IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Data Security Of Medical Data In Cloud Computing Environments Through A Combination Of Elliptic Curve Cryptography With A Hybrid Encryption Framework

[1]Madhira Srinivas, [2]Porika Sammulal

[1]Research Scholar, [2]Professor

[1]Department of Computer Science & Engineering, JNTUH University, Hyderabad, Telangana, India.

[2]Department of Computer Science & Engineering, JNTUH University, Hyderabad, Telangana, India.

Abstract: Recent advancements in smart cloud computing have yielded numerous advantages, particularly through innovations like the Internet of Things (IoT), which interconnects ordinary objects via the Internet. These IoT devices, equipped with sensors and actuators, collect and transmit data. However, maintaining the confidentiality of users' medical data is paramount, as any breach could endanger lives. To address this, attribute-oriented encryption (AOE) is commonly used for data security and access control. Yet, conventional AOE's processing demands are substantial. To tackle this, an efficient security approach merges AOE with Fully Homomorphic Encryption (FHE) to safeguard sensitive medical information and financial data. For cloud-based data encryption, AOE is a suitable choice for one-to-many communication and access control. Cloud servers can employ FHE to process encrypted data directly. Additionally, elliptic curve cryptography (ECC), known for its high security and compact key size, is integrated. This hybrid AOE-FHE-ECC approach offers reduced computational and storage burdens compared to existing methods. The proposed approach's security is supported by the Decisional Bilinear Diffie-Hellman postulate. Experimentation reveals its superiority, especially for resource-constrained devices, compared to traditional AOE.

Index Terms **- Internet of Things, Attribute oriented Encryption, Fully Homomorphic Encryption, Elliptical Curve Cryptography, Elliptical Curve Encryption, Computational Cost, Storage Burden, Secure Transmission.**

I. INTRODUCTION

Connectivity between mobile phones, sensors, RFID tags, and smart structures has been made possible by improvements to the IoT's underlying global information system architecture. These connected devices may collect and share information over both wireless and wired networks. The development of the Internet of Things has made it possible to access almost anything, at any time, from almost any location, and have it do virtually any task. The Internet of Things, or IoT, is made up of a network of interconnected devices that enable distributed computation and monitoring. Challenges with the Internet of Things include limited power, connection, and computing power. Medical devices have been quick to embrace IoT because of its potential to improve service quality and efficiency (Khari et al., 2020; Pulkkis et al., 2017; Y. Yang et al., 2017).

In smart cities, S-health (Smart health) has emerged as a situational upgrade to telehealth, allowing for more precise and effective illness and accident prevention. In fact, the Internet of Things is often employed as a foundational technology in smart cities to connect easily available healthcare resource services and to provide reliable and effective s-health care to the elderly patients (Y. Zhang et al., 2018). Recent healthcare policy shifts throughout the globe have shifted focus from treating diseases to caring for individual patients (SA, 2018). Implementing an EHR system has been shown to improve patient continuity, healthcare system efficiency, patient safety, and the quality of medical treatment all while reducing costs. Because of how effortlessly it handles and communicates health data, it has made its way into the medical sphere.

For continuous physiological monitoring, chronic illness evaluation, and therapeutic training, the s-health (Y. Yang et al., 2017) system may link a variety of healthcare equipment. Until then, s-health can increase the standard of treatment while decreasing costs. Cloud-based smart health is expected to provide sufficient medical care in the coming years as a result of the rapid development of Cloud technology advances. As a relatively new field, s-health has a way to go before it is ready for widespread use. It is still difficult to ensure the security and privacy of IoT users' highly sensitive personal healthcare information without compromising the usefulness of these devices (Y. Zhang et al., 2018). reducing the value of the information (Y. Yang et al., 2017). Vital signs like heart rate and blood pressure are recorded in a patient's s-health records (SHRs), which are normally only accessible to authorized qualified healthcare professionals. But most access control solutions either don't care about data security or just provide rudimentary protections.

This line of thinking implies that traditional methods of securing end-to-end data confidentiality via the exchange of keys are inadequate in light of these new challenges. Therefore, Attribute Oriented Encryption (AOE) (Salvador et al., 2017) is a novel security feature that enables encrypting data users' self-access restrictions, which describe the requirements a subject must meet to completely decode data; hence, AOE is seen as a potential method for achieving perfectly alright access control (Y. Zhang et al., 2018). Both KP-ABE and CP-AOE, or Key- and Ciphertext-based Attribute-based Encryption, exist as ABE schemes. Private keys of user data are connected with a wide range of qualities in accordance with the access control method indicated in CP-AOE schemes, ensuring the safety of personal health records (PHRs). These encrypted PHRs are only accessible to those whose profiles match the criteria for gaining entry to the data. CP-AOE systems do not have a substantial key management cost or repeated ciphertexts, in contrast to traditional encryption algorithms that encrypt data using paired keys or create many ciphertexts for several users.

The KP-AOE method involves linking the decryption key of a participant to a tree-like access structure and the ciphertext to a set of parameters. Tree access structure must be satisfied by the ciphertext parameters before they may be decoded by the user (Iao et al., 2019; Tu et al., 2021). Using both private and public information (such as its job), the AOE algorithm creates a unique key for each topic. The user's key can decode the data successfully only if the recipient's attributes match the access requirements inside that access policy (Salvador et al., 2017). Current AOE methods, however, require a great deal of computing and so are unsuitable for use in s-health. Energy consumption and processing speed are perennial limitations for microelectromechanical systems and other small smart devices. Multiple owners and users of an Internet of Things system need a lightweight access control system (Y. Yang et al., 2017). One of the most common methods for dealing with this problem is fully homomorphic encryption (FHE). FHE allows an endless number of arithmetic operations to be done on encrypted data with the same results as operations on plain data. When it comes to the outcomes of calculations performed on encrypted data, the persons in charge of such computations know nothing about either the data or the computations themselves (Wang et al., 2017). In 1978, (Rivest et al.) examined the possibility of creating a homomorphic encryption method. This concept is the result of several attempts by researchers to create homomorphic systems with many operations.

According to (Acar et al., 2018; Sen, 2013), homomorphic encryption refers to a family of cyphers that may be used for a wide range of computations on encrypted data. Acar et al. (2018) and Gentry (2009) list many common homomorphic encryption schemes, including partially homomorphic, relatively homomorphic, leveled fully homomorphic, and absolutely homomorphic encryption. With fully homomorphic encryption (FHE), any number of operations may be performed in parallel. For any given function, FHE systems may theoretically conduct an infinite number of homomorphic operations (Acar et al., 2018; Armknecht et al., 2015; Gentry, 2009), making this theory the cornerstone of homomorphic encryption. IoT systems must fulfill tougher security and reliability criteria than the vast majority of other IoT systems (Pulkkis et al., 2017) to preserve the privacy and confidentiality of persons. The Situation As It

Is The quantity of out-patient health data that end users can readily handle is expected to expand dramatically with the development of biosensors and mobile computing technologies (Bao et al., 2017).

However, there is still a lack of consensus on how to safeguard highly sensitive personal health data in IoT without compromising data usefulness (Y. Yang et al., 2017) despite the fact that these concerns are becoming more widespread in s-health (Y. Zhang et al., 2018). The transport of patient data from sensing equipment to the web and then to physicians' mobile devices requires a sophisticated encryption approach to ensure patient privacy. Purpose and Goals This project intends to develop a lightweight hybridized AOE-FHE system using elliptic curve encryption to safeguard data inside Smart Healthcare. The goals are to (i) create a lightweight hybridized AOE-FHE method for securing data in Smart Healthcare and (ii) assess the system with the use of a Decisional Bilinear Diffie-Hellman (DBDH) assumption. Why This Research Is Important All the pieces necessary to safeguard intelligent healthcare data are included in this study's coverage of AOE and FHE methods. These methods were then used to ECC in order to shrink the final output file. These capabilities allow for secure computation on encrypted data, private and secure user information, one-to-many communication, and fine-grained access control.

II. Related Work

In healthcare, all 5 Vs are crucial since so many different kinds of information, from patient names and birth dates to vital sign numbers, are gathered on a regular basis and need to be stored in different databases. The amount of data gathered throughout time is expected to grow exponentially if data collection is performed on a daily basis. In a recent study (Boyi et al., 2014), researchers assessed the diversity and amount of health information to create a digital memory system supporting vital medical treatment. The program's ultimate goal is to have all relevant medical personnel able to quickly access and review a wide variety of relevant biological information in the event of an emergency. Some studies on the best methods for securing a medical facility have been conducted (Baker et al., 2017).

Patient data ownership is emphasised in (Thilakanathan et al., 2016), where a comprehensive access control method called "Safe Protect" is proposed. In (Pacheco et al., 2016), a secure cloud technique is described for "enhanced lifestyles," which frequently include both wearables used by the patient and intelligent home technologies with the goal of supporting elderly or disabled people in living independently. With FHE (Wang et al., 2017), encrypted data may undergo unconstrained multiplications and additions, with encrypted results being equal to those of operations performed on plain data. For this reason, cloud infrastructure may lawfully process encrypted data without first decrypting it (Y. Liu et al., 2021). Homomorphic technology began with the introduction of asymmetric encryption in 1978, and the idea of homomorphic encryption was first proposed by (Rivest et al., 1978).

RSA is a multiplicative-only partial homomorphic approach. Neither addition nor multiplication are guaranteed by PHE systems. Multiple homomorphic encryption schemes followed shortly afterwards (Kara et al., 2021). Researchers have lately voiced worry about the FHE problem due to the growing volume of collected data and the resulting lack of sufficient resources to process or store it. The concept of FHE was initially presented by (Gentry, 2009). He used a "bootstrapping" method to limit the growth of noise and check the decryption's precision, and then he added homomorphic multiplication and the summing of encrypted data to the system. However, the private key must be encrypted before it can be used in the "boot-strapping" process and made available as a public parameter. Since the scheme's inception in 2009, numerous methods have been implemented to enhance it, such as Fully Homomorphic Encryption based on BGV, GSW, Integer, and Multi-key Fully Homomorphic Encryption Schemes (Yousuf et al., 2021). Van Dijk et al. (2010) suggested a basic FHE technique based on the approximate greatest common divisions problem (A-GCD). The proposed technique is theoretically less complex than the one used in (Gentry, 2009). The recommended bootstrap security method makes use of arithmetic over integers rather than depending simply on ideal lattices a top polynomial bands.

However, the very lengthy public key length of O (N) is a trade-off for this ease of use. Instead of decrypting the data, the transformation may be performed in a recursive fashion by using the Advanced Encryption Standard (AES) to FHE conversion method proposed by (Gentry et al., 2012). Using AES for data collection

and then converting into FHE using the Advanced Encryption Standard-to-Fully homomorphic encryption (FHE) transformation mechanism was found to be a potential good solution (Kocabas et al., 2016), which compared FHE to both the traditional AES and the recently developed ABE. To protect data integrity, FHE was investigated by (Khedr & Gulak, 2018), however, it was found that FHE necessitates a lot of computer power. Using the learning-with-errors (LWE) assumption, Boneh et al. (2018) presented a threshold FHE.

To solve the issue of threshold inscriptions of lattices in a single round, the suggested TFHE is implemented in a universal thresholdizer. Threshold features are then integrated into many other systems, including authentication platforms, CCA-public-key encryption (PKE) secured procedures, and more (Kara et al., 2021). (W. Cheng et al., 2020) proposed a framework for protecting patients' personal information using federated learning and verification. The system combines homomorphic encryption, cryptography, and distributed learning to keep patient data secure while allowing for decentralized and centralized data training. Each client, or device, collects data locally and shares it with the central server. A more robust security clustering approach for data encryption was presented by (H. Lin et al., 2021). This complements the opportunity strategy that encourages people to submit material to the health system.

The approach combines mobile edge computing (MEC) with the IoT to facilitate COVID-19 functions such as storing, processing, and analysing data. All data processing is performed at the network's periphery rather than in a centralised cloud. Data processing is performed on MEC, which offers better speeds and secrecy protection, and was shown in a distributed system with data sharing and dispatching capabilities (Nguyen et al., 2021). Smart contracts are the design's defining characteristic since they enable the authentication and monitoring of data transmissions. There is no longer any requirement for a central system or party to accept an access request in order to publish material when contracts are in place to verify the validity of the participant. Since data is stored in chunks, its integrity is preserved; any attempts to compromise it would be revealed by a new hash. Smart contracts that save hash functions directly reduce data search times and provide unfiltered access to private information stored in the Interstellar System. The authors of this study (Salim et al., 2021) propose a homomorphic mechanism-based confidentiality technique to prevent unauthorised parties from accessing sensitive healthcare data. (Vizitiu et al., 2020) presented a fully homomorphic encryption solution for directly executing artificial neural computations on floating-point values with minimal computational overhead. This is accomplished by distributing computations to a large number of simulated terminals at the corner, where they remain hidden from any untrustworthy web servers. The key may be decrypted using either the homomorphic encryption technique or the Matrix Operation for Randomization. Data security and privacy might be compromised if an attacker used an optimization model to discover the encryption key with several key pairings.

Although the suggested method does not encrypt data in transit, sensitive information would still be transferred to a remote, encrypted Cloud service. Homomorphic encryption built on matrices (HEBM) was used by wireless sensor networks (WSNs) (Huang et al., 2017) to securely transfer electronic health records (EHRs) from WBANs to WPANs. Recent work by (Zhou et al., 2018) has reduced the bootstrap time from six to three, leading to better data security. (Dowlin et al., 2017) used Simple Encrypted Arithmetic Library (SEAL) to create a Homomorphic Encryption for crucial medical and genetic data, making it available to the public in bioinformatics and providing pr(A. Chatterjee & Sengupta, 2018) used FHE, encoding confidential material, and keeping it within server guaranteeing confidentiality. Due to the importance of secret data sharing in cryptography, a new homomorphic encryption approach has been presented (Zhang et al., 2018) for outsourcing this function.

Applications include e-mail relaying, data interchange, and access restrictions, and the leading multi-hop homomorphic identity-based proxy re-encryption solution is presented in (Li et al., 2017). Instead of using a query trapdoor approach, the server in (Wu et al., 2018) builds a downward encrypting access structure to speed up searches for unique terms. (Tsoutsos & Maniatakos, 2018) presents not only secrecy but also integrity guarantees for encrypted computations by using additive homomorphic encryption. Despite the increasing number of FHE algorithms discovered, none have proven practical due to the high degree of distortion they generate, which increases computational complexity (Acar et al., 2018). In contrast, ABE uses a kind of public-key encryption that allows several people to safely communicate information (Kocabas et al., 2016). (Attrapadung, 2011) suggested a KP-ABE strategy by integrating a non-monotonic access

control mechanism and a fixed cipher-text length, building on the results of many CP-ABE tests undertaken to secure e-health data (Oh et al., 2021).

An entirely secure Data Sharing Framework (DSF) that permits electronic encoding and external decoding was established in this research (Iao et al., 2019). Using an s-health setting as an example, the authors showed that DSF could be implemented in a cloud-assisted s-health system. In addition, (Ning et al., 2018) developed an audit trails -time leased ABE technique that gets rid of unnecessary decryption delay and provides unlimited access rights on mobile devices, thereby decreasing the cost of encryption or decryption. (Y. Yu et al., 2018) provide a small break-glass access management structure for the Internet of Things, and (Y. Yang et al., 2018) give a direct contact assured elimination approach for rollout using CP-ABE. If the characteristic combination satisfies the access control policy for the medical file, a health professional can decode and extract data in the vast majority of situations. Break-glass entry allows emergency medical staff or rescue workers immediate access to data by bypassing the medical file's access control mechanism. Since the present CP-ABE approach ignores the underlying hierarchical structure of the shared files, S. Working file directories (FH-CP-ABE) were designed by Wang et al. for use in cloud programs (S. Wang et al., 2016).

The approach employs embedded access structure encryption to save both time and space while protecting structured data. Zhong et al. (2021) present an effective ABE system that delegates partial encryption and decryption to edge endpoints and allows for attribute updates, enabling more dynamic control. Guan et al. (2021) proposed a modified CP-ABE technique with consistent ciphertext length and less processing required for encryption and decoding. The authors of (R. Cheng et al., 2021) suggest a modern CP-ABE system that makes use of cryptography (ECC), in which the bilinear pairing process is replaced with simple multiplications, and the bulk of the decryption tasks are delegated onto edge devices. It has been found that the method described by (Odelu et al., 2016) is insecure (Herranz, 2017). It was shown that the strategy may be countered with the support of a dissatisfied policyholder. This presumption is based on the fact that when any combination of user attribute sets fits the access policy criteria, such an attack is possible. In addition, a revised version of the strategy proposed by (Odelu et al., 2016) was provided by (Raj & Pais, 2020).

The suggested method uses ECC and a secret private key of constant size in conjunction with an AND gate access restriction. ECC can encrypt and decode data at a low cost. An AES-to-FHE transformation has been identified as a viable strategy for safeguarding medical records. ABE's evident advantages in cloud security have led to the belief that using it to gather and make available health data would be advantageous. Therefore, it is suggested that improving the current ABE-to-FHE modification approach, which always decrypts and re-encrypts data, might be useful for safeguarding patient information. Given the decentralized nature of the IoT environment, multi-authority ABE is necessary for implementing seamless access control; this may lighten the load on a central attribute authority and improve the system's overall performance. In the article "Safe and Streamlined User Access Control System for Data Consumption in the Internet of Things" (Banerjee et al., 2020), the authors described such a system. Because the ABE key size stored on the individual's chip card and the cypher-text length necessary for connection requests remain identical regardless of the number of characteristics, the three-factor access management system enables multi-authority ABE and is extremely flexible. The novel lattice-based CP-ABE system was created by (G. Wang et al., 2019) and has a three-to-one recording mechanism.

Taking cues from (Gorbunov et al., 2013), (Dong et al., 2020) designed a lattice-based ABE system that is indirectly removable and provides effective and protected user denial inside lattices. Although (Brakerski & Vaikuntanathan, 2020) presented a circuit access policy CP-ABE system, they did not address the issue of security, which remains an open concern. Imagine a situation in which a very large number of users send messages 1, 2,... are stored and encrypted on a remote server. The cloud platform's ciphertext must be handled by the function without sacrificing privacy in order to decrease processing and communication costs. If you have the ciphertext that processes, you may decode it to get (1,2,...). Lattice-based ABE algorithms, such as the ones discussed above, do not permit homomorphic operations on the ciphertext. There are two problems with using traditional CP-ABE in smart medicine as it is. The first is that private health information may be at risk since access rules are written in plaintext whereas smart medical files are encoded. Because the number of its public parameters rises proportionally with the size of the attribute universe, it often only takes a limited selection of attributes, which sets an unfavorable limitation on the usage of CP-ABE applications.

To deal with these problems, PASH (Y. Zhang et al., 2018) introduced a smart health access management platform that is privacy conscious. The most important factor is a partly constructed, large-universe CP-ABE. Given that the actual values for access policy attributes are hidden in the encoded SHRs of PASH, only their names were shown to the user. The CP ABE method presented in (Odelu et al., 2017) allows for a small number of encrypted messages and secret keys, which may be used on devices with limited storage space, regardless of the number of attributes. The scheme can only use AND gates at the moment, thus it has to be extended so that OR gates may be used in access controls as well. ECC MA-CPABE, which gives better strength, a shorter key length, and needs less computation load, was also suggested by (Sandhia & Raja, 2020), but it is not appropriate in a wide range of IoT applications where more expressive power is required. The problem of choosing which attributes to upload was handled, however, the technique we just described doesn't work with the idea of revoking uploaded attributes. An enhanced CP ABE technique with fixed ciphertext size was developed in this study for fast encryption and decryption (Guan et al., 2021). More recently, a novel approach that combines the flexibility and speed of attribute-based encryption with the efficiency of symmetric key encryption for carrying out secure information interactions across the various entities that make up this new IoT (Salvador et al., 2017) was developed to stop legitimate people from spilling content while also protecting the privacy of data owners.

However, this approach has to be supported by incorporating authentication methods and doing numerous testing on actual devices. Researchers (Han et al., 2018) proposed an ABE technique that conceals both user and access policy attributes out of concern that user attribute security would be compromised during key structure and encoding stages due to public access regulations. For the sequential system of secret sharing, (K. Yang et al., 2014) created a dynamic policy updating approach. In ECC, a KP-ABE based on bilinear pairing sets was utilised to implement the approach. With the help of an update key, the proxy may transform encrypted messages from the old access structure into the new one. The sensors' data was collected by a centralized server, which then encoded it using ABE so that it could be decoded by a user with the right set of characteristics. A plan for managing high levels of attribute authority was developed in 2011 (Ruj et al., 2011). Using cryptanalysis, (S. Chatterjee & Roy, 2014) determined that the methods described in (Ruj et al., 2011; S. Yu et al., 2009) are vulnerable to insider threats since they provide access to sensitive data to people with less authority.

Based on the KP-ABE technique, (S. Chatterjee & Das, 2014) proposes a streamlined way of user access control for WSNs that is resistant to insider attacks. A safeguard for the WBAN was proposed by (Tian et al., 2014), using the KPABE and a user repudiation mechanism based on bilinear pairing operations as its foundations. In 2017, (Ma et al.) published a new version of the KPABE, termed the KPABE employing a timeframe. The receiver, using their method, may decode the ciphertext in the allotted time. The potential use of this technique in cloud timeframe settings was also highlighted. Another variant of the KPABE is presented by Ge et al. (2018), which uses backdoor reencryption. The method is shown by means of a flexible strategy that accounts for both the CCA and the monotonic access policy. After analyzing a single application case, (J. Li et al., 2018) proposed a KPABE method that would be robust against continual auxiliary input loss. All of the aforementioned KPABE structures rely on a bilinear pairing mechanism.

A small-scale KPABE scheme using ECC for the Internet of Things (IoT) without the use of bilinear pairing was presented by (Yao et al., 2014), but the method has a number of limitations, such as no key update mechanism and restricted scalability. Due to its small size and equivalent security resilience to other public key techniques, ECC has become one of the most well-known cryptographic algorithms (Sowjanya et al., 2020; Xiao et al., 2021). Due to the limitations of IoT nodes in terms of persistence, storage, physical resources, and computing power, there is growing support for the usage of ECC with hardware or software implementations (Cano & Caavate sanchez, 2020). Several ECC-based authentication methods have been proposed, and some of them have been proved to be effective (lightweight) for smart technology (Hong & Sun, 2016; Kaur et al., 2016). Using a random database structure, (Hong & Sun, 2016) suggested a more effective key-protected KPABE approach that does not need pairing but is still secure under the computational Deffie-Hellman (CDH) hypothesis. Lightweight key-policy ABE based on elliptic-curve-cryptography with a key refresh/update technique and no bilinear pairing was proposed by the authors (Sowjanya et al., 2020). Key distribution, which includes direct attribute/user termination, is also the responsibility of the authority. Since it is not reliant on a random oracle, this system is safe thanks to the EC decisional Diffie-Hellman (ECDDH) hypothesis in an attribute-based selective-set framework.

A physical unclonable function (PUF) and ECC technology-based access control and verification system is recommended for use in telecare medical information systems (TMIS) (Xiao et al., 2021). However, hardware deterioration and instability are real issues with the current crop of PUF systems. An innovative security approach is given in this paper (Vincent & Folorunso, 2020) that combines a cyclotomic elliptic curve with elliptic curve embedded cryptography. The presented method employs a cyclotomic function and the Weierstrass version inside an elliptic curve to construct a hash function that may be utilized to produce a structure from a curve coordinate and a polynomial variable. The research might be improved upon even more by using elliptic curves of other types than the Weierstrass reduced variant that was employed. Recently, a novel small-scale flexible cryptography solution was developed (Abdulraheem & Balogun, 2021) to improve the safety of HPC for medical data.

The proposed solution not only increased security but also significantly sped up the process of encrypting data. In 2021 (Y. Liu et al., 2021) a compact ciphertext attribute-based completely homomorphic approach was created based on the LWE problem on lattices. The researchers avoided the reliance of the cipher-text length on the parameters of this system by specifying the characteristics of each system and making use of the distinctive structural array of MP12. This means that the cipher-text length will not grow with the total number of parameters in the system. By using function 1 in the homomorphic methods, they completely re-randomize every standard error inside that most recent cipher-text, allowing for a highly accurate and straightforward error breakdown based on sub-Gaussianity. While the "AND" access policy improves space and time efficiency, it does not allow for any other access rules to be implemented.

III. THEORY

The suggested area of study was derived from an analysis of the existing literature in the field. The method presented to put this research into practise is a mashup of the ABE and FHE security system algorithms, capitalising on the strengths of each. Additional encryption of healthcare data using the ECC algorithm would be used to provide a more foolproof security system and more effective method for Smart healthcare. ABE is a kind of public-key encryption that permits secure data transmission between a large number of parties. Attribute threshold gates (k, n) may be used in combination with disjunctions and conjunctions to define an access policy P.

This opens the door for a cardiologist, nurse, or EMT to enter the building. When decoded, FHE ciphertexts may be subjected to an arbitrary number of multiplications and sums, with the results being identical to those of operations done on plain data. Because of this, ciphertexts may be used in cloud hosting for legitimate reasons without the need for decoding. Example 1: Elliptic Curve Cryptography (ECC) is a strong and fast-processing encryption option for use in smart healthcare systems. Due to the storage, durability, computational power, and hardware limitations of smart nodes, there is a growing body of knowledge about the usage of ECC with hardware or software solutions (Cano & Caavate-sanchez, 2020).

3.1 Preliminaries

A. Attribute and access structures:

The access structures and attribute described in (Banerjee et al., 2020) is further extended here. The galaxy of attributes is defined as having n attribute parameters and n attribute controllers. An n-bit string $a_1,a_2, \ldots a_n$, defines access structure $A \subseteq U$, while $a_1=1$ if $A_1 \in A$ otherwise 0 if $A_1 \notin A$. The total of all access structures $A_k = a_{1k}\, a_{2k} \ldots a_{nk}$ from attribute controller C_k, when $k \in [1,n]$, makes up a user access structure A. $A_k$defines the Every participant can only access a gadget having access structure $\mathbb{P} \subseteq U$ in which $\mathbb{P} = b_1,b_2 \ldots b_n$ and only if $\mathbb{P} \subseteq A$ if they have the approved access structure listed in the AND gate access policy. Likewise, the requirement $(a_1 - b_1) \geq 0$ must be satisfied for A to satisfy $\mathbb{P}$, $\forall i \in [1,n]$.

B. Attribute Encryption Algorithm:

KP-ABE method provided by (Odelu et al., 2017)with the CP-ABE method presented is combined to create a fundamental cipher text policy attribute-based encryption (CP-ABE) method, which includes four phases (Banerjee et al., 2020).

1. Setup: A master secret and public key pair are created using the secret key as well as a universe of attributes U ={A_1,A_2,…,A_n} parameters (MSK,MPK).

2. Encrypt: It makes use of an encryption operation to create a ciphertext C from inputs with access policy $\mathbb{P}$, an unencrypted message Msg, with P,K_u.

3. KeyGen: It is given an attribute setA, master secret key MSK, as well as master public key "MPK" in order to get an output known as decoding key D of A.

4. Decrypt: To return the real plaintext message Msg or ⊥ (null) as an output, it uses a decoding mechanism which will be provided along cipher-text C constructed using $\mathbb{P}$, Q similar to MSG and P as parameters.

C. Fully Homomorphic Encryption Algorithm:

Key Generation, Encrypt, Decrypt, and Evaluation are the four algorithms that make up Fully Homomorphic Encryption (Y. Liu et al., 2021).

1. KeyGen(1^n): When the security parameter 1 is entered, public key pk and secret key sk are produced by this algorithm.

2. Encrypt (pk,μ): an incoming message μ depending on public key pk. A ciphertext c is produced by the scheme.

3. Decrypt (sk,c) → μ: It outputs the message μ built on secret key sk and cipher-text c inputs.

4. Eval(pk,c,c,…,c,f): takes as input public key pk, list of cipher-text,c,…,c, a functional f ∈ F.It produces a new cipher-text cin which Decrypt (sk,c) = f(μ,μ,…,μ).

5. Decrypt (sk,c) = f(μ_1, μ_2,…,μ_n) on output new ciphertext c given parameter public key pk, cipher-text set c_1,c_2,…,c_n, as well as functional f ∈ F.

Simple calculations may be performed on encrypted data using Homomorphic Encryption methods. Due to the fact that the calculations are done on encrypted data, confidentiality is maintained. The encrypted sum or encrypted product of two encrypted communications is usually something a third party can figure out.

This property of homomorphic cryptosystems makes them applicable to many privacy-preserving protocols for safe multiparty computing. The public key of the encryption system, together with two ciphertexts, are fed into an additive homomorphic algorithm, and the resulting ciphertexts are deciphered.

$$E_{P_k}(m_1) +_{P_k} E_{P_k}(m_2) = E_{P_k}(m_1 + m_2);$$

where + P_k is the homomorphic addition function, E_{P_k} is the public-key encryption function m_1 *and* $m_2$are elements in the domain of data. We refer additively homomorphic encryption scheme based on ECC in this paper.

D. Elliptic Curve Cryptography Algorithm:

Assuming an elliptic curve E(Fp) over a finite prime field Participants A and B in a conversation agree on a point E(Fp) that is freely available in the communication channel. Participant A selects a probable positive integer k_A, computes k_A, Q, and communicates it to party B in secret. In addition, participant B chooses a probable positive integer k_B, computes k_B, Q, and transmits it to member A. P = $k_A k_B$. Q is the shared secret. By estimating the obtained k_B, Q point with secret private key k_A, participant A determines. By calculating the received point k_A, Q with secret private key k_B, participant B obtains P (Elliptic Curve Cryptography: ECDH and ECDSA - Andrea Corbellini, n.d.).

The four standard components of the suggested smart health security approach: S-Health Cloud (SHC), S-Health Authority (SHA), Data User (DU), and Data Owner (DO).

- SHC has a large amount of storage and keeps SHRs that have been encrypted as well as their DO-partially concealed access policies.
- SHA is in control of user authentication and system initialization. It is reliable and gives DUs fine-grained access permissions according to their attributes.
- A DU is SHR holder who requires access to the protected SHRs in SHC, such as a physician or a researcher in medicine. Each DU has a defined collection of features and a secret key associated with that particular collection of characteristics.A DU could pass attribute verification thus decode an encoded SHR if his group of attributes matches the concealed access policy associated with it.
- DO is the owner and manager of SHRs, and it contracts with SHC to provide ciphertexts for healthcare. A hospital that handles SHRs on behalf of its patients may be a DO. Local computers, smart devices, and a WBAN made up of several implantable wearables and a control system are all components of DO. The WBAN control system or the local server encrypts SHRs coming from sensors or other smart devices before sending them to SHC for sharing with DU. For encoded SHRs, DO is in charge of developing and monitoring access controls.

- ECC is a public key cryptography approach based on the algebraic structure of elliptic curves over finite fields [10,11]. There are two types of finite fields where the elliptic curves are defined: prime fields Fp, where p is a large prime number, and binary fields F_2^m. In this work, we are interested in the use of elliptic curves over prime fields E (Fp). A nonsuper singular elliptic curve E over Fp is defined as the solution of $(x, y) \in (Fp \times Fp)$ to the cubic equation:

$$y^2 = x^3 + ax + b \bmod p$$

where $a, b \in Fp$, such that $4a^3 + 27b^2 \neq 0 \pmod p$ to- gether with a special point ∞ called the point at infinity, The group of points forms an abelian group with addition operation so that the addition of any two points results in another point on the same curve. ECC-based cryptographic protocol security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP can be defined as the problem of finding the scalar k such that Q = kP given Q and P (generator point).

Table 1: Inputs and Outputs of various phases

Work Phase	Input	Output
Key Generation phase	A,MSK,MPK	$k_u = (u_1,u_2)$
Setup phase	U,p	MSL,MPK
Encrypt Phase	P,MPK, M	C=[P,R_m,K_{1m},K_{2m},$C_{\sigma m}$,C_m}
Decrypt phase	C, k_u, MPK,A	T or message M

Performance Evaluation:

The following compares the effectiveness of ABE FHE-ECC algorithm to that of three other current schemes: (Sowjanya et al., 2020), (Y. Liu et al., 2021) and (Zhong et al., 2021). The comparison would be based on the schemes' functionality and computing costs. Computability, a large number of attributes, storage capacity, and an ECC-based function are among the features. Each scheme's encryption and decryption times are also compared. Functions compare all of the schemes based on significant characteristics such as computability, a large number of attributes, storage capacity, and ECC-based action. The results show that all of the schemes allow big attributes to be utilized as access policies. Only the ABE-FHE-ECC scheme and (Y. Liu et al., 2021) scheme allow full computation on encrypted data. The ECC-based ABE-FHE-ECC and (Sowjanya et al., 2020) methods are totally secure against an external attack while also reducing storage capacity. According to the aforementioned comparisons, only ABE-FHE-ECC and (Sowjanya et al., 2020) schemes could handle huge attribute amounts and low memory capacity at the same time, whereas the latter cannot allow encrypted data calculation.

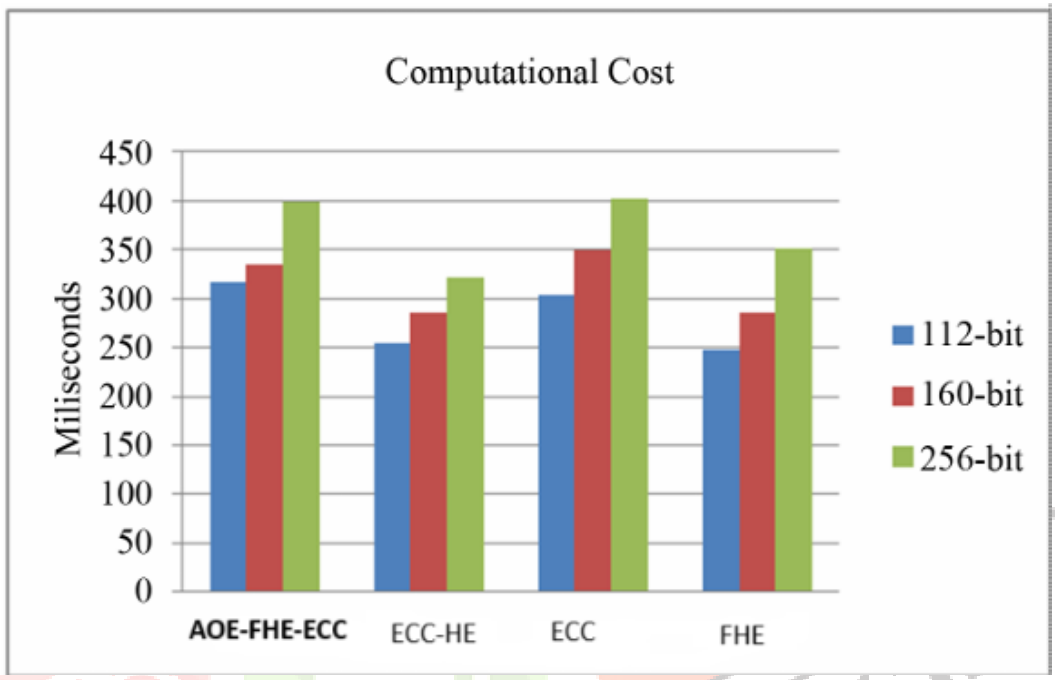

Fig.1. Computational cost comparison

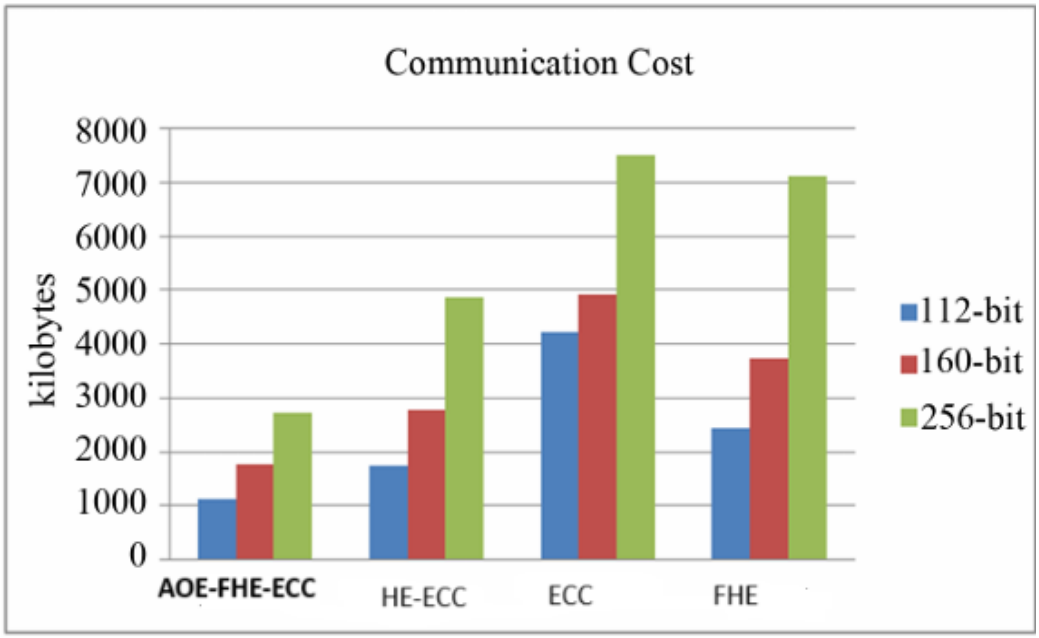

Fig.2. Communication cost comparison

Computational Cost and Communication costs:

The majority of the computing cost comes from the ciphertext storage size, encryption, and decryption. With regard to computing costs, compare the ABE-FHE-ECC system to various existing schemes. Figure 1 & 2 shows the comparison of the proposed algorithm with the existing algorithms. When compared to previous schemes, the figure shows that the proposed method uses a consistent ciphertext size for the specified attributes, which runs from 4 to 128. This is due to the fact that content is encrypted utilizing ECC prior to being transmitted to the web. The link of both attributes is chosen by the user as well as the time needed to encode all data collected. The graph shows how much quicker the proposed method encodes data as compared to conventional systems. Because the decryption technique just uses a minimum pairing operation. It is worth noting that a short ciphertext can save not just computing costs but also the time it takes to perform encryption, decryption, and homomorphic functions.

IV. CONCLUSION AND FUTURE SCOPE

This is possible because of the small ciphertext. depicts the relationship between attributes and data decryption in the same way. In comparison with existing systems, this suggested model's decryption time is extremely fast An efficient ABE-FHE system becomes more crucial as Internet-based technologies and Internet of Things gadgets become more prevalent across smart healthcare. A lightweight hybridized ABE FHE algorithm based on ECC is proposed in this approach to reduce computing costs in resource-constrained devices. The evidence on security proves this method to be secured under the DBDH assumption. Performance research shows that users and data owners always bear the computing burden of this encryption approach. As a result, it solves the issue of a device with limited resources being unable to do a large amount of computation. It also reveals that our encryption method performs better than the other three.

The findings of this research demonstrate that using this technique to secure smart healthcare data would significantly increase the security of data users as well as patients in the health industry. Research for further study Adding attribute revocation and policy updating to the security scheme can be explored for further research in order to enhance and increase its efficiency.

References

[1]. AbdulRaheem, M., Balogun, G. B., Abiodun, M. K., Taofeek-Ibrahim, F. A., Tomori, A. R., Oladipo, I. D., & Awotunde, J. B. (2021). An enhanced lightweight speck system for cloud-based smart healthcare. In Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4 (pp. 363-376). Springer International Publishing.

[2]. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), 1–35. https://doi.org/10.1145/3214303

[3]. Banerjee, S., Roy, S., Odelu, V., Kumar, A., Chattopadhyay, S., Rodrigues, J. J. P. C., Park, Y., & Abe, M. (2020). Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment. Journal of Information Security and Applications, 53. https://doi.org/10.1016/j.jisa.2020.102503

[4]. Bao, S. Di, Chen, M., & Yang, G. Z. (2017). A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications. IEEE Journal of Biomedical and Health Informatics, 21(6), 1487–1494. https://doi.org/10.1109/JBHI.2017.2679979

[5]. Brakerski, Z., & Vaikuntanathan, V. (2020). Lattice Inspired Broadcast Encryption and Succinct. IACR Cryptology, 28, 1–20.

[6]. Cano, M., & Cañavate-sanchez, A. (2020). Preserving Data Privacy in the Internet of Medical Things Using Dual Signature ECDSA. Hindawi Security Communication Networks, 2020.

[7]. Chatterjee, A., & Sengupta, I. (2018). Translating Algorithms to Handle Fully Homomorphic Encrypted Data on the Cloud. IEEE Transactions on Cloud Computing, 6(1), 287–300. https://doi.org/10.1109/TCC.2015.2481416

[8]. Chatterjee, S., & Das, A. K. (2014). An effective ECC-based user access control scheme with attribute-based encryption for wireless. https://doi.org/10.1002/sec

[9]. Chatterjee, S., & Roy, S. (2014). Cryptanalysis and Enhancement of A Distributed Fine-grained Access Control in Wireless Sensor Networks. 2074–2083.

[10]. Cheng, R., Wu, K., Su, Y., Li, W., Cui, W., & Tong, J. (2021). An efficient ECC-based cp-ABE scheme for power IOT. Processes, 9(7), 1 16. https://doi.org/10.3390/pr9071176

[11]. Dong, X., Zhang, Y., Wang, B., & Chen, J. (2020). Server-Aided Revocable Attribute-Based Encryption from Lattices. 2020.

[12]. Dowlin, N., Gilad-Bachrach, R., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2017). Manual for Using Homomorphic Encryption for Bioinformatics. Proceedings of the IEEE, 1-16; https://doi.org/10.1109/jproc.2016.2622218

[13]. Elliptic Curve Cryptography: ECDH and ECDSA - Andrea Corbellini. (n.d.). Retrieved January 2, 2022, from https://andrea.corbellini.name/2015/05/30/el liptic-curve-cryptography-ecdh-and-ecdsa/

[14]. Ge, C., Susilo, W., Wang, J., Shi, Y., & Fang, L. (2018). A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for Dropbox data sharing system. Designs, Codes and Cryptography. https://doi.org/10.1007/s10623-018-0462-9

[15]. Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. Ruan Jian Xue Bao/Journal of Software, 26(10), 2696 2719. https://doi.org/10.13328/j.cnki.jos.004808

[16]. Gentry, C., Halevi, S., & Smart, N. P. (2012). Homomorphic evaluation of the AES circuit. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7417 LNCS, 850–867. https://doi.org/10.1007/978-3-642-32009 5_49

[17]. Gorbunov, S., Vaikuntanathan, V., & Wee, H. (2013). Attribute-Based Encryption for Circuits. Guan, Z., Yang, W., Zhu, L., Wu, L., & Wang, R. (2021). Achieving adaptively secure data access control with privacy protection for lightweight IoT devices. Science China Information Sciences, 64(6), 1–14. https://doi.org/10.1007/s11432-020-2957-5

[18]. Han, Q., Zhang, Y., & Li, H. (2018). Efficient and Robust Attribute-based Encryption Supporting Access Policy Hiding in Internet of Things. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2018.01.019

[19]. Herranz, J. (2017). Attribute-based encryption implies identity-based encryption. IET Information Security, 11(6), 332–337. https://doi.org/10.1049/iet-ifs.2016.0490

[20]. Hong, H., & Sun, Z. (2016). High efficient key insulated attribute based encryption scheme without bilinear SpringerPlus, pairing 5(1), operations. 1–12. https://doi.org/10.1186/s40064-016-1765-9

[21]. Kara, M., Laouid, A., Yagoub, M. A., Euler, R., Medileh, S., Hammoudeh, M., Eleyan, A., & Bounceur, A. (2021). A fully homomorphic encryption based on magic number fragmentation and El-Gamal encryption: Smart healthcare use case. Expert Systems, February, 1–14. https://doi.org/10.1111/exsy.12767

[22]. Kaur, K., Kumar, N., Singh, M., & Obaidat, M. S. (2016). Lightweight authentication protocol for RFID-enabled systems based on ECC. 2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings, Id. https://doi.org/10.1109/GLOCOM.2016.784 1955

[23]. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2020). Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73 80. https://doi.org/10.1109/TSMC.2019.290378 5

[24]. Khedr, A., & Gulak, G. (2018). SecureMed: Secure Medical Computation Accelerated Using GPU Homomorphic Encryption Scheme. IEEE Journal of Biomedical and Health Informatics, 22(2), 597–606. https://doi.org/10.1109/JBHI.2017.2657458

[25]. Kocabas, O., Soyata, T., & Aktas, M. K. (2016). Emerging Security Mechanisms for Medical Cyber Physical Systems. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 13(3), 401–416. https://doi.org/10.1109/TCBB.2016.252093 3

[26]. Li, J., Yu, Q., Zhang, Y., & Shen, J. (2018). Key Policy Attribute-Based Encryption against Continual Auxiliary Information Input Leakage. Sciences. https://doi.org/10.1016/j.ins.2018.07.077

[27]. Li, Z., Ma, C., & Wang, Di. (2017). Towards Multi Hop Homomorphic Identity-Based Proxy Re-Encryption via Branching Program. IEEE Access, 5, 16214–16228. https://doi.org/10.1109/ACCESS.2017.2740 720

[28]. Lin, H., Garg, S., Hu, J., Wang, X., Jalil Piran, M., & Hossain, M. S. (2021). Privacy-Enhanced Data Fusion for COVID-19 Applications in Intelligent Internet of Medical Things. IEEE Internet of Things Journal, 8(21), 1568315693. https://doi.org/10.1109/JIOT.2020.3033129

[29]. Liu, Y., Pan, Y., Gu, L., Zhang, Y., & An, D. (2021). Attribute-Based Fully Homomorphic Encryption Scheme from Lattices with Short Ciphertext. Mathematical Problems in Engineering, 2021. https://doi.org/10.1155/2021/6656764

[30]. Ma, S., Deng, R. H., & Ding, X. (2017). Adaptable key-policy attribute-based encryption with time

interval Adaptable key-policy attribute based encryption with time. Soft Computing, 6191–6200. https://doi.org/10.1007/s00500 016-2177-z

[31]. Magons, K. (2016). Applications and benefits of elliptic curve cryptography. Workshop Proceedings, 1548, 32–42. CEUR Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. IEEE Internet of Things Journal, 8(14), 1174311757. https://doi.org/10.1109/JIOT.2021.3058953

[32]. Ning, J., Cao, Z., Dong, X., Liang, K., Ma, H., & Wei, L. (2018). Auditable σ-Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing. IEEE Transactions on Information Forensics and Security, 13(1), 94–105. https://doi.org/10.1109/TIFS.2017.2738601

[33]. Odelu, V., Das, A. K., & Goswami, A. (2016). An Efficient CP-ABE with Constant Size Secret Keys using ECC for Lightweight Devices. IEEE Transactions Electronics, 62(1), 1–15.