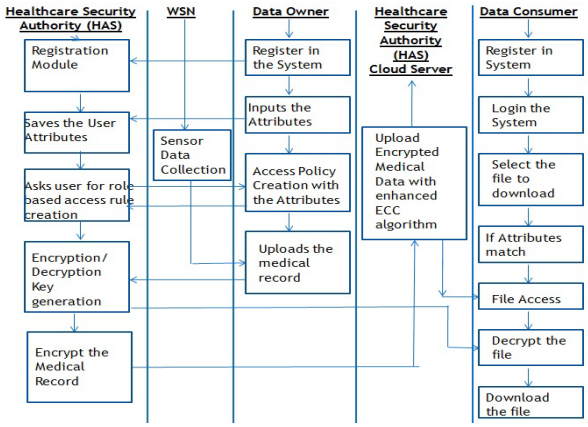

Figure 3. Workflow of the Proposed Framework

5.2 Encryption, Decryption, Key-Generation Time Analysis

The varying size files of size 10KB, 20KB, 30KB, 40KB, 50KB, 60 KB were used which contains data from various medical sensors for the purpose of evaluating the time needed for encrypting, decrypting and key generation for these files by existing CP-ABE scheme as compared with the proposed scheme. It is observed that our proposed scheme produces better result in all these three circumstances. The figures 4, 5, 6 clearly depict these analysis.

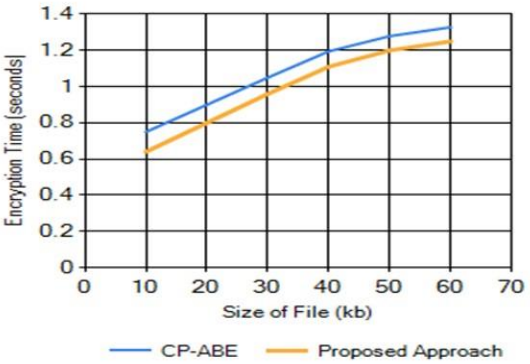

Figure 4. Encryption time analysis

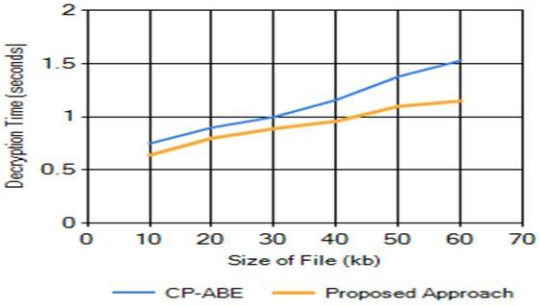

Figure 5. Decryption time analysis

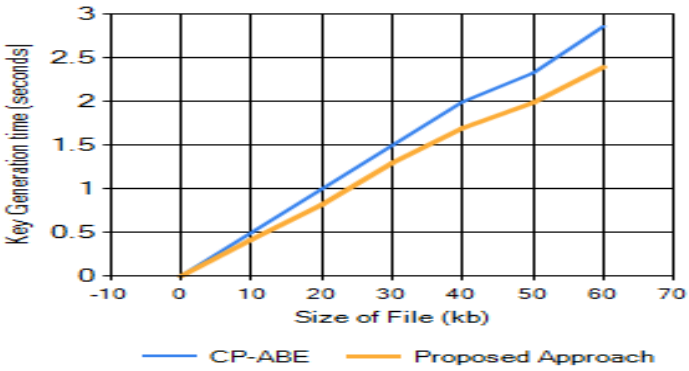

Figure 6. Key-Generation time analysis

Table 3. Summary of Complexity Analysis

S. No.	**Size of File (Kb)**	**Encryption Time (seconds)**		**Decryption Time (seconds)**		**Key Generation Time (seconds)**	
		CP-ABE	Proposed Approach	CP-ABE	Proposed Approach	CP-ABE	Proposed Approach
1	10	0.75	0.64	0.75	0.64	0.5	0.42
2	20	0.9	0.8	0.9	0.8	1	0.82
3	30	1.05	0.96	1.0	0.89	1.5	1.299
4	40	1.195	1.11	1.16	0.96	2	1.699
5	50	1.279	1.2	1.38	1.1	2.33	1.99
6	60	1.328	1.25	1.53	1.15	2.866	2.399
7	90	1.561	1.29	1.58	1.21	2.99	2.401
8	100	1.588	1.31	1.59	1.26	3.19	2.446
9	150	1.725	1.41	1.68	1.34	3.57	2.563

Conclusion

Healthcare data security is crucial in today's era in order to protect patient privacy, comply with regulations, prevent data breaches, ensuring continuity of care and maintain trust in the healthcare system. By prioritizing data security healthcare organizations can safeguard sensitive information, mitigate risks, and contribute to the delivery of high-quality healthcare services. The healthcare industry faces numerous cyber attacks targeting patient data among which some of the common attacks includes Ransomware Attacks, Data Breaches, Phishing Attacks, Insider Threats. DoS/DDoS Attacks, Credential Theft etc. In order to mitigate against these threats there must be a security authority deployed that can provide efficient as well as transparent defence mechanism. Our proposed approach makes use of enhanced ECC encryption algorithm based on user defined attributes on the sensor-cloud architecture, in order to provide an efficient as well as transparent security mechanism through which data owner can have complete control over their data by specifying the role based access control rules. The proposed framework contributes to the development of secure and trustworthy

smart healthcare systems that can harness the benefits of sensor data at the same time safeguarding patient privacy. The results clearly depicts that the proposed approach achieves faster encryption, decryption and key generation along with the more complex ECC keys as compared with traditional CP-ABE.

Refrences

[1] Sensor-Cloud, http://sensorcloud.com/system-overview.
[2] Dwivedi, R.K., Saran, M., Kumar, R.: A Survey on Security over Sensor-Cloud. In: *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, pp. 31-37, 2019.
[3] Dwivedi, R.K., Pandey, S., Kumar, R.: A Study on Machine Learning Approaches for Outlier Detection in Wireless Sensor Network. In: *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 189-192, 2018.
[4] Dwivedi, R.K., Singh, S., Kumar, R.: Integration of Wireless Sensor Networks with Cloud: A Review. In: *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, pp. 115-120, 2019.
[5] Dwivedi, R.K., Kumar, R.: Sensor Cloud: Integrating Wireless Sensor Networks with Cloud Computing. In: 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, India, 2018.
[6] Alamri, A., Ansari, W.S., Hassan, M.M., Hossain, M.S., Alelaiwi, A., Hossain, M.A.: A Survey on Sensor-Cloud: Architecture, Applications, and Approaches. In: International Journal of Distributed Sensor Networks, pp. 917-923, 2013.
[7] Islam, M.M., Hassan, M.M., Lee, G.W., Huh, E.N.: A Survey on Virtualization of Wireless Sensor Networks. In: Sensors, pp. 2175-2207, 2012.
[8] Thilakanathan, D., Chenb, S., Nepal, S., Calvo, R., Alemb, L.: A platform for secure monitoring and sharing of generic health data in the Cloud. In: Future Generation Computer Systems, pp. 102-113, 2014.
[9] Tu, S., Niu, S., Li, H., Xiao-ming, Y., Li, M.: Fine-grained access control and revocation for sharing data on clouds. In: 26th international parallel and distributed processing symposium workshops and PhD forum, pp. 2146–2155, 2012.
[10] Li, M., Yu, S., Zheng, Y., Ren, K., Lou, W.: Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. In: IEEE Transactions on Parallel and Distributed Systems, pp. 131–143, 2013.
[11] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: Symposium on Security and Privacy, pp. 220-239, 2007.
[12] Sayantani, S.: Secure Sensor Data Management Model in a Sensor-Cloud Integration Environment. In: Applications and Innovations in Mobile Computing, pp. 325-332. 2015.
[13] Lauter, K.: The Advantages of Elliptic Curve Cryptography For Wireless Security. In: IEEE Wireless Communications, pp. 62-67, 2004.
[14] Li, J., Zhao, G., Chen, X., Xie, D., Rong, C., Li, W., Tang, L., Tang, Y.: Fine-grained data access control systems with user accountability in cloud computing. In: IEEE second international conference on cloud computing technology and science, pp. 89–96, 2010.
[15] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: 13th ACM conference on computer and communications security, pp. 89–98 2006.
[16] Yang, K., Han, Q., Li, H., Zheng, K., Su, Z., Shen, X.: An efficient and fine-grained big data access control scheme with privacy-preserving policy. In IEEE Internet of Things Journal, pp. 563-571, 2017.
[17] Odelu, V., Das, A.K.: Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography. In: Security and Communication Networks, pp. 4048-4059, 2016.

[18] Pussewalage, H.S.G., Oleshchuk, V.: A patient-centric attribute based access control scheme for secure sharing of personal health records using cloud computing. In: 2nd International Conference on Collaboration and Internet Computing, pp. 46-53, 2016.
[19] Sharma, P., Dwivedi, R.K.: Detection of High Transmission Power Based Wormhole Attack Using Received Signal Strength Indicator In: Verma S., Tomar R., Chaurasia B., Singh V., Abawajy J. (eds) Communication, Networks and Computing. CNC 2018. Communications in Computer and Information Science, vol 839, Springer, Singapore, pp. 142-152, 2019.
[20] Chandrasekaran, B., Balakrishnan, R.: Efficient pairing computation for attribute based encryption using MBNR for big data in cloud. In: 2nd International Conference on Applied and Theoretical Computing and Communication Technology, pp. 243-247, 2016.
[21] Tran, D.H., Nguyen, H.L., Zha, W.: Towards security in sharing data on cloud based social networks. In: 8th International conference on information, communications and signal processing, pp. 1–5, 2011.
[22] Hung, N.T., Giang, D.H., Keong, N.W., Zhu, H.: Cloud-enabled data sharing model. In IEEE International Conference on Intelligence and Security Informatics, 2012.
[23] Yang, Y., Zhang, Y.: A Generic Scheme for Secure Data Sharing in Cloud. In 40th International Conference on Parallel Processing Workshops, 2011.
[24] Pérez, S., Rotondi, D., Pedone, D., Straniero, L., Núñez, M.J., Gigante, F.: Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts. In: International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 917-926, 2017.
[25] Chhabra, A., Arora, S.: An Elliptic Curve Cryptography Based Encryption Scheme for Securing the Cloud against Eavesdropping Attacks. In: International Conference on Collaboration and Internet Computing, pp. 261-269, 2017.
[26] Gupta, D.S., Biswas, G.P.: A Secure Cloud Storage using ECC-Based Homomorphic Encryption. In: International Journal of Information Security and Privacy, pp. 550-578, 2017.