A HYBRIDIZED ENCRYPTION SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY FOR SECURING DATA IN SMART HEALTHCARE

[1]Babatunde A. O., [2]Dauda S. O., [3]RAJI A. K., [4]Oladipo I. D, [5]Ogunwobi Z. O., [6]Taofeek-Ibrahim F. A, [7]Balogun G. B.

[1,2,4,7]Department of Computer Science, University of Ilorin, Ilorin, Nigeria
[3]Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin
[5]Department of Mathematical Sciences, Olabisi Onabanjo University, Ago-iwoye
[6]Department of Computer Science, Federal Polytechnic Offa
[1]babatunde.ao@unilorin.edu,ng ; [2]olawoyinolayinka20@gmail.com, [3]kamalayour2004@gmail.com, [4]odidowu@unilorin.edu.ng, [5]ogunwobi.zachaeus@oouagoiwoye.edu.ng. [6]fatty_fatty2@yahoo.com.au, [7]balogun.gb@unilorin.edu.ng

ABSTRACT

Recent developments in smart healthcare have brought us a great deal of convenience. Connecting common objects to the Internet is made possible by the Internet of Things (IoT). These connected gadgets have sensors and actuators for data collection and transfer. However, if users' private health information is compromised or exposed, it will seriously harm their privacy and may endanger their lives. In order to encrypt data and establish perfectly alright access control for such sensitive information, attribute-based encryption (ABE) has typically been used. Traditional ABE, however, has a high processing overhead. As a result, an effective security system algorithm based on ABE and Fully Homomorphic Encryption (FHE) is developed to protect health-related data. ABE is a workable option for one-to-many communication and perfectly alright access management of encrypting data in a cloud environment. Without needing to decode the encrypted data, cloud servers can use the FHE algorithm to take valid actions on it. Because of its potential to provide excellent security with a tiny key size, elliptic curve cryptography (ECC) algorithm is also used. As a result, when compared to related existing methods in the literature, the suggested hybridized algorithm (ABE-FHE-ECC) has reduced computation and storage overheads. A comprehensive safety evidence clearly shows that the suggested method is protected by the Decisional Bilinear Diffie-Hellman postulate. The experimental results demonstrate that this system is more effective for devices with limited resources than the conventional ABE when the system's performance is assessed by utilizing standard model.

Keywords: *Ant Internet of Things, Privacy, Encrypt Data, Homomorphic Encryption, Cryptography, Hybridized algorithm*

INTRODUCTION

Background to the Study

The worldwide architecture of the information system known as Internet of Things (IoT) had also evolved to enable communication between smart phones, sensing devices, RFID tags, and smart buildings. To gather and exchange data, these technological gadgets communicate via wired or wireless networks. With the advancement of the IoT, practically anything may be accessed from anywhere, at any time, and deliver almost any activity. The IoT is generally composed of tiny parts that are connected to one another to facilitate cooperative calculating situations. Constraints in the IoT include energy cost, connectivity, and processing resources. Healthcare is one of the quickest fields that has adopted IoT the fastest due to the ability of medical instruments to incorporate

IoT capabilities that increase service quality and efficiency (Khari et al., 2020; Pulkkis et al., 2017; Y. Yang et al., 2017).

S-health (Smart health) has been the situational improvement of telehealth in smart metropolises, enabling precise and efficient disease and accident avoidance. In fact, the Internet of Things has frequently been used as a foundational technology in smart cities to link readily accessible healthcare resources services and deliver dependable and effective s-health care to both the elderly and patients (Y. Zhang et al., 2018). Around the world, healthcare administration recently changed from a disease-centered to a patient-centered perspective (SA, 2018). Putting in place an Electronic Health Record (EHR) system is able to enhance patient consistency and the healthcare system, increase safety and level of medical care, and save time and money.It has infiltrated the medical domain due to the ease with which it manages and shares health data. The s-health (Y. Yang et al., 2017) system might connect a range of health-care devices, enabling continuous physiological observation, chronic disease assessment, and therapy training. Until then, s-health has the ability to improve healthcare quality while cutting medical expenses. In the upcoming years, it is anticipated that cloud-based smart health will offer enough medical treatment due to the quick rise of Cloud technology innovations. Though s-health is still in its infancy, there are still a number of issues that need to be solved before it can be used in real-world settings. Data breaches in the s-health sector have become a major concern for individuals (Y. Zhang et al., 2018), and it is still a challenge to protect IoT users' extremely sensitive personal healthcare information' security and privacy without compromising the utility of the data (Y. Yang et al., 2017). Only authorized trained healthcare practitioners typically have access to a patient's s-health records (SHRs), which include measurements like pulse rate and blood pressure. On the other hand, typical access control systems either compromise data security or only provide coarse-grained access controls.

This reasoning suggests that sharing key techniques, which have historically been used to secure end-to-end data secrecy, are insufficient in such new circumstances. Accordingly, a novel security feature called Attribute Based Encryption (ABE) (Salvador et al., 2017) enables encrypting data users' self-access restrictions, which describe the requirements a subject must meet to completely decode a data; thus, ABE (Y. Zhang et al., 2018) is seen as a potential method for achieving perfectly alright access control. ABE schemes come in 2 varieties: Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE). According to the stated access control mechanism in CP-ABE schemes, personal health records (PHRs) are secured, and the private keys of user data are associated with a variety of attributes. Data users can access these encrypted PHRs only and only if their characteristics line up with the access rules. Contrary to conventional encryption techniques that encrypt data using paired keys or produce several ciphertexts for numerous users, CP-ABE systems does not have a significant key handling cost or duplicated ciphertexts. In the KP-ABE technique, a participant's decryption key is connected to a tree access structure and a ciphertext is connected to a class of parameters. The parameters of the ciphertext must fulfill the tree access structure in order for user to be able to decode it (Iao et al., 2019; Tu et al., 2021). A personal key is generated for each subject by the ABE algorithm using a combination of private and public data (e.g. its role). If a recipient's characteristics meet the access criteria within that access policy, only then will the user's own key be capable of effectively decode given data (Salvador et al., 2017). However, the present ABE algorithms are not suited for application in s-health since they need a high number of computations. Micro-electromechanical systems and tiny smart devices are continually constrained by the amount of energy they can use and their processing power. For an Internet of Things system with multiple owners and users, it's essential to have a small access management system (Y. Yang et al., 2017). Fully homomorphic encryption (FHE) is among the primary strategies for addressing this issue. When encrypted data is decrypted, FHE enables an unlimited amount of arithmetic operations be performed on it with the same results as operations on plain data. To put it another way, people in charge of performing computations on encrypted data have no information from the data or the results of such computations (Wang et al., 2017).

The development of a homomorphic encryption technique was initially looked at by (Rivest et al., 1978) in that year. Researchers made multiple attempts to develop homomorphic systems with numerous operations, and this idea is the outcome of those efforts. Homomorphic encryption is a group of encrypting techniques which are applicable to various computations over encrypted data, according to (Acar et al., 2018; Sen, 2013). Partially homomorphic, somewhat homomorphic, leveled entirely homomorphic, and totally homomorphic encryption are some of the most frequent types of homomorphic encryption (Acar et al., 2018; Gentry, 2009). Fully homomorphic encryption (FHE) allows an unlimited number of tasks to be carried out simultaneously. The most essential idea in homomorphic encryption is that the FHE systems may perform an endless amount of homomorphic operations for any function (Acar et al., 2018; Armknecht et al., 2015; Gentry, 2009). To protect the privacy and confidentiality of individuals, IoT systems must meet stricter security and reliability requirements than the majority of other IoT systems (Pulkkis et al., 2017)

Problem Statement

With the development of biosensor and mobile computing technologies, the amount of out-patient health data that end users can easily manage will increase significantly (Bao et al., 2017). Concerns about data privacy and protection are indeed increasingly prevalent in s-health (Y. Zhang et al., 2018), and it is still unclear on what to do to protect extremely sensitive personal health data in IoT without sacrificing data usefulness (Y. Yang et al., 2017). A sophisticated cryptographic technique will be needed to protect the confidentiality of the patient's records throughout transfer from sensing devices towards the web and via the web to clinicians' smart phones.

Aim and Objectives

In order to protect data within Smart Healthcare, this project aims to create a lightweight hybridized ABE-FHE system employing elliptic curve cryptography.

The specific objectives are to:

i. design and implement a lightweight hybridized ABE-FHE technique to secure data in Smart Healthcare and
ii. evaluate the system using Decisional Bilinear Diffie–Hellman (DBDH) presumption.

Significance of the Study

This study covers ABE and FHE approaches, which encompass all of the elements needed to secure smart healthcare data in this proposed research work. These approaches were further used with ECC so as to reduce the size of the output file. Computation on encrypted data, user data security and privacy, one-to-many interaction, and good access control are all possible with these features.

LITERATURE REVIEW

Each of the 5 Vs (Value, Variety, Velocity, Veracity, and Volume) is important to consider in healthcare since a wide range of data is collected at frequent basis and must be retained for numerous systems, varying from patient name, birthdate, and species to vital sign numbers. Data collected on daily basis would generate high velocity, resulting in rapid increase in total data volume. A digital memory system supporting critical medical care was built in recent study (Boyi et al., 2014) that evaluated the variety and quantity of health records. It aims to arrange diverse biological records during an emergency and have this readily available to the required medical professionals.

There has been some research on building security techniques which are appropriate for medical system (Baker et al., 2017). In (Thilakanathan et al., 2016), a complete access control method called "SafeProtect" is proposed, emphasizing patient ownership over their data.(Pacheco et al., 2016) describes a secure cloud technique for "enhanced lifestyles," that frequently include both wearables used by patient and intelligent home technologies, for the goal of supporting elderly or disabled people in living independently.

FHE (Wang et al., 2017) enables unrestricted multiplications and adds on encrypted data with results that are identical to those of operations on plain data when decrypted. Due to this, cloud infrastructure can operate legally on encrypted data without first needing to decode anything (Y. Liu et al., 2021). The development of asymmetric encryption in 1978 marked the beginning of homomorphic technology, and the concept of homomorphic encryption was originally raised by (Rivest et al., 1978). RSA is a partial homomorphic technique that only looks at multiplicative operations. The PHE systems only ensure addition or multiplication, never both. After that, several homomorphic encryption methods appeared(Kara et al., 2021).

Researchers have recently expressed concern about the FHE issue because of the increase of records being obtained as well as shortage of adequate capacities (in terms of computation or storage). FHE was proposed for the first time by (Gentry, 2009). To control the rise of noise and test the accuracy of decrypting, he devised a "bootstrapping" approach, and then he incorporated homomorphic multiplication and sum of encrypted data in this system. Though, the "boot-strapping" must first encrypt the private key before setting it as a public parameter.Following 2009, many approaches were used to improve the scheme, including the Fully Homomorphic Encryption based on BGV, GSW, Integer and Multi-key Fully Homomorphic Encryption Schemes(Yousuf et al., 2021). A straightforward FHE method built on the approximate greatest common divisions problem (A-GCD) was proposed by Van Dijk et al. in (van Dijk et al., 2010). Compared to (Gentry, 2009) approach, the suggested strategy is simpler conceptually. Instead of relying solely on perfect lattices atop polynomials band, the bootstrappable security measure that is advised uses arithmetic above numbers.

This simplicity, nevertheless, comes at the expense of a public key length that is O (γ^{10}) which is incredibly long. The Advanced Encryption Standard (AES) to FHE conversion approach suggested by (Gentry et al., 2012) enables the transformation to be carried out recursively instead of decrypting the data. FHE was compared to both the traditional AES and the recently developed ABE in (Kocabas et al., 2016), and it was found that employing AES in data collection then converting into FHE utilizing Advanced Encryption Standard-to-

Fully homomorphic encryption (FHE) transformation mechanism could result in a good solution. FHE was explored by (Khedr & Gulak, 2018) as a strategy for safeguarding data integrity, but it was discovered that FHE requires large computing capacity to likely succeed. A threshold

FHE built on learning with errors (LWE) assumption was described by Boneh et al. in (Boneh et al., 2018). The proposed TFHE is used to create a universal thresholdizer that addresses the problem of single-round threshold inscriptions of lattices. Additionally, threshold characteristics is then incorporated to a variety of platforms, such as authentication systems, CCA-public-key encryption (PKE) secured processes, and more (Kara et al., 2021).

A concept for federated learning verification-based patient privacy protection was presented by (W. Cheng et al., 2020). To maintain the security of medical records because data training occurs both locally and centrally, the system blends homomorphic encryption, cryptography, and distributed learning. Data collected locally and uploaded to the central server by every client, or device is used to build the algorithm. In addition to opportunity strategy that encourages users to share content with the health system, (H. Lin et al., 2021) introduced a stronger security clustering method for data encryption. Many mobile edge computing (MEC) application traffic supports COVID-19 operations, storing, processing, and analyzing data, and the method merges mobile edge computing as well as the IoT. The network edge handles entire data analysis instead of using facilities from the Central cloud. A distributed system with data sharing and dispatching capabilities was presented by (Nguyen et al., 2021); data computation gets carried out on MEC providing faster speeds and confidentiality protection.

The distinctive feature of this design is the use of smart contracts for data transmission authentication and tracking. Contracts that confirm the legitimacy of the participant remove the need for a centralized system / party to approve an access request permission to publish content. Since data is kept in chunks, integrity of data remains maintained, so any tampering would be visible in updated hashing. Direct hash function storing in smart contracts decreases data lookup time and allows direct access to sensitive data in the Interstellar System Files. In this article (Salim et al., 2021), they suggested a confidentiality strategy that uses a homomorphic mechanism to prevent intruders in obtaining clinical original data. In order to keep untrustworthy web servers from knowing about the activities conducted with encrypted patient data, secret sharing distributes computations to a large number of simulated terminals at the corner and conceals the arithmetic operations.(Vizitiu et al., 2020) presented a completely homomorphic encryption solution for directly executing artificial neural computations on floating-point values with the least amount of computing overhead. Both the homomorphic encryption scheme and Matrix Operation for Randomization can be used to decrypt the key. An attacker could employ an optimization model to locate the encryption key with lot of key couples, risking the confidentiality and integrity of data. The proposed technique does not encrypt data while it is being delivered, but actual data would still be sent to an external, secure Cloud platform for security reasons. (Huang et al., 2017) used wireless sensor networks (WSNs) to transmit e-health records via WBANs to WPANs using homomorphic encryption built on the matrices (HEBM). The recent work of (Zhou et al., 2018) where the authors expedited the bootstrap by three steps, resulting in improved data security performance. In order to comprehend algorithms and handle the disconnect between server and the client by establishing communication, (A. Chatterjee & Sengupta, 2018) were able to use FHE, encoding confidential material, and keep it within server guaranteeing confidentiality.(Dowlin et al., 2017) used Simple Encrypted Arithmetic Library (SEAL) to create a Homomorphic Encryption for critical medical and genetic data, making it available to the public in bioinformatics and providing privacy. Because secret data sharing is a crucial component of cryptography, a novel homomorphic encryption strategy (Zhang et al., 2018) is proposed for outsourcing secret data sharing. (Li et al., 2017) presents the leading multi-hop homomorphic identity-based proxy re-encryption approach, which has applications in e-mail relaying, data exchange, and access controls. In order to lessen the temporal complexity of unique term searches, the server in (Wu et al., 2018) constructs a downward encrypting access structure instead of employing a query trapdoor technique. (Tsoutsos & Maniatakos, 2018), which uses additive homomorphic encryption to offer encrypted computations effectively, proposes not only confidentiality but also integrity guarantees. Given the growing discovery of numerous FHE algorithms, none have shown to be viable in terms of the large proportion of produced distortion, which boosts computer complexity (Acar et al., 2018).

ABE, on the other hand, entails a kind of public-key encryption which enables numerous individuals to securely share data (Kocabas et al., 2016). Several CP-ABE experiments were conducted to protect electronic health (e-health) data (Oh et al., 2021).(Attrapadung, 2011) proposed a KP-ABE approach by including a non-monotonic access control mechanism and a fixed cipher - text length. In this study (Iao et al., 2019), the authors developed a completely secure Data Sharing Framework (DSF) that enables for electronic encoding and external decoding. The authors demonstrated that DSF may be applied in a cloud-assisted s-health system utilizing s-health context as research study. In addition, to reduce the encryption or decryption cost, (Ning et al., 2018) created an audit trails σ-time leased ABE approach that eliminates excessive decryption latency and offers unrestricted access permissions on mobile devices. In the context of Internet of Things, (Y. Yu et al., 2018) suggested a compact break-glass access management structure, and (Y. Yang et al., 2018) presented simplified and direct contact guaranteed elimination method for rollout using CP-ABE. In majority of cases, a health professional can decode and extract data if the characteristic combination complies with access control policy for the medical file. In an emergency, the medical file's access control policy is circumvented via a break-glass entrance technique, giving emergency medical personnel or rescue personnel quick access to data. Because the current CP-ABE method does not take underlying hierarchical system of file shared into account, S. Wang et al. developed a working file directory (FH-CP-ABE) scheme within cloud applications (S. Wang et al., 2016). In order to conserve time and storage space when encrypting structured records, the method encrypts them through an embedded access structure. (Guan et al., 2021) suggested a modified CP-ABE technique featuring consistent ciphertext length as well as less processing required for encryption and decoding.(Zhong et al., 2021) presents an efficient ABE system that delegates partial encryption and decryption to edges endpoints and allows for attribute updates, allowing for more dynamic control. A contemporary CP-ABE system that utilizes cryptography (ECC) is proposed in (R. Cheng et al., 2021), where the bilinear pairing operation gets replaced with straightforward multiplications and the majority of the decryption work are delegated onto edge devices. It was discovered that the (Odelu et al., 2016) technique has a security flaw (Herranz, 2017). It was shown that the technique may be defeated with the help of an unsatisfied user of the policy. This assumption is made on the grounds that such attack is feasible when anycombination of users' attribute sets satisfies the access policyrequirements. In addition, (Raj & Pais, 2020) presented a modified plan which was first offered by (Odelu et al., 2016). This proposed approach relies on ECC and employs an

AND-gate access policy upon a consistent size secret private key. ECC is a cost-effective encryption and decryption algorithm. A type of AES-to-FHE approach has been recognized to be a suitable method of protecting patient information. Given the obvious benefits of ABE for securing healthcare data in the cloud, it is believed that employing it for the collecting and availability of health data would be beneficial. It is therefore proposed that a better ABE-to-FHE modification method, which never decrypts and re-encrypts data, could become helpful for protecting patient data. Because of the intrinsically distributed condition of the IoT context, multi-authority ABE is required for the application of smooth access control, which can also relieve the burden of a single attribute authority and increase the performance of the system. (Banerjee et al., 2020) presented a safe, streamlined user access control system regarding data consumption within IoT context. The approach, a three-factor access management system, supports multi-authority ABE and is very versatile because the ABE key size saved on the person's chip card and the cipher - text length required for connection requests stay unchanged in regards to the number of characteristics. In 2019, (G. Wang et al., 2019)developed a three-to-one recording mechanism and unveiled a new lattice-based CP-ABE system. A lattice-based ABE system that is indirectly removable and offers effective and protect user denial within lattices was created by (Dong et al., 2020), with inspiration from (Gorbunov et al., 2013). (Brakerski & Vaikuntanathan, 2020) provided a circuit access policy CP-ABE system, but they left safety as an unanswered question by omitting a security restriction from this design. Consider a scenario where huge number of user's texts $\mu 1, \mu 2, \ldots$ are encoded and preserved on a cloud server. In order to reduce the cost of processing and communication, he wants the function f to handle ciphertext provided by the cloud platform without compromising privacy. The ciphertext handled by f can then be decrypted to $f(\mu 1, \mu 2, \ldots)$. The homomorphic operations on the ciphertext are not supported by the aforementioned lattice-based ABE algorithms. Two shortcomings exist in the direct application of classic CP-ABE in smart medical. The first is that smart medical files are encoded yet access policies are written in plaintext, exposing sensitive medical-related data. Another is that it frequently only accepts a small set of attributes, therefore places a disadvantageous restriction upon the use of CP-ABE applications because the number of its public parameters grows proportionately with the size of the attribute universe. PASH (Y. Zhang et al., 2018), a privacy-aware smart healthaccess management platform was presented to address these issues. A large universe CP-ABE with partially designed access restrictions is the most crucial element. Only the labels of the access policy attribute values were visible since the values remain concealed in PASH's encoded SHRs. The possibility of implementing such a system on resource-constrained devices is increased by the CP-ABE approach provided in (Odelu et al., 2017) to achieve a compact set of encrypted message and secret keys, independent on the amount of attributes. The scheme is currently limited to the usage of AND-gates, hence it must be expanded to accommodate OR-gates in access regulations. As a result, it is inapplicable invariety of IoT applications where greater expressive power is necessary.ECC-MA-CPABE which provides higher strength, a smaller key length and requires less calculation load, was also recommended by (Sandhia & Raja, 2020). The solution discussed above only resolved attribute selection during data uploading and does not support the concept of attribute revocation. In this work, the researchers created an improved CP-ABE method using set ciphertext size enabling quick encryption and decryption (Guan et al., 2021). Additionally, two updated techniques were developed to stop legitimate persons in spilling content but also protect the privacy of data owners by combining bloom filters, CP-ABE, and chameleon hash.(Salvador et al., 2017) present a novel method that integrates attribute-based encryption's adaptability and speedy resolution with the efficiency of symmetric key encryption for conducting secure information interactions across the numerous entities that comprise this new IoT environment. However, this strategy should be supplemented by integrating authentication mechanisms and doing various tests on real gadgets with limited resources. Some researchers are also concerned about user privacy being compromised as a result of public access regulations.(Han et al., 2018) proposed an ABE technique that hides both user and access policy attributes since they expected the user attribute security would get compromised throughout key structure and encoding stages. (K. Yang et al., 2014) developed a dynamic policy updating technique for the sequential system of secret sharing structure. With the aid of an update key, the proxy can change encrypted message through the old access structure into a fresh one.In ECC, a KP-ABE centered on bilinear pairing sets was used to execute the method. The central server took data from sensors and encoded it with ABE, which could be decoded by a user with appropriate attributes. (Ruj et al., 2011) proposed a scheme to handle large attribute authority. (S. Chatterjee & Roy, 2014) cryptanalyzed the techniques given in (Ruj et al., 2011; S. Yu et al., 2009) and found out that both techniques are susceptible to insider threats, allowing users with less authority access to sensitive data. (S. Chatterjee & Das, 2014) suggested a smooth user access management approach for WSNs that is resilient to insider threats based on the KP-ABE methodology. The KPABE and a user repudiation technique built on bilinear pairing operations were the foundations of a protective measure for the WBAN suggested by (Tian et al., 2014).(Ma et al., 2017) presented fresh version of KPABE, called KPABE using timeframe, in 2017. The recipient can decrypt the ciphertext within the specified timeframe, as per their technique. They also demonstrated how this method could be used in cloud timeframe scenarios. By proposing the KPABE with backdoor reencryption, other form of the KPABE is proposed (Ge et al., 2018). The technique is demonstrated utilizing adaptable approach that takes into account the chosen ciphertext attack (CCA) and a monotonic access policy. A KPABE approach that would be resistant to constant auxiliary input loss was also suggested by (J. Li et al., 2018) after they examined one application scenario. Bilinear pairing processes are used in the KPABE systems listed above.

The idea of compact size with no bilinear pairing has been explored in recent years.(Yao et al., 2014) presented a small-scale KPABE scheme that employs ECC for the Internet of Things (IoT) without the use of bilinear pairing, however the method has a number of limitations, including no key update mechanism and restricted scalability. ECC is a high-security, high-processing-speed encryption algorithm which is one of the most well-known cryptographic algorithms due to its compact size characteristic with comparable security robustness to other public key strategies (Sowjanya et al., 2020; Xiao et al., 2021). A consensus for the use of ECC with hardware or software implementations has risen as a result of IoT nodes' limits in regards to durability, storage, physical resources, and processing power (Cano & Cañavate-sanchez, 2020). Many ECC-based authentication approaches have been presented (Hong & Sun, 2016; Kaur et al., 2016), which could be shown to be effective (lightweight) for smart technology. (Hong & Sun, 2016) proposed a more efficient key protected KPABE method with no pairing, yet their system is sensitive to the colluding attack and safe under the computational Deffie–Hellman (CDH) hypothesis utilizing randomizeddatabase framework. The authors (Sowjanya et al., 2020)suggested lightweight key-policy ABE with elliptic-curve-cryptography using key refresh/update approach and no bilinear pairing. The authority is also in charge of key distribution, which includes direct attribute/user termination. The system is secure because it is based on EC decisional Diffie–Hellman (ECDDH) hypothesis in attribute-based selective-set framework, rather than the random oracle framework. In order to address the security issues of telecare medical information system (TMIS), (Xiao et al., 2021)suggests a physical unclonable function (PUF) and ECC technology-based access control and verification system ideal in TMIS. However, the hardware degradation and instabilities with existing PUF systems do exist. In this study (Vincent & Folorunso, 2020), a novel security method is presented that combines elliptic curve embedded cryptography with a cyclotomic elliptic curve that can be proven to be secure. A hash function that may be used to create a structure from a curve coordinate and a polynomial variable is built using the described method, which also uses a cyclotomic function and the Weierstrass version within elliptic curve. Other elliptic curve forms can be utilized to enhance the said study even more than Weierstrass shortened version, which was used in it. Recently, a new small-scale flexible cryptography method that boosts the security of high-performance computing for medical data was developed (Abdulraheem & Balogun, 2021). The suggested method showed a significant improvement in data encryption speed as well as enhanced security.

A small ciphertext attribute-based fully homomorphic technique built around LWE issue on lattices was developed in 2021 (Y. Liu et al., 2021). Through defining every system's attributes and utilizing the unique structural array of MP12, the investigators eliminated the dependence of the cipher - text length upon this system's parameters ℓ so the cipher - text length will be no further extended with overall number of system's parameters. They also entirely re-randomize all standard error within that latest cipher - text by adding the function $G - 1$ in the homomorphic procedures, resulting in a very precise and uncomplicated error breakdown utilizing sub-Gaussianity. Unfortunately, this system uses a "AND" access policy to increase space and time efficiency, which does not permit more versatile access policies.

RESEARCH METHODOLOGY

A thorough review of literature was conducted in the subjected field, thereby came up with the recommended research topic.

The proposed technique for implementing this study is a hybridization of the ABE and FHE security system algorithms, which takes advantage of best qualities of each. In order to come up with a more solid security and efficient technique for Smart healthcare, ECC algorithm would be employed to further encrypt healthcare data.

ABE is a kind of public-key cryptography that enables a large number of participants to safely communicate data. A definition of an access policy $\mathbb{P}$ might include disjunctions, conjunctions, and (k, n) – threshold gates of attributes such as

$$(\text{Nurse} \wedge \text{Emergency}) \vee (\text{Doctor} \wedge \text{Cardiology})$$

this allows entry for a cardiology doctor, OR a nurse, OR emergency personnel.

FHE allows ciphertexts to be subjected to an unspecified number of multiplications and sums, with the output being the same as the outcome of operations performed on plain data when the data is decrypted. This makes it possible for cloud hosting to use ciphertexts for legal purposes without first requiring to decode it.

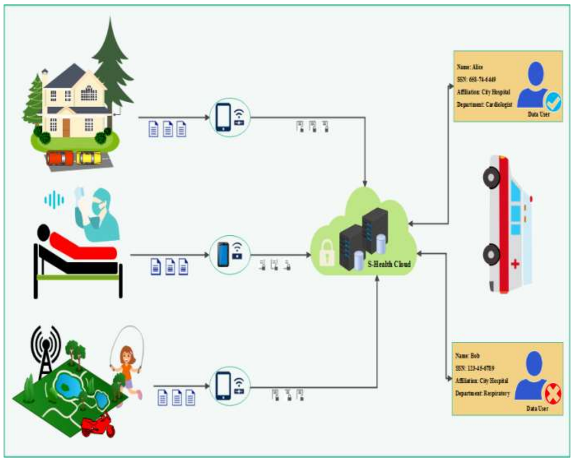

Figure 1: Smart Healthcare system

Elliptic Curve Cryptography (ECC) is a highly secure and quick-processing encryption method.A widespread knowledge of the use of ECC with hardware or software solutions has arisen as a result of the limits of smart nodes in terms of storage,durability, computing power, andhardware (Cano & Cañavate-sanchez, 2020).

Preliminaries

A. Access Structures and Attribute

Theaccess 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. A n-bit string $a_1a_2 \dots a_n$, defines access structure $\mathbb{A} \subseteq \mathbb{U}$, while $a_1 = 1$ if $A_1 \in \mathbb{A}$ otherwise 0 if $A_1 \notin \mathbb{A}$.

The total of all access structures $\mathbb{A}_k = a_{1_k}a_{2_k} \dots a_{n_k}$ from attribute controller C_k , when $k \in [1, N]$, makes up a user access structure $\mathbb{A}$. $A_k$defines the attributes that are within the jurisdiction of attribute controller AC_k. A lone attribute controller controls a single attribute. We get $a_{i_k} = 0$for attribute $A_i$that is not measured by attribute controllers AC_k. It's worth noting that we can express $\mathbb{A} = \sum_{k=1}^{N} \mathbb{A}_k$as $\mathbb{A}_j \cap \mathbb{A}_k = \emptyset$, where $j, k \in [1, N]$ and $j \neq k$.

Every participant can only access a gadget having access structure $\mathbb{P} \subseteq \mathbb{U}$ in which $\mathbb{P} = b_1b_2 \dots b_n$ and only if $\mathbb{P} \subseteq \mathbb{A}$ if they have the approved access structure listed in the AND gate access policy.Likewise, requirement $(a_1 - b_1) \geq 0$must be satisfied for $\mathbb{A}$ to satisfy$\mathbb{P}$, $\forall i \in [1, n]$.

B. Bilinear Pairing

Consider$\mathbb{G}_1, \mathbb{G}_2$be distinct multiplicative cyclic sets of order p and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be the bilinear map that meets three characteristics stated below (Iao et al., 2019):

1) Bilinearity – Given the random elements $a, b \in \mathbb{Z}_p, g_1, g_2 \in \mathbb{G}_1$, the equation $e(g_1^a, g_2^b) = e(g_1, g_2)^{a\,b}$ holds;
2) Non-degeneracy– The $\mathbb{G}_1$generator cannot mapped by bilinear map e to the identification “1” of $\mathbb{G}_2$, namely $e(g, g) \neq 1$;
3) Efficient computation – To compute $e(g_1, g_2)$, there is an efficient algorithm.

C. Attribute Based Encryption Algorithm

KP-ABE method provided in (Odelu et al., 2017)with CP-ABE methodpresented are combined to create 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 secret key as well as universe of attributes $\mathbb{U} = \{A_1, A_2, \dots, A_n\}$ as 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 M, withMPK.
3. **KeyGen:** It is given an attribute set$\mathbb{A}$, master secret key MSK, as well as master public-key "MPK" in order to get an output known as decoding key k_u of $\mathbb{A}$.
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 $\mathbb{P}, k_u$similar to$MPK$and $\mathbb{A}$ as parameters.

D. Fully Homomorphic Encryption Algorithm

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

1. KeyGen(1^n): when the security parameter 1^n is entered, public key pk and secret key sk are produced by this algorithm.
2. Encrypt (pk, μ): an incoming message μdepending on public key pk. A cipher-text c is produces by the scheme.
3. Decrypt $(\mathrm{sk}, \mathrm{c}) \rightarrow \mu$: it outputs the message μ built on secret key sk and cipher-text c inputs.
4. Eval$(\mathrm{pk}, \mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_\mathrm{k}, \mathrm{f})$: takes as input public key pk, list of cipher-text$\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_\mathrm{k}$, a functional$\mathrm{f} \in \mathrm{F}$.It produces a new cipher-text $\mathrm{c}_\mathrm{f}$in which Decrypt $(\mathrm{sk}, \mathrm{c}_\mathrm{f}) = \mathrm{f}(\mu_1, \mu_2, \ldots, \mu_\mathrm{k})$.
5. Decrypt $(\mathrm{sk}, \mathrm{c}_\mathrm{f}) = \mathrm{f}(\mu_1, \mu_2, \ldots, \mu_\mathrm{k})$ on output new ciphertext $\mathrm{c}_\mathrm{f}$given parameter public key pk, cipher-text set $\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_\mathrm{k}$,as well as functional$\mathrm{f} \in \mathrm{F}$.

E. Elliptic Curve Cryptography Algorithm

ECDH's algorithm: Assuming an elliptic curve $E(\mathbb{F}_p)$ over a finite prime field Participants A and B in a conversation agree on a point $E(\mathbb{F}_p)$ 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 point $k_B Q$ with secret private key k_A, participant A determines P. 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.).

Fig. 2 illustrates 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.

Table 2: Inputs and Outputs for various phases.

Phase	Input	Output
Setup Phase	$\mathbb{U}$, $\boldsymbol{\rho}$	*MSK, MPK*
Encrypt Phase	$\mathbb{P}$, *MPK, M* message	$C = \{\mathbb{P}, R_m, K_{1m}, K_{2m}, C_{\sigma m}, C_m\}$
KeyGen Phase	$\mathbb{A}$, *MSK, MPK*	$k_u = (u_1, u_2)$
Decrpyt Phase	$C, k_u, MPK, \mathbb{A}$	⊥ormessage*M*

Table 3: Expressions.

Expression	Description
$\mathbb{A}$	User-defined attributes, $\mathbb{A}\subseteq\mathbb{U}$
$\mathbb{P}$	$\mathbb{P}\subseteq(\mathbb{U}/A_n)$, Access policy
$\mathbb{U}$	Universe of n attributes
(α, k_1, k_2)	System private keys
$\mathbb{G}$	Elliptic curve group $\{p, E_p(a, b), P\}$ generated by P
P	A base point in $E_p(a, b)$whose order is a 160-bit number in Z_p
xP	$P + P + \cdots P(x\ times)$, scalar multiplication, $P \in E_p(a, b)$
P	A large prime number
Z_p	$[\{0,1, \ldots, p - 1\}$
$E_p(a, b)$	An elliptic curve $y_2 = [[x_3 + ax + b(modp)$ defined over the finite fieldZ_p

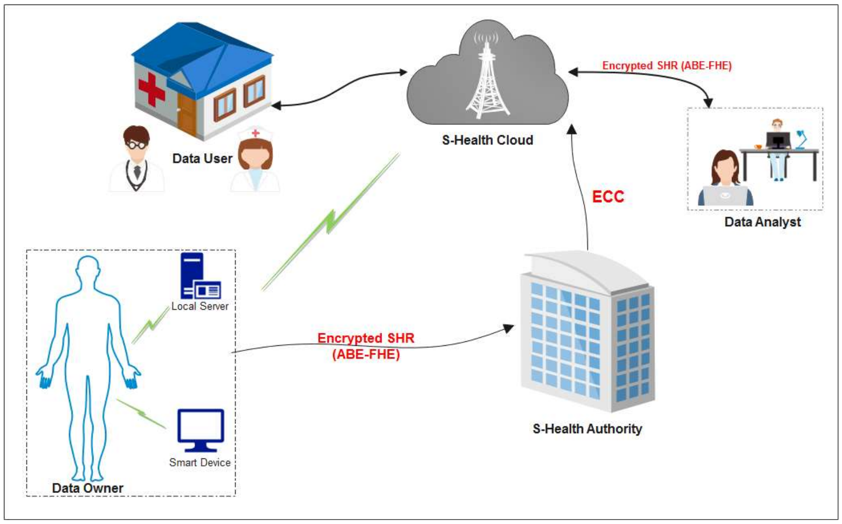

Figure 2: Framework of the proposed smart health security scheme

EXPERIMENTS, RESULTS AND DISCUSSION

In smart healthcare, the ABE-FHE-ECC algorithm have been proven secure. External attackers are unable to make use of the algorithms in Section 3.2. The security mechanism is first described, after which this scheme is contrasted with three distinct techniques, specifically (Zhong et al., 2021), (Sowjanya et al., 2020) and (Y. Liu et al., 2021).

Security Model

This security strategy is defined and adapted from (Banerjee et al., 2020; Odelu et al., 2017), where adversary stipulates challenge access policy prior Setup phase, to demonstrate the level of security of the ABE-FHE-ECC algorithm. In order to represent indistinguishability in communications as well as collusion-resistance of participantprivate keys, consider the following security game between an Adversary Adv as well as a Challenger Sim.

- **Initialization:** Adv transfers to Sim a n-bit challenge access policy $\mathbb{P}$`.
- **Setup:** By using Setup command with the security parameter ρ, Sim creates master pair key (MPK, MSK). A master public-key MPK is therefore given to Adv by Sim.
- **Query:** Adv asks Sim these subsequent questions.
  - Adv queries secret key $k_{u_i}$of every attribute set $\mathbb{A}^i$.
  - The decoding of the ciphertext $Enc(\mathbb{P}^i, M^i)$ is questioned by Adv.
- **Challenge:** In this task, Adv outputs (M_0, M_1). Keep in mind that Adv did not attempt to find the private key about an attribute set $\mathbb{A}$ fulfilling given association: $\mathbb{P}' \subseteq \mathbb{A}$. Sim now chooses a random $c' \in \{0,1\}$, then in turn evaluates the challenge cipher-text $E(\mathbb{P}', M_{c'})$and sent over to Adv.
- **Query:** With the exception of secret key query to each attribute set A fulfilling the relationship $\mathbb{P}' \subseteq \mathbb{A}$ as well as decryption query of $E(\mathbb{P}', M_{c'})$, Adv maintains to answer all private key and decoding queries.
- **Guess:** In the end, Adv outputs a randomized assumption bit, c'_g, and is declared the winner when $c'_g = c'$.

The strength ∈on Adv is determined via $\in = Pr[c'_g = c'] - \frac{1}{2}$ within that game.

Within this coming sections, decisional bilinear Diffie-Hellman (DBDH) issue was developed and improved upon from related earlier research (Banerjee et al., 2020). Let $\mathbb{G} = \{G_1, G_2, G_t, p, e\}$ become a pairedset. Consider multiple co-prime polynomials, $\varphi(x)$ and $\vartheta(x)$ in two different polynomials. Let the generators for the paired sets $G_1$and G_2also be g_1 and g_2, respectively. Provided that

$$g_1, g_1^{\alpha}, g_1^{\alpha^2}, \dots, g_1^{\alpha^{n-1}}, g_1^{\alpha\varphi(\alpha)},$$
$$g_2, g_2^{\alpha}, g_2^{\alpha^2}, \dots, g_2^{\alpha^n},$$
$$g_2^{1/\vartheta(\alpha)}, g_2^{\alpha/\vartheta(\alpha)}, g_2^{\alpha^2/\vartheta(\alpha)}, \dots, g_2^{\alpha^n/\vartheta(\alpha)},$$
$$g_1^{\gamma\varphi(\alpha)}, g_2^{\gamma},$$

and

$T \in G_T$, where $T = e(g_1, g_2)^{\gamma\varphi(\alpha)}$ or T is a random element of G_t, DBDH problem decides whether the element $T = e(g_1, g_2)^{\gamma f(\alpha)}$or just a random element of G_t .

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

Table 3 compares all of the schemes based on significant characteristics such as computability, large number of attributes, storage capacity, and ECC-based function. Table 3 shows 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 amount and low memory capacity at the same time, whereas the latter cannot allow encrypted data calculation.

Table 4: Functional Comparison

Scheme	(Zhong et al., 2021)	(Sowjanya et al., 2020)	(Y. Liu et al., 2021)	ABE-FHE-ECC
Computability	×	×	Full	Full
Large number of Attributes	✓	✓	✓	✓
Storage Capacity	High	Low	High	Low
ECC Based	×	✓	×	✓

Computing Cost

The majority of the computing cost comes from the ciphertext storage size, encryption, and decryption. With regards to computing costs, Figures 3, 4, and 5 compare the ABE-FHE-ECC system to various existing schemes. Figure 3 illustrates the link of both cipher-text produced and attributes of user. 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 into the web.The link of both attributes chosen by the user as well as time needed to encode all data collected is shown in Figure 4. The graph shows how much quicker the proposed method encodes data as compared to conventional systems. This is possible because of the small ciphertext. Figure 5 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 because 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.

CONCLUSION

An efficient ABE-FHE system becomes more crucial as internet-based technologies and Internet of things gadgets become more prevalent across smart healthcare. 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 user and data owner 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.

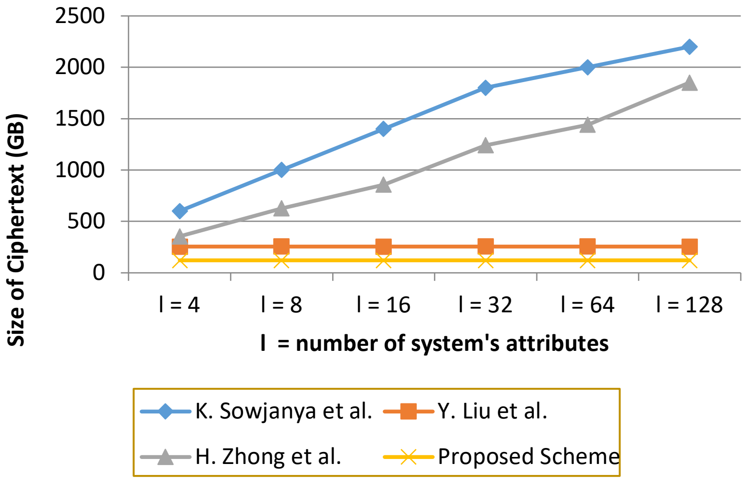

Figure 3: Comparing the storage requirements for ciphertext across ABE-FHE-ECC and comparable methods

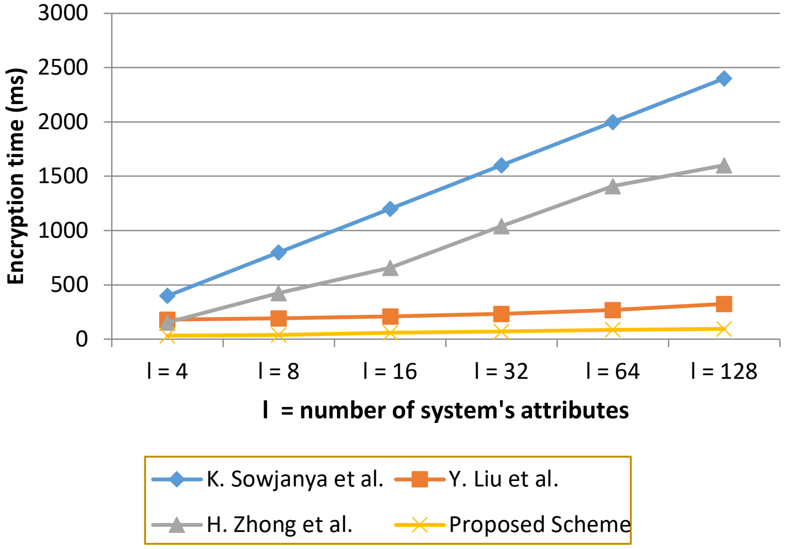

Figure 4: Total Encryption Time

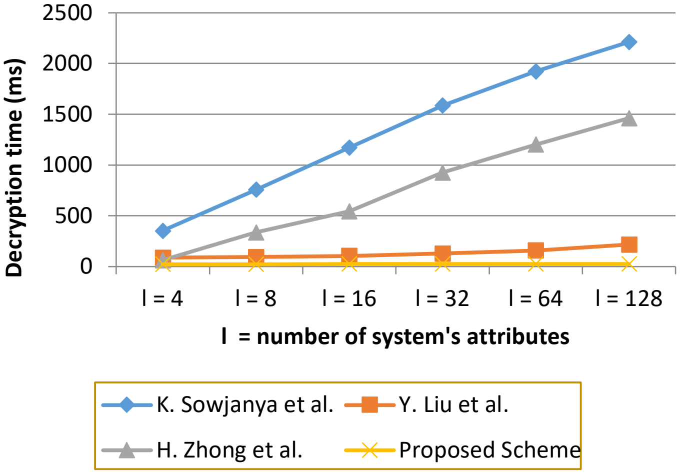

Figure 5: Total Decryption time

Contributions to Knowledge

The primary benefit of the ABE-FHE-ECC scheme is that it eliminates the requirement to decrypt encoded smart healthcare data in order to perform operations on it. The following are some of the other contributions:

i. The ECC Access Control Policy improves efficiency in the first place.

ii. The attribute set and key generation procedure are maintained by a trusted authority. This cuts down on both overhead and computation time.

iii. The speed and computing capacities have been enhanced.

iv. Allows multiple parties with permission to access private data.

v. The Decisional Bilinear Diffie-Hellman (DBDH) hypothesis is used to prove how secure this method is, thus practical findings indicate that it works well for data in health-care IoT.

Limitation

This suggested approach has a good security technique; however, it lacks attribute revocation and policy updating, which would enable user direct revocation and keep the revocation list short.

Recommendations

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 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

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.

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

Armknecht, F., Boyd, C., Carr, C., Gjosteen, K., Jaschke, A., Reuter, C. A., & Strand, M. (2015). A Guide to Fully Homomorphic Encryption. *Cryptology EPrint Archive*, 1–35. https://eprint.iacr.org/2015/1192

Attrapadung, N. (2011). Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. *International Workshop on Public Key Cryptography*, 1–18.

Baker, S. B., Xiang, W. E. I., Member, S., & Atkinson, I. A. N. (2017). *Internet of Things for Smart Healthcare : Technologies , Challenges , and Opportunities*. *5*, 24.

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

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

Boneh, D., Gennaro, R., Goldfeder, S., Jain, A., Kim, S., Rasmussen, P. M. R., & Sahai, A. (2018). Threshold cryptosystems from threshold fully homomorphic encryption. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10991 LNCS*, 565–596. https://doi.org/10.1007/978-3-319-96884-1_19

Boyi, X., Li Da, X., Hongming, C., Cheng, X., Jingyuan, H., & Fenglin, B. (2014).

Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, *10*(2), 1578–1586. https://doi.org/10.1109/TII.2014.2306382

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Huang, H., Gong, T., Ye, N., Wang, R., & Dou, Y. (2017). Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System. *IEEE Transactions on Industrial Informatics*, *13*(3), 1227–1237. https://doi.org/10.1109/TII.2017.2687618

Iao, Y., Tong, Q., Choo, K. R., Member, S., Liu, X., Deng, R. H., & Li, H. (2019). Secure Online / Offline Data Sharing Framework for Cloud-Assisted Industrial Internet of Things. *IEEE Internet of Things Journal*, *PP*(c), 1. https://doi.org/10.1109/JIOT.2019.2923068

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

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.2016.7841955

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.2019.2903785

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

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.2016.2520933

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

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.2017.2740720

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), 15683–15693. https://doi.org/10.1109/JIOT.2020.3033129

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

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

Magons, K. (2016). Applications and benefits of elliptic curve cryptography. *CEUR Workshop Proceedings*, *1548*, 32–42.

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), 11743–11757. https://doi.org/10.1109/JIOT.2021.3058953

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

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

Odelu, V., Das, A. K., Rao, Y. S., Kumari, S., Khan, M. K., & Choo, K. K. R. (2017). Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. *Computer Standards and Interfaces*, *54*, 3–9. https://doi.org/10.1016/j.csi.2016.05.002

Oh, S.-R., Seo, Y.-D., Lee, E., Kim, Y.-G., Elkhodr, M., Darwish, O., & Alsinglawi, B. (2021). A Comprehensive Survey on Security and Privacy for Electronic Health Data. *Public Health*, *18*, 9668. https://doi.org/10.3390/ijerph18189668

Pacheco, J., Tunc, C., Satam, P., & Hariri, S. (2016). Secure and Resilient Cloud Services for Enhanced Living Environments. *IEEE Cloud*

Computing, *3*(6), 44–52. https://doi.org/10.1109/MCC.2016.129

Pulkkis, G., Westerlund, M., Karlsson, J., & Tana, J. (2017). *Secure and Reliable Internet of Things Systems for Healthcare*. 169–176. https://doi.org/10.1109/FiCloud.2017.50

Raj, N., & Pais, A. R. (2020). CP-ABE scheme satisfying constant-size keys based on ECC. *ICETE 2020 - Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*, *3*(Icete), 535–540. https://doi.org/10.5220/0009590905350540

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On Data Banks and Privacy Homomorphism. *Massachusetts Institute of Technology Cambridge, Massachusetts*, *15*(2), 313–337. https://doi.org/10.1075/jpcl.15.2.04lef

Ruj, S., Nayak, A., & Stojmenovic, I. (2011). *Distributed Fine-grained Access Control in Wireless Sensor Networks*. https://doi.org/10.1109/IPDPS.2011.42

SA, S. (2018). Big Data in Healthcare Management: A Review of Literature. *American Journal of Theoretical and Applied Business*, *4*(2), 57. https://doi.org/10.11648/j.ajtab.20180402.14

Salim, M. M., Kim, I., Doniyor, U., Lee, C., & Park, J. H. (2021). Homomorphic Encryption Based Privacy-Preservation for IoMT. *MDPI - Journal of Applied Sciences*.

Salvador, P., Skarmeta, A. F., Pedone, D., Rotondi, D., & Straniero, L. (2017). A Digital Envelope approach using Attribute-Based Encryption for Secure Data Exchange in IoT Scenarios. *IEEE*.

Sandhia, G. K., & Raja, K. (2020). Elliptic Curve Cryptography integrated with Multi-Authority CiphertextPolicy Attribute Based Encryption (ECC-MA-CPABE) for Data Security in Cloud Environment. *International Journal of Advanced Science and Technology*, *29*(5), 7115–7129.

Sowjanya, K., Dasgupta, M., Ray, S., & Obaidat, M. S. (2020). An Efficient Elliptic Curve Cryptography-Based without Pairing KPABE for Internet of Things. *IEEE Systems Journal*, *14*(2), 2154–2163. https://doi.org/10.1109/JSYST.2019.2944240

Thilakanathan, D., Chen, S., Nepal, S., & Calvo, R. (2016). SafeProtect: Controlled Data Sharing with User-Defined Policies in Cloud-Based Collaborative Environment. *IEEE Transactions on Emerging Topics in Computing*, *4*(2), 301–315. https://doi.org/10.1109/TETC.2015.2502429

Tian, Y., Peng, Y., Peng, X., & Li, H. (2014). *An Attribute-Based Encryption Scheme with Revocation for Fine-Grained Access Control in Wireless Body Area Networks*. *2014*(1).

Tsoutsos, N. G., & Maniatakos, M. (2018). Efficient detection for malicious and random errors in additive encrypted computation. *IEEE Transactions on Computers*, *67*(1), 16–31. https://doi.org/10.1109/TC.2017.2722440

Tu, Y., Wang, J., Yang, G., & Liu, B. (2021). *An efficient attribute-based access control system with break-glass capability for cloud-assisted industrial control system*. *18*(November 2020), 3559–3577. https://doi.org/10.3934/mbe.2021179

van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010). Fully homomorphic encryption over the integers: From theory to practice. *NTT Technical Review*, *12*(7), 1–28.

Vincent, O. M. L. O. R., & Folorunso, A. A. A. A. O. (2020). An improved hybrid scheme for e-payment security using elliptic curve cryptography. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-020-00517-6

Vizitiu, A., Niă, C. I., Puiu, A., Suciu, C., & Itu, L. M. (2020). Applying Deep Neural Networks over Homomorphic Encrypted Medical Data. *Computational and Mathematical Methods in Medicine*, *2020*. https://doi.org/10.1155/2020/3910250

Wang, D., Guo, B., & Lin, Y. (2017). A Faster Fully Homomorphic Encryption Scheme in Big Data. *IEEE 2nd International Conference on Big Data Analysis*, 345–349.

Wang, G., Liu, Z., & Gu, D. (2019). *Ciphertext Policy Attribute-Based Encryption for Circuits from LWE Assumption*. 378–396.

Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., & Xie, W. (2016). An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1265–1277. https://doi.org/10.1109/TIFS.2016.2523941

Wu, D. N., Gan, Q. Q., & Wang, X. M. (2018). Verifiable Public Key Encryption with Keyword Search Based on Homomorphic Encryption in Multi-User Setting. *IEEE Access*, *6*, 42445–42453. https://doi.org/10.1109/ACCESS.2018.2861424

Xiao, L., Xie, S., Han, D., Liang, W., Guo, J., & Chou, W. (2021). A lightweight authentication scheme for telecare medical information system. *Connection Science*. https://doi.org/10.1080/09540091.2021.1889976

Yang, K., Jia, X., Ren, K., Xie, R., & Huang, L. (2014). *Enabling Efficient Access Control with Dynamic Policy Updating for Big Data in the Cloud*. 2013–2021.

Yang, Y., Liu, X., & Deng, R. H. (2018). Lightweight break-glass access control system for healthcare internet-of-things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3610–3617. https://doi.org/10.1109/TII.2017.2751640

Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. *Journal of Network and Computer Applications*, *89*, 26–37. https://doi.org/10.1016/j.jnca.2016.11.017

Yao, X., Chen, Z., & Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2014.10.010

Yousuf, H., Lahzi, M., Salloum, S. A., & Shaalan, K. (2021). *Systematic Review on Fully Homomorphic Encryption Scheme and Its Application*. *January*. https://doi.org/10.1007/978-3-030-47411-9

Yu, S., Ren, K., & Lou, W. (2009). FDAC : Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks. *IEEE Xplore*.

Yu, Y., Xue, L., Li, Y., Du, X., Guizani, M., & Yang, B. (2018). Assured Data Deletion with Fine-Grained Access Control for Fog-Based Industrial Applications. *IEEE Transactions on Industrial Informatics*, *14*(10), 4538–4547. https://doi.org/10.1109/TII.2018.2841047

Zhang, E., Peng, J., & Li, M. (2018). Outsourcing secret sharing scheme based on homomorphism encryption. *IET Information Security*, *12*(1), 94–99. https://doi.org/10.1049/iet-ifs.2017.0026

Zhang, Y., Zheng, D., & Deng, R. H. (2018). Security and Privacy in Smart Health : E ffi cient Policy-Hiding Attribute-Based Access Control. *IEEE INTERNET OF THINGS JOURNAL*, *3*(1), 1–15. https://doi.org/10.1109/JIOT.2018.2825289

Zhong, H., Zhou, Y., Zhang, Q., Xu, Y., & Cui, J. (2021). An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. *Future Generation Computer Systems*, *115*, 486–496. https://doi.org/10.1016/j.future.2020.09.021

Zhou, T., Yang, X., Liu, L., Zhang, W., & Li, N. (2018). Faster bootstrapping with multiple addends. *IEEE Access*, *6*, 49868–49876. https://doi.org/10.1109/ACCESS.2018.2867655