Secure Healthcare Monitoring Sensor Cloud With Attribute-Based Elliptical Curve Cryptography

Rajendra Kumar Dwivedi, Madan Mohan Malaviya University of Technology, Gorakhpur, India
https://orcid.org/0000-0001-6682-1942

Rakesh Kumar, Madan Mohan Malaviya University of Technology, Gorakhpur, India

Rajkumar Buyya, The University of Melbourne, Melbourne, Australia

ABSTRACT

Sensor networks are integrated with cloud in many internet of things (IoT) applications for various benefits. Healthcare monitoring sensor cloud is one of the application that allows storing the patients' health data generated by their wearable sensors at cloud and facilitates the authorized doctors to monitor and advise them remotely. Patients' data at cloud must be secure. Existing security schemes (e.g., key policy attribute-based encryption [KP-ABE] and ciphertext policy attribute-based encryption [CP-ABE]) have higher computational overheads. In this paper, a security mechanism called attribute-based elliptical curve cryptography (ABECC) is proposed that guarantees data integrity, data confidentiality, and fine-grained access control. It also reduces the computational overheads. ABECC is implemented in .NET framework. Use of elliptical curve cryptography (ECC) in ABECC reduces the key length, thereby improving the encryption, decryption, and key generation time. It is observed that ABECC is 1.7 and 1.4 times faster than the existing approaches of KP-ABE and CP-ABE, respectively.

KEYWORDS

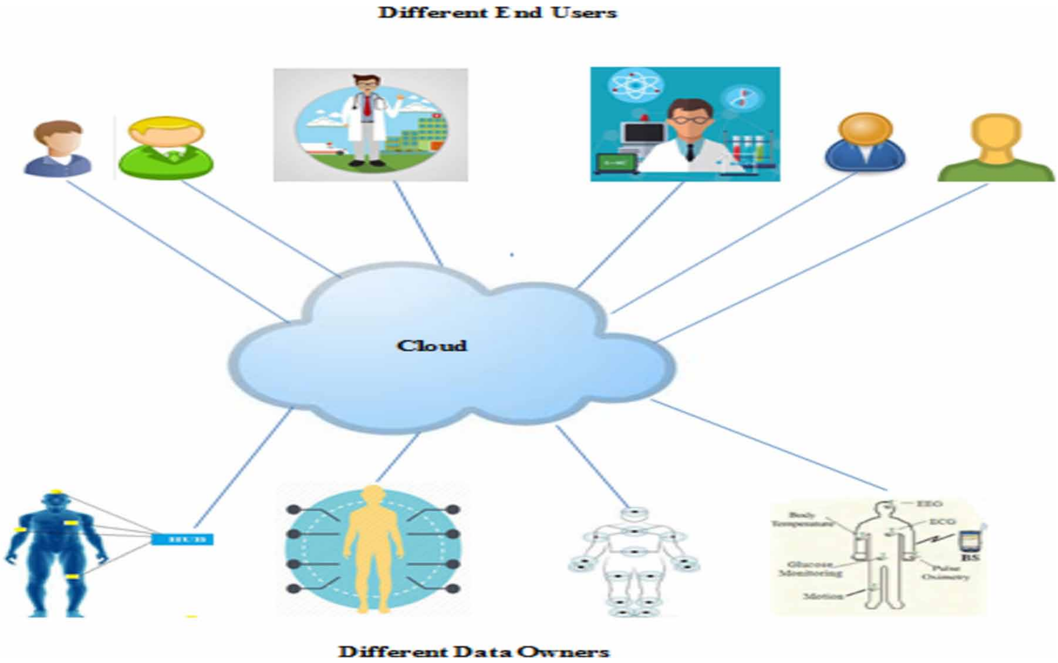
Cloud Computing, Data Security, Elliptical Curve Cryptography, Internet of Things, Sensor Cloud, Wireless Sensor Network (WSN), Wearable Sensors

1. INTRODUCTION

Sensor based Internet of Things (IoT) have various applications such as healthcare applications, battlefield monitoring, street monitoring, disaster management, military, forest fire detection, unmanned vehicles and manufacturing industries (Ahuja et al. 2020; Rashid et al. 2016). Such IoT applications generate a huge amount of data that is usually stored at cloud to increase the usefulness of resources (Lin et al. 2019; Zhou et al. 2018). Sensor networks are integrated with cloud to improve the effectiveness of the application. This integration is termed as sensor cloud which is beneficial for both sensor networks and cloud. Various sensor networks store their sensed data at the cloud and cloud provides sensor as a service with help of virtualization to the multiple users according to their choice and demand. Any genuine end user can access the data of one or all authorized sensor networks just in one click with help of this integration (Dwivedi et al. 2018). Figure 1 presents a healthcare monitoring system where each human body behaves as a sensor network. Here, data from various wearable body sensors of many patients have been stored at cloud through base station such

DOI: 10.4018/IJCAC.2021070101

Figure 1. Healthcare monitoring sensor cloud



as mobile phone. Different types of authorized users viz., doctors, medical students, researchers can access the health records of the patients using their credentials. Doctors can provide medical support to the patients anytime and from anywhere. They can help the patients instantly if the emergency case is monitored. Cloud can provide sensor as a service to the authorized students and researchers too by providing them various types of data. Thus, legitimate end users can get data of one or more patients easily and quickly. Doctors, students, researchers and patients may belong to either same or different hospitals. In this way, everyone is benefitted with this sensor cloud integration.

There are several challenges to sensor cloud and security is one of them (Altaf et al. 2019; Díaz et al. 2016). Various security mechanisms have been devised to provide data security at the cloud (Park et al. 2011; Fernández-Alemán et al. 2013; Sangeetha et al.2017; Masood et al. 2018; Sun et al. 2018; Dwivedi et al. 2019). Some of them are less complex but have coarse grained access control. On the other hand, some schemes provide fine grained access control but they have some computational overheads. Hence, there is a need to provide an improved security mechanism having fine grained access control with reduced computational complexities. This paper focuses its work on sensor cloud of healthcare monitoring system. There are many medical cases in which the continuous monitoring of health conditions is required which allow doctors to know the health status of the patients regularly or when required (Ghoneim et al. 2018; Liu et al. 2019). Several computations may be involved before fetching the desired information (Goléa et al. 2019; Al-Ayyoub et al. 2018). IoT based healthcare system is very helpful in such situations which minimizes the healthcare treatment cost and allows the mobility of patients (Ko et al. 2010). In such systems, various body sensors are applied at the patients for the purpose of continuous monitoring of their health status. These body sensors are wearable devices worn by patients that can collect various body data such as blood pressure, body temperature and heart beat rate. Data collected by these sensors are sent to gateways via wireless communication medium and from gateways finally transferred to the cloud for storage and processing. Medical data of the patients collected by various body sensors are very crucial. Any alteration or loss in the medical data of the patients may result in negative health conditions or sometimes lead to very serious stages even death of the patient. Hence, it must be secured.

Therefore, a novel design is proposed in this paper to secure the sensor cloud data for healthcare applications. Proposed approach uses attribute based elliptic curve encryption technique that provides fine grained access control and allows only authentic users to have access on the healthcare records of the patients. This approach improves the encryption, decryption and key generation time as compared to the existing schemes namely Key Policy Attribute Based Encryption (KP-ABE) and Ciphertext Policy Attribute Based Encryption (CP-ABE). Thus, it enhances security with reduced computational complexities. It also ensures confidentiality, integrity, reliability, availability, scalability, authenticity and collusion resistance. The major contributions of the paper are given below:

- Design of a security mechanism called Attribute Based Elliptical Curve Cryptography (ABECC) for sensor cloud of health monitoring system
- Security analysis to justify the novelty of the proposed work
- Complexity analysis to justify the improvements in the proposed scheme

The rest of the paper is organized as follows. Section 2 focuses on preliminaries and background. Survey of the related work is done in section 3. Section 4 describes the proposed scheme ABECC. Section 5 presents performance evaluation where proposed approach is compared with the existing schemes on certain parameters. This section also presents various characteristics of ABECC. Finally, section 6 concludes the paper with a proposal for future work.

2. BACKGROUND

Before moving further, we present some preliminaries of the related work as follows:

2.1 Attribute Based Encryption (ABE)

In ABE, the cryptographic process is improved. It states that the identity of the recipient is not atomic but comprises of multiple attributes. Here, size of ciphertexts increases with the increase of number of attributes (Li et al. 2012; Muller et al. 2008). Attribute based encryption allows decryption of the ciphertext only if the receiver has the key of corresponding attributes. The security policies are defined on the set of given attributes using conjunctions, disjunctions etc. The complete set attributes is known as universal attributes set and the policy describing the authorization such as "who can access what", using conjunctions, disjunctions etc. is called access structure. Let us say that {M, N, O, P} is the set of attributes. User ABC has attributes {M, N} while user XYZ has attribute {P}. Now suppose if the file is encrypted with the policy $(M \wedge O) \vee P$. The file will be accessible only to user XYZ because his attribute satisfies the access policy and thus further can decrypt it. On the other hand, user ABC cannot either access or decrypt the file because its attributes does not satisfy the access policy. ABE provides the fine grained access control and can be of two types:

2.1.1. Key Policy ABE (KP-ABE)

In this approach, sender labels the ciphertexts with attributes and trusted authority issues private key of the user. Private keys are accompanied with the policies known as access structures which tell about the key holder and ciphertexts i.e. who could decrypt which ciphertexts (Wang 2013; Goyal et al. 2006).

2.1.2. Ciphertext Policy ABE (CP-ABE)

In this method, the user's private key is combined via group of attributes. Here, ciphertext specifies security policies on the attributes (Premkamal et al. 2020; Bethencourt et al. 2007).

2.2 Elliptical Curve Cryptography (ECC)

Both the sender and receiver must agree on the common elliptic curve equation in this cryptography. ECC is used in many applications viz., smart cards, wireless communication devices, web servers that handle several encryption sessions etc. ECC is a form of asymmetric cryptography like RSA, AES and ElGamal in which every user has public-private key pair. But, ECC uses shorter key lengths for the purpose of encryption and decryption than other cryptosystems (Saran et al. 2019; Athena et al. 2017; Bansal et al. 2017).

2.3 Coarse and Fine Grained Access Control

Sometimes user is imposed with low level authorization like he is authorized to a particular page or a service on basis of only his role (Carvalho et al. 2018). This type of authorization is called role based access control or coarse grained access control. If authorization level is high then it is known as fine grained access control. Above scenario with further authorization to the page and service results in fine grained access control. For example, user has constraints on role, gender and age etc to access the page. Similarly, he may have constraints on role, location, service timings, IP address etc to access the service. Thus, it can be observed that security is increased in fine grained access control (Sambrekar et al. 2019).

3. RELATED WORK

Tembhare et al. (2019) presented a scheme for maintaining privacy of patient's records in healthcare application of cloud. This scheme is the integration of ABE and role based access control policy. It is a novel approach with lower computational complexity but may suffer from role explosion because of growing number of various roles.

Sun et al. (2018) have designed a framework for searchable personal health records. This scheme is a combination of ABE and search encryption technology. It provides secure and efficient solution in cloud-fog environment. This method provides keyword search function with fine-grained access control but has lack of expressive search.

Perez et al. (2017) have devised a CP-ABE and symmetric key encryption based scheme for securing data in Internet of Things (IoT) contexts. It is focusing on healthcare application of IoT. Method is good because privacy is preserved and data sharing is secure. But it has some computational overheads in real contexts which can be further optimized.

Lounis et al. (2016) proposed a secure framework for data collection from body sensor networks which is based on CP-ABE. It provides an easy data sharing among healthcare professionals in normal and emergency situations. This scheme provides fine grained access control and ensures confidentiality, integrity, scalability.

Thilakanathan et al. (2014) had given a secure scheme to monitor as well as share health related data in cloud environment. They used ElGamal-based proxy re-encryption method for implementing the security. It handles large datasets and efficient user revocation in healthcare monitoring cloud. Limitation of this scheme is that it assumes that data sharing party is fully trusted.

Li et al. (2013) provided a security mechanism for securing the health records while sharing by using ABE. The framework described in this approach consists of pre-defined list of legitimate users. The list includes medical professionals as well as family members. Attributes based on roles are assigned to each user. The corresponding secret keys are retrieved from the authority and distributed to the users. Role based policy provide better key management facility to the users. Also, this framework is much more effective than the existing schemes because data owners need not to be online always in this approach.

Hung et al. (2012) have given a multi user data encryption scheme through multiple proxies instead of just single proxy. Separate storage and query keys are provided to every user. This makes the queries of a user to remain unrevealed to the other user. Storage and query keys can be changed by the user even without decrypting the complete database.

Tu et al. (2012) proposed revocation mechanism using CP-ABE which provides fine-grained access control. This paper addresses major problems of sharing the data in cloud as well as removing the access rights from the same user when he is not the part of the system concerned. This approach is very efficient in revoking the access rights from the users but not suitable for very large datasets.

Tran et al. (2011) gave a framework which states that same group users can access the data of each other. This helps in data sharing among the group members. There is a group administrator who is responsible for the revocation of group members. This framework uses proxy re-encryption where private key of data owner is divided into two halves. The first part is stored on the proxy through which the complete data is encrypted. The second part is kept in machine of data owner by which he encrypts the data. In this scheme, proxy may suffer excessive encryption and decryption operations.

Yang et al. (2011) introduced a generic scheme using attribute based encryption with proxy re-encryption to secure the sharing of data in cloud environment. This scheme provides fine grained access control. It is an efficient scheme in case of simple user revocation but fails when a revoked user joins again. Revocation of user does not cause key redistribution or data re-encryption.

Bethencourt et al. (2007) provided CP-ABE scheme. In this technique, several attributes specify user's private key and access policies are defined over the attributes which specifies that who can decrypt the data. If receiver satisfies these security policies then data will be available to the user. This design is secure against collusions but is proved secure.

Goyal et al. (2006) presented KP-ABE scheme in which ciphertexts are labeled with a number of attributes and private key is accompanied with access policies which control that a user can decrypt which ciphertexts. A user can decrypt the data if he satisfies the security policy. This technique provides fine grained access control but does not hide the set of attributes.

A summary of various existing security techniques used in sensor cloud is presented in Table 1. This table also describes the findings and limitations of the existing approaches. Earlier, many existing schemes use access control lists which provide coarse grained access to data. Later, ABE (KP-ABE / CP-ABE) has been used which provides fine grained access control, but it has some complex computations too which results in computational delay and other overheads. In order to reduce these complexities, there is a need to devise a security model to ensure the overall security of sensor data that guarantees the confidentiality and integrity and at the same time reducing the overall computational overheads with fine grained access control. This in turns makes the system more efficient.

4. PROPOSED APPROACH

This paper proposes a security mechanism termed as Attribute Based Elliptical Curve Cryptography (ABECC) which provides security with less computational overheads and fine grained access control.

Figure 2 describes sensor cloud architecture which incorporates the proposed security mechanism. There are four essential entities involved in this proposed approach viz., data consumer, security authority, cloud database and data owner. Healthcare monitoring system has various actors such as patient (P1, P2…Pz), relatives of patient (R1, R2…Rm), doctors (D1, D2…Dn), junior doctors (JD1, JD2…JDo), medical students (MS1, MS2...MSp), nurses (N1, N2...Nq), insurance company (IC1, IC2…ICr)) etc. These actors have various attributes like name, age, location, purpose etc. Here, patients are the data owners who are denoted at lower layer and other actors are the end users who are located at the upper layer of the system model. Middle layer of the model represents virtualization and security implementation at cloud. Security authority has information about the necessary attributes of data consumers which are obtained after their registration. The role for data owner is to collect the sensor data through various body sensors and also create role based policy on attributes provided by the security authority. Policies are created using conjunction or disjunction for the authentic data access which clearly states that who can access what. After this step, the data is encrypted through

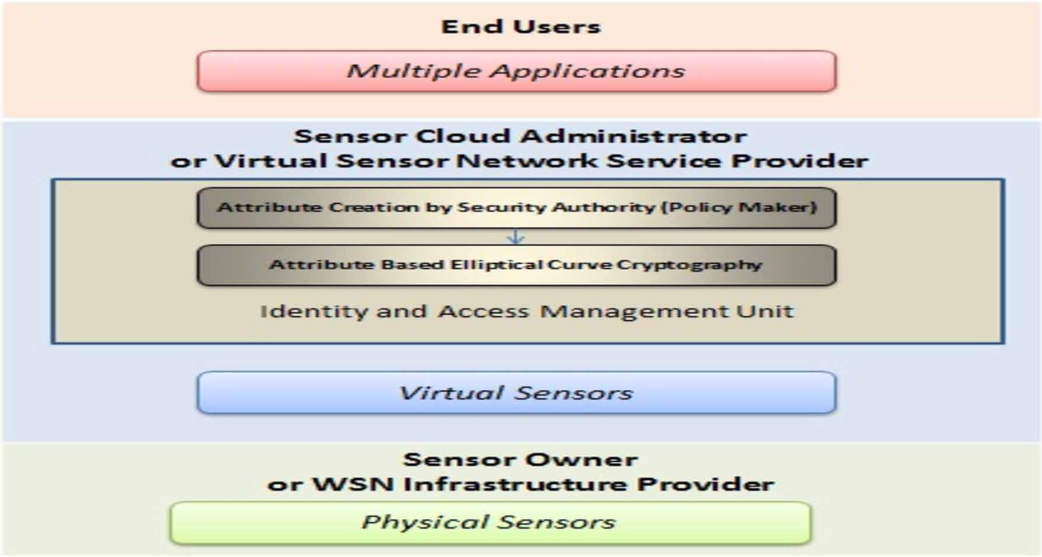
Table 1. Summary of security techniques used in sensor cloud

Authors (Year)	Technique Used	Findings	Limitations
Tembhare et al. (2019)	ABE with role based access control	Maintains privacy of patient's data in cloud with lower computational complexity	May suffer from role explosion because of growing number of various roles
Sun et al. (2018)	ABE with search encryption technology	Provides keyword search function with fine-grained access control	Lack of expressive search
Perez et al. (2017)	CP-ABE and symmetric key encryption	Privacy is preserved and data sharing is secure in healthcare application of IoT	Higher computational complexities in real contexts
Lounis et al. (2016)	CP-ABE based scheme	Provides fine grained access control and ensures confidentiality, integrity, scalability	Works for only single healthcare authority
Thilakanathan et al. (2014)	Proxy re-encryption with ElGamal encryption	Handles large data sizes and efficient user revocation in healthcare monitoring cloud	Assumes that data sharing party is fully trusted
Li et al. (2013)	ABE with role based access control	Supports dynamic modification of file attributes and security policy	Suffers from complex computational overheads in ABE
Hung et al. (2012)	Proxy re-encryption	Allows multiple users to access the shared database securely	More numbers of proxies are used
Tu et al. (2012)	CP-ABE based dual encryption system	Very efficient in revoking the access rights from the users	Not suitable for very large datasets
Tran et al. (2011)	Proxy re-encryption	Provides security and allows users to access another user's data who are in the same group	Proxy may suffer excessive encryption and decryption operations
Yang et al. (2011)	ABE with proxy re-encryption	Efficient scheme in case of simple user revocation	Fails when a revoked user joins again
Bethencourt et al. (2007)	CP-ABE	Secure against collusion attacks	Secure under generic group heuristic
Goyal et al. (2006)	KP-ABE	Fine grained access control	Does not hide the attributes

key provided by security authority and stored on the cloud. Only authentic data consumers whose attributes satisfies the security policy for selected file can decrypt the file with decryption key provided from security authority. This security model can serve various types of end users by providing them patients' data which can be obtained from multiple healthcare centers. This is possible because of virtualization at middle layer of sensor cloud integration. Proposed approach ABECC is described in Algorithm I. This algorithm is divided into two parts. First part explains "Attribute based policy creation for access control using ECC" and the second part describes "Authentication validation of end user to access the data".

```
Algorithm I.  Attribute Based Elliptical Curve Cryptography
(ABECC)
A.  Attribute based policy creation for access control using ECC
Begin
Step 1:  Data collection from various body sensors
Step 2:  Attribute are decided by security authority
```

Figure 2. Architecture of healthcare sensor cloud with proposed security scheme


End Users
Multiple Applications
Sensor Cloud Administrator
or Virtual Sensor Network Service Provider
Attribute Creation by Security Authority (Policy Maker)
Attribute Based Elliptical Curve Cryptography
Identity and Access Management Unit
Virtual Sensors
Sensor Owner
or WSN Infrastructure Provider
Physical Sensors

```
Step 3:  Role based policy creation on attributes by data owner
Step 4:  Data encryption using Elliptical Curve Cryptography (ECC)
Step 5:  Encrypted data is now ready for data processing at cloud
End;
B.   Authentication validation of end user to access the data
Begin
Step 1:  If (registered user) then
Step 2:   If (authenticated user: access policy is true) then
Step 3:     Decrypt data and allow user to view or download the
data
Step 4:   Else
Step 5:         Data access is not allowed
Step 6:  Else
Step 7:     Register to access the services
End;
```

5. PERFORMANCE EVALUATION

The work is implemented as a web application on x86_64 architecture based Intel core i7 processor with Windows 10 platform. We describe experimental setup as well as encryption, decryption and key generation time analysis in this section. Then we discuss some salient features of the proposed scheme.

5.1 Experimental Setup

ABECC is developed as a web application which consists of patients' health data. This application is deployed in cloud using virtualization. The proposed system has four modules namely Security Authority, Data Owner, Data Consumer and Cloud Database which are implemented through a web application in .NET framework. For cloud storage, the model uses Microsoft Azure SQL database. Encryption, Decryption and Key Generation Time are used as performance metrics. Table 2 presents the summary of the implementation setup.

Table 2. Implementation environment

Category	Implementation
IDE used	Visual Studio
Framework	Microsoft .NET
Front end	C#, ASP.NET
Back end	SQL Server
File size	100KB to 500KB
Number of attributes	2 to 10
Modules involved Performance Metrics	Security Authority, Data Owner, Data Consumer, Cloud Database
	Encryption, Decryption and Key Generation Time

5.2 Security Analysis

Proposed approach ABECC provides security with fine grained access control. The various security services of ABECC scheme such as data confidentiality, integrity, authenticity, availability, scalability, collusion resistance and reliability are discussed as follows:

5.2.1. Fine Grained Access Control

ABECC guarantees fine grained access control of records stored at the cloud. This access control is achieved due to use of ABE in the proposed scheme.

5.2.2. Data Confidentiality

Users who don't have the required attributes are not allowed to access the data. In this way, the proposed framework of ABECC guarantees the data confidentiality.

5.2.3. Integrity and Authenticity

A user authenticates any information obtained by the other user and then access is granted. Thus, proposed methodology ensures integrity of healthcare information during message communication.

5.2.4. Collusion Resistance

The approach ensures that users do not collude with each other to have any illegal access. ABECC provides collusion resistance to prevent from any unauthorized access.

5.2.5. Reliability

Probability of data loss or leak is very less in the proposed scheme because the data owner controls the process of sharing and storing data. Thus, we can say that proposed scheme is highly reliable.

5.2.6. Scalability and Availability

Proposed model confirms availability of the service to authentic users as per the requirements. It is also robust to the access of large number of users concurrently.

5.3 Encryption, Decryption and Key Generation Time Analysis

Different files of size 100 KB to 500 KB which contain data from various medical sensors were used for evaluating the time needed for encryption, decryption and key generation by the proposed scheme (ABECC). Security policies were made for 2 to 10 number of attributes. First of all, numbers of attributes were fixed to 6 and results are obtained for various file sizes. Then file size is fixed to 300 KB and results are obtained on varying number of attributes. When comparison of ABECC is done with existing KP-ABE and CP-ABE schemes, it is found that ABECC produces better results at these three performance evaluation metrics.

5.3.1. Effect of File Size on Encryption, Decryption and Key Generation Time

Figure 3 presents the encryption time analysis for various file sizes with fixed number of attributes that is 6. It shows that encryption time taken by the proposed scheme (ABECC) is lower than the encryption time of existing security schemes (KP-ABE, CP-ABE). It is noticed that encryption time increases in all the three approaches when file size is increased but it is lowest in case of the proposed scheme. It is due to use of ECC which reduces the key length that in turns reduces the encryption time.

Figure 4 describes the decryption time analysis for different file sizes with fixed number of attributes that is 6. It can be found from the results that decryption time of ABECC is lesser than decryption time of existing security schemes (KP-ABE, CP-ABE). It is also observed that decryption time increases in all three mechanisms when size of file is increased but it is lowest in case of the proposed scheme. It is due to use of ECC which reduces the key length that in turns reduces the decryption time.

Figure 3. Effect of file size on encryption time analysis

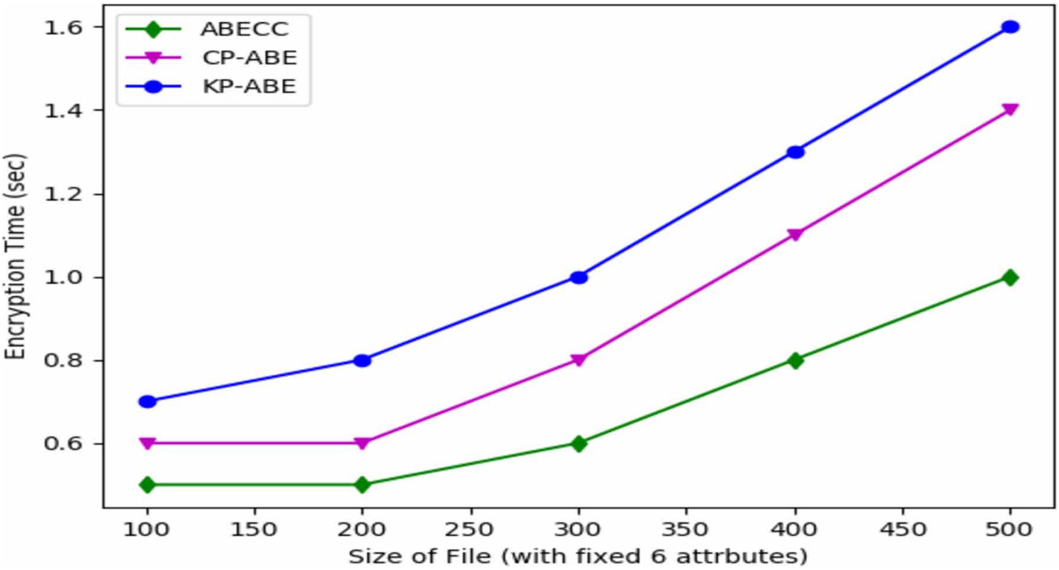


Figure 5 depicts the key generation time analysis for several file sizes with fixed number of attributes that is 6. Results show that key generation time of ABECC is also lower than key generation time of existing security mechanisms. It is also noticed that key generation time increases in all schemes presented here when file size is increased but it is lowest in case of the proposed scheme. It is due to use of ECC which reduces the key length that in turns reduces the key generation time.

5.3.2. Effect of Attributes on Encryption, Decryption and Key Generation Time

Figure 6 presents the encryption time analysis for numerous numbers of attributes with fixed file size of 300 KB. It shows that encryption time of ABECC is lower than that of existing KP-ABE and

Figure 4. Effect of File Size on decryption time analysis

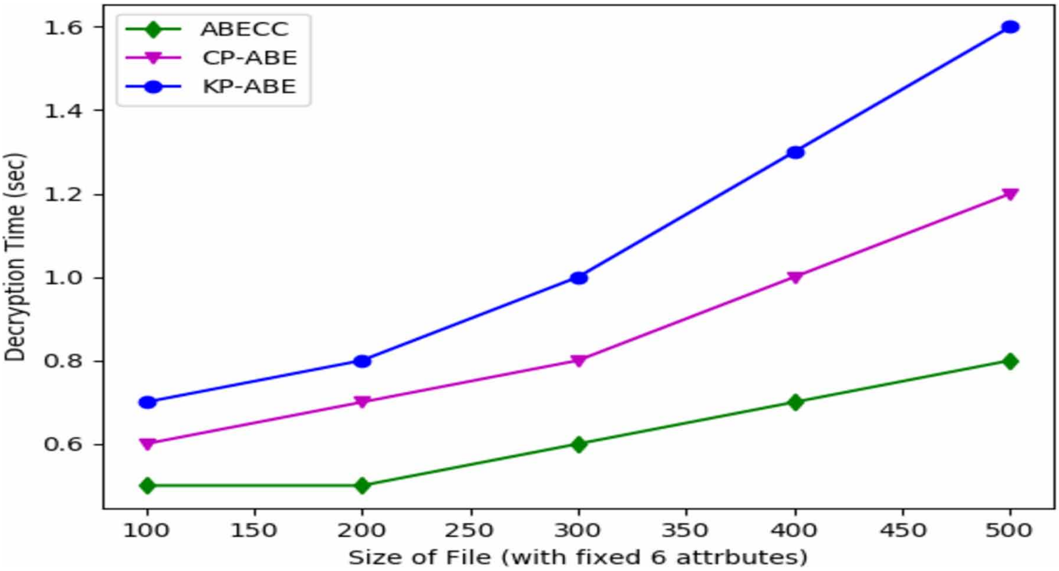
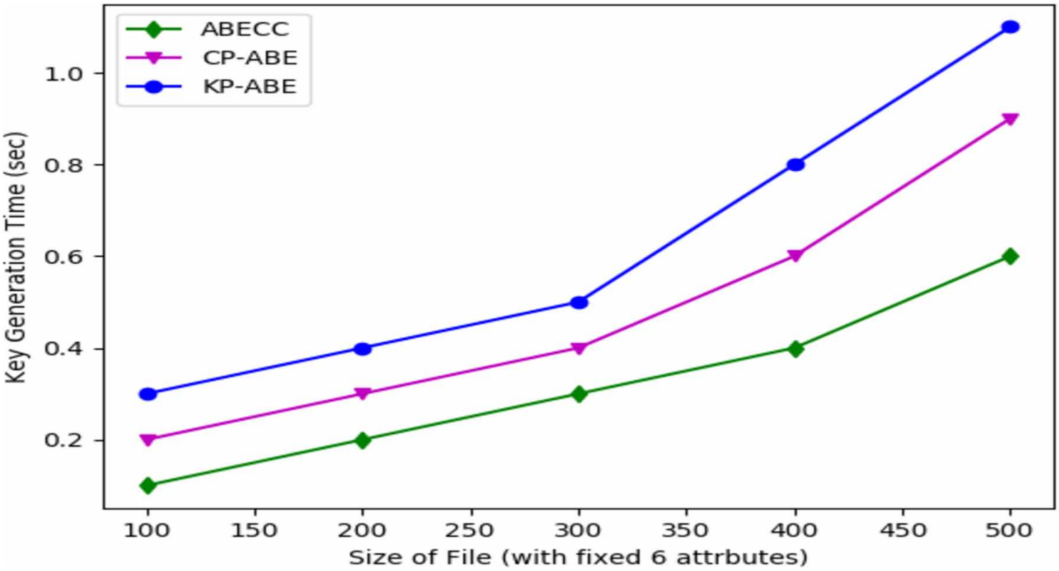


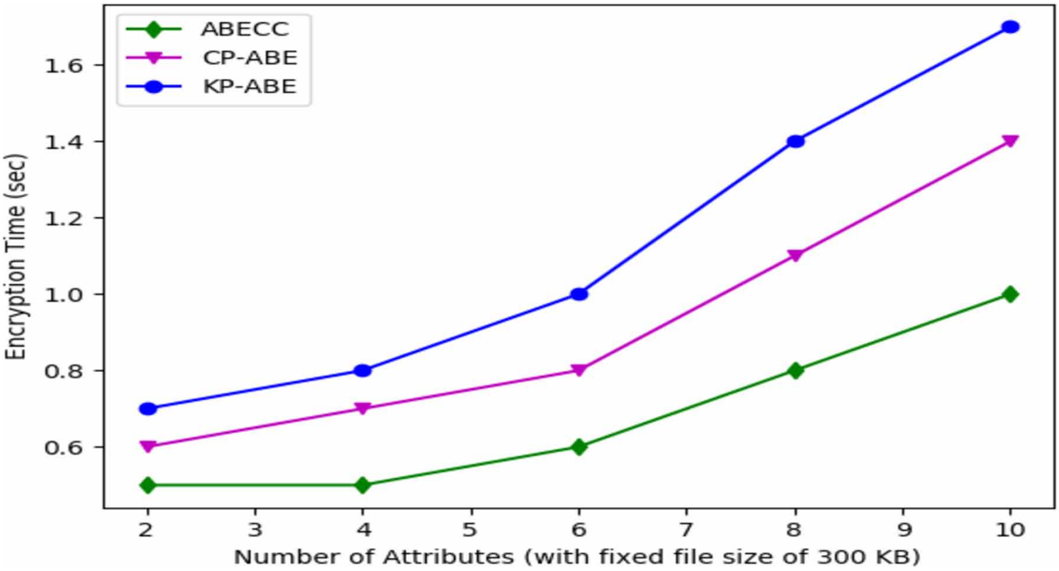
Figure 5. Effect of File Size on key generation time analysis



CP-ABE schemes. It can be seen that encryption time increases in all the three approaches when number of attributes is increased but it is lowest in case of the proposed scheme. It is due to use of ECC which reduces the key length that in turns reduces the encryption time.

Figure 7 describes the decryption time analysis for many numbers of attributes with fixed file size of 300 KB. It can be observed from the results that decryption time of the ABECC is lesser than that of KP-ABE and CP-ABE. It is also found that decryption time increases in all the three mechanisms

Figure 6. Effect of number of attributes on encryption time analysis



when number of attributes is increased but it is lowest in case of the proposed scheme. It is due to use of ECC which reduces the key length that in turns reduces the decryption time.

Figure 8 explains the key generation time analysis for a number of attributes with fixed file size of 300 KB. Results show that key generation time of ABECC is also lower than that of security mechanisms KP-ABE and CP-ABE. It is also noticed that key generation time increases in all the three schemes when number of attributes is increased but it is lowest in case of the proposed scheme. It is due to use of ECC which reduces the key length that in turns reduces the key generation time.

Figure 7. Effect of number of attributes on decryption time analysis

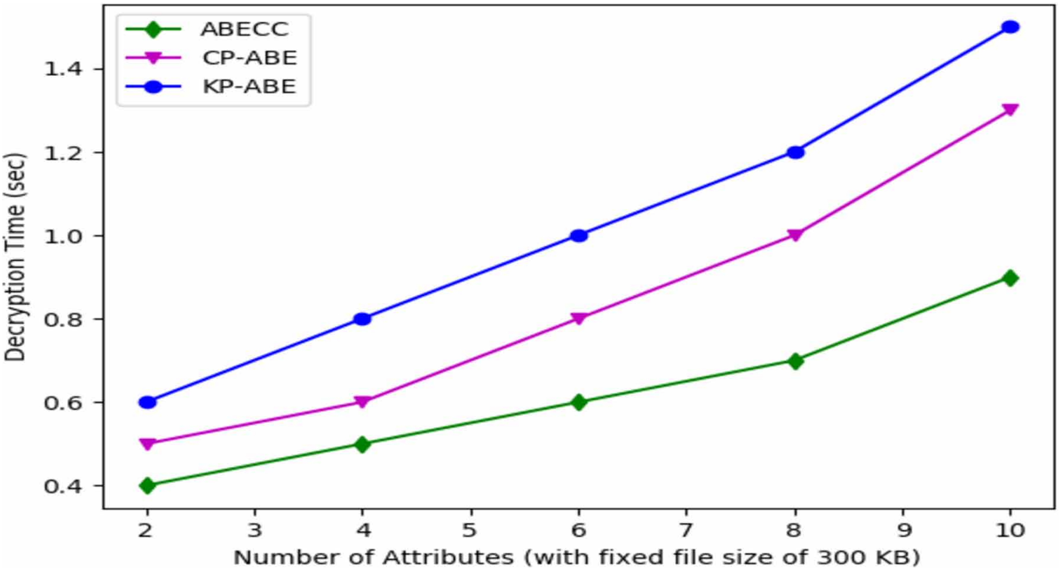
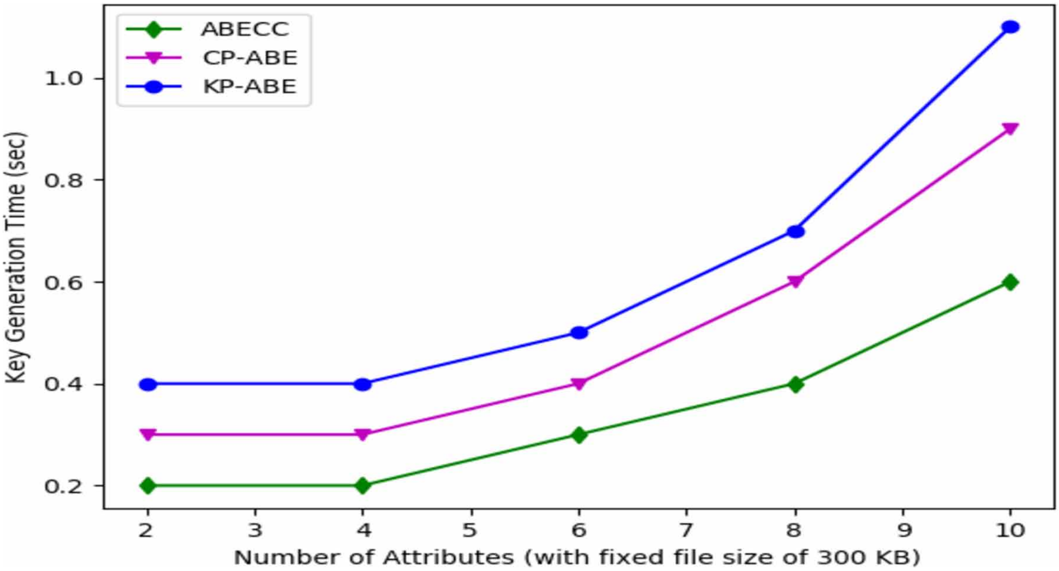


Figure 8. Effect of number of attributes on key generation time analysis



5.3.3. Discussion

Table 3 presents a comparative analysis which describes the effect of file size on encryption, decryption and key generation time. Here, attribute count is same and is equal to 6 for all cases. This analysis shows that proposed ABECC scheme performs better than existing security schemes.

Table 4 presents the comparative complexity analysis which describes the effect of number of attributes on encryption, decryption and key generation time with fixed file size of 300 KB. Here, it can be observed that proposed ABECC scheme outperforms the existing schemes.

5.4 Computational Overhead Analysis

Proposed approach ABECC ensures security with lower computational complexities as compared to the existing schemes (KP-ABE, CP-ABE). This is due to use of ECC which uses shorter key length. When we compute average encryption time of these schemes then we find that ABECC is 1.6 times and 1.3 times faster than the existing approaches of KP-ABE and CP-ABE respectively. Average decryption time computation shows that ABECC is 1.7 times and 1.4 times faster than these

Table 3. Comparative analysis to know effect of file size

Number of attributes with fixed size file (300KB)	**Encryption Time (sec)**			**Decryption Time (sec)**			**Key Generation Time (sec)**		
	KP-ABE	*CP-ABE*	*AB-ECC*	*KP-ABE*	*CP-ABE*	*AB-ECC*	*KP-ABE*	*CP-ABE*	*AB-ECC*
2	0.7	0.6	**0.5**	0.6	0.5	**0.4**	0.4	0.3	**0.2**
4	0.8	0.7	**0.5**	0.8	0.6	**0.5**	0.4	0.3	**0.2**
6	1.0	0.8	**0.6**	1.0	0.8	**0.6**	0.5	0.4	**0.3**
8	1.4	1.1	**0.8**	1.2	1.0	**0.7**	0.7	0.6	**0.4**
10	1.7	1.4	**1.0**	1.5	1.3	**0.9**	1.1	0.9	**0.6**

Table 4. Comparative analysis to know effect of number of attributes

Size of file (KB) with fixed attributes (6)	Encryption Time (sec)			Decryption Time (sec)			Key Generation Time (sec)		
	KP-ABE	*CP-ABE*	*AB-ECC*	*KP-ABE*	*CP-ABE*	*AB-ECC*	*KP-ABE*	*CP-ABE*	*AB-ECC*
100	0.7	0.6	**0.5**	0.7	0.6	**0.5**	0.3	0.2	**0.1**
200	0.8	0.6	**0.5**	0.8	0.7	**0.5**	0.4	0.3	**0.2**
300	1.0	0.8	**0.6**	1.0	0.8	**0.6**	0.5	0.4	**0.3**
400	1.3	1.1	**0.8**	1.3	1.0	**0.7**	0.8	0.6	**0.4**
500	1.6	1.4	**1.0**	1.6	1.2	**0.8**	1.1	0.9	**0.6**

existing approaches respectively. Similarly, computation of average key generation time indicates that ABECC is 1.9 times and 1.5 times faster than the same existing approaches respectively. Finally, on computing the average of total computational time for these approaches, we observe that proposed scheme ABECC is 1.7 times and 1.4 times faster than the existing approaches of KP-ABE and CP-ABE respectively. Thus, we can say that ABECC outperforms over the existing schemes.

5.4.1. Effect of File Size on Computational Complexity

Figure 9 presents the computational overhead analysis for various file sizes with fixed number of attributes that is 6. It shows that ABECC is on average 1.7 times and 1.4 times faster than the existing approaches of KP-ABE and CP-ABE respectively. This indicates that proposed scheme ABECC provides security with lesser computational overheads than the existing security schemes viz., KP-ABE and CP-ABE.

5.4.2. Effect of Number of Attributes on Computational Complexity

Figure 10 presents the effect of number of attributes on computational overheads with fixed file size of 300 KB. It shows that ABECC is on average 1.7 times and 1.4 times faster than the existing approaches of KP-ABE and CP-ABE respectively. Thus, it can be observed that that ABECC offers security with lesser computational overheads than the existing security schemes viz., KP-ABE and CP-ABE.

5.5 Novelty and Merits of ABECC

This manuscript proposes a novel security model viz., ABECC for providing security in the healthcare sensor cloud with lower computational overheads than the existing security schemes. ABECC uses attribute based elliptic curve encryption technique to design its security model. This approach offers fine grained access control that means a better security than the coarse grained access control. This approach improves the encryption, decryption and key generation time as compared to the existing schemes (KP-ABE and CP-ABE). Thus, it enhances security and reduces the computational overheads. It also ensures confidentiality, integrity, reliability, availability, scalability, authenticity and collusion resistance of the system. ABECC is a security scheme proposed for the healthcare information system. However, the core engine of this security model is also useful to various other industrial as well as non-industrial IoT and sensor cloud applications such as smart building, smart city, smart automotive manufacturing, smart agriculture, forest fire information system and military applications. Thus, we can say that ABECC is a novel security scheme and it has several advantages over the existing security schemes.

Figure 9. Effect of file size on computational overhead

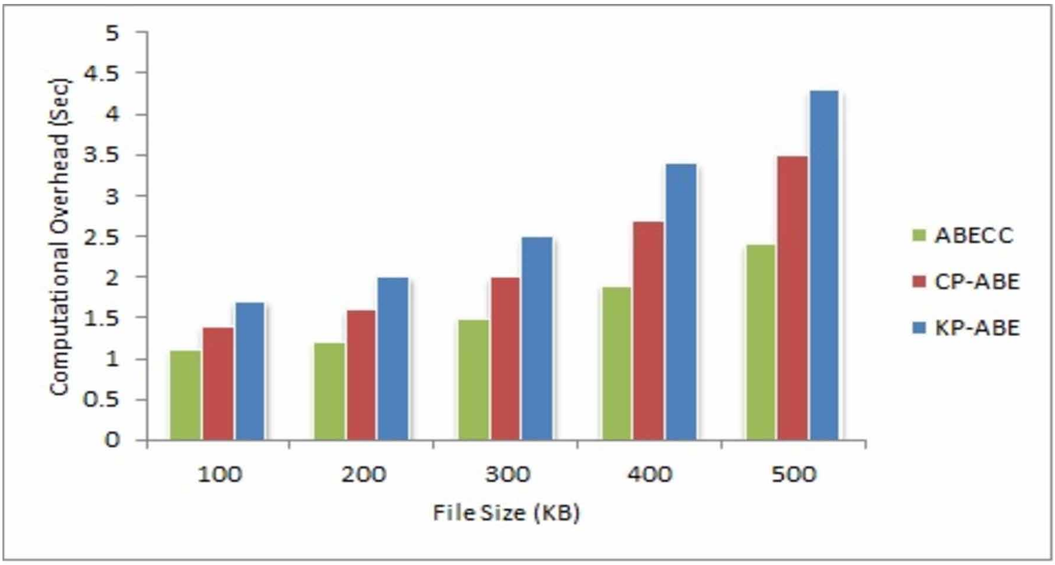
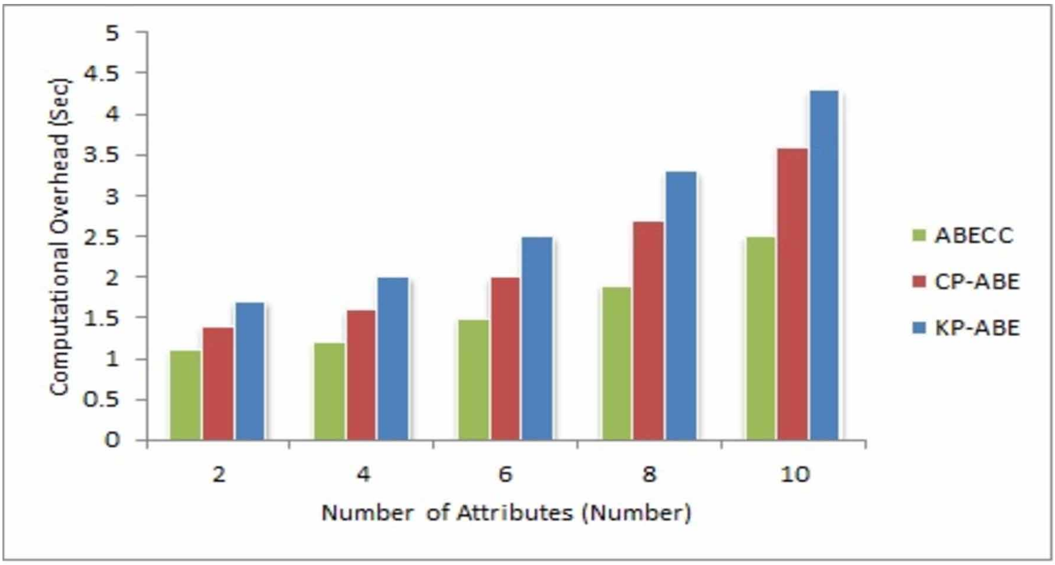


Figure 10. Effect of number of attributes on computational overhead



6 CONCLUSION AND FUTURE WORK

To implement dynamic and advanced security policies on patient’s health records in any medical application, a novel design ABECC is devised in this paper which secures the healthcare data of patients in sensor cloud environment. The proposed security model encrypts sensor data on the basis of some access policies and users having the specified policies can decrypt that data. Here, an attribute based scheme is developed with elliptic curve cryptography (ECC) to maintain privacy of patient's data. Use of ECC reduces the key length that causes better performance. Results prove that ABECC outperforms the existing schemes KP-ABE and CP-ABE. ABECC provides security with improved efficiency and lower computational overheads. It makes the process 1.7 times and 1.4 times faster than the existing approaches of KP-ABE and CP-ABE respectively. It also ensures fine grained access control and offers confidentiality, integrity, authenticity, reliability, availability, scalability and collusion-resistance. This approach can cater the needs of multiple kinds of users and researchers by providing data that is obtained from several wearable sensors of patients from same or different healthcare centers. This is possible due to sensor cloud integration and virtualization.

In future, this work can be extended with more advanced constraints on access policies. This model can be made more secure and robust for very large datasets. Further, this technique could also be used in various other IoT and sensor cloud applications viz., agricultural IoT, industrial IoT, smart city, smart building, smart farming system, underground applications, underwater monitoring system, forest fire detection system and military applications. We can impose some application specific constraints too in the security schemes of such applications.

ACKNOWLEDGMENT

This research is partially funded by Technical Education Quality Improvement Program (TEQIP III).

REFERENCES

Ahuja, S. P., & Wheeler, N. (2020). Architecture of Fog-Enabled and Cloud-Enhanced Internet of Things Applications. *International Journal of Cloud Applications and Computing, 10*(1), 1-10.

Al-Ayyoub, M., AlZu'bi, S., Jararweh, Y., Shehab, M. A., & Gupta, B. B. (2018). Accelerating 3D medical volume segmentation using GPUs. *Multimed Tools Appl, Springer*, *77*(4), 4939–4958. doi:10.1007/s11042-016-4218-0

Altaf, A., Abbas, H., Iqbal, F., & Derhab, A. (2019). Trust models of internet of smart things: A survey, open issues, and future directions. *Journal of Network and Computer Applications, Elsevier*, *137*, 93–111. doi:10.1016/j.jnca.2019.02.024

Athena, J., Sumathy, V., & Kumar, K. (2017). An identity attribute–based encryption using elliptic curve digital signature for patient health record maintenance. *International Journal of Communication Systems, Wiley*, *31*(2), 1–22.

Bansal, A., & Agrawal, A. (2017). Providing security, integrity and authentication using ECC algorithm in cloud storage. *IEEE International Conference on Computer Communication and Informatics - ICCCI 2017*, 1-5. doi:10.1109/ICCCI.2017.8117749

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, 321-334. doi:10.1109/SP.2007.11

Carvalho, M. A. Jr, & Bandiera-Paiva, P. (2018). Health Information System Role-Based Access Control Current Security Trends and Challenges. *Journal of Healthcare Engineering*, 1–8.

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications, Elsevier*, *67*, 99–117. doi:10.1016/j.jnca.2016.01.010

Dwivedi, R. K., & Kumar, R. (2018). Sensor Cloud: Integrating Wireless Sensor Networks with Cloud Computing. *5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering – UPCON 2018*, 820-825. doi:10.1109/UPCON.2018.8597008

Dwivedi, R. K., Saran, M., & Kumar, R. (2019). A Survey on Security over Sensor-Cloud. *9th IEEE International Conference on Cloud Computing, Data Science & Engineering – Confluence 2019*, 31-37. doi:10.1109/CONFLUENCE.2019.8776897

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. A. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562.

Ghoneim, A., Muhammad, G., Amin, S. U., & Gupta, B. (2018). Medical Image Forgery Detection for Smart Healthcare. *IEEE Communications Magazine*, *56*(4), 33–37. doi:10.1109/MCOM.2018.1700817

Goléa, N. E., & Melkemi, K. E. (2019). ROI-based fragile watermarking for medical image tamper detection. *International Journal of High Performance Computing and Networking, 13*(2), 199–210. doi:10.1504/IJHPCN.2019.097508

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of CCS'06*, 89-98. doi:10.1145/1180405.1180418

Hung, N. T., Giang, D. H., Keong, N. W., & Zhu, H. (2012). Cloud-enabled data sharing model. *IEEE International Conference on Intelligence and Security Informatics*, 1-6.

Ko, J. G., Lu, C., Srivastava, M. B., Stankovic, J. A., Terzis, A., & Welsh, M. (2010). Wireless Sensor Networks for Healthcare. *Proceedings of the IEEE*, *98*(11), 1947–1960. doi:10.1109/JPROC.2010.2065210

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*, *24*(1), 131–143. doi:10.1109/TPDS.2012.97

Lin, H., Yan, Z., & Fu, Y. (2019). Adaptive security-related data collection with context awareness. *Journal of Network and Computer Applications, Elsevier*, *126*, 88–103. doi:10.1016/j.jnca.2018.11.002

Liu, H., Guo, Q., Wang, G., Gupta, B. B., & Zhang, C. (2019). Medical image resolution enhancement for healthcare using nonlocal self-similarity and low-rank prior. *Multimed Tools Appl, Springer*, *78*(7), 9033–9050. doi:10.1007/s11042-017-5277-6

Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2016). Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Future Generation Computer Systems, Elsevier*, *55*, 266–277. doi:10.1016/j.future.2015.01.009

Masood, I., Wang, Y., Daud, A., Aljohani, N. R., & Dawood, H. (2018). Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure. *Wireless Communications and Mobile Computing*, 1–23.

Muller, S., Katzenbeisser, S., & Eckert, C. (2008). Distributed Attribute-Based Encryption. *Proceedings of Springer International Conference on Information Security and Cryptology ICISC 2008*, 20-36.

Park, N. (2011). Secure Data Access Control Scheme Using Type-Based Re-encryption in Cloud Environment. In Semantic Methods for Knowledge Management and Communication. Springer. doi:10.1007/978-3-642-23418-7_28

Pérez, S., Rotondi, D., Pedone, D., Straniero, L., Núñez, M. J., & Gigante, F. (2017). Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts. In *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. Springer.

Premkamal, P. K., Pasupuleti, S. K., & Alphonse, P.J.A. (2020). Efficient Escrow-free CP-ABE with Constant Size Ciphertext and Secret Key for Big Data Storage in Cloud. *International Journal of Cloud Applications and Computing, 10*(1), 28-45.

Rashid, B., & Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *Journal of Network and Computer Applications, Elsevier*, *60*, 192–219. doi:10.1016/j.jnca.2015.09.008

Sambrekar, K., & Rajpurohit, V. S. (2019). Fast and Efficient Multiview Access Control Mechanism for Cloud Based Agriculture Storage Management System. *International Journal of Cloud Applications and Computing, 9*(1), 33-49.

Sangeetha, D., & Vaidehi, V. (2017). A secure cloud based personal health record framework for a multi owner environment. *Annals of Telecommunications, 72*(1-2), 95–104. doi:10.1007/s12243-016-0529-4

Saran, M., Dwivedi, R. K., & Kumar, R. (2019). Attribute Based Elliptic Curve Encryption for Security in Sensor-Cloud. *2nd Springer International Conference on Data & Information Sciences – ICDIS 2019*, 1-11.

Sun, J., Wang, X., Wang, S., & Ren, L. (2018). A searchable personal health records framework with fine-grained access control in cloud-fog computing. *PLoS One*, *13*(11), 1–23. doi:10.1371/journal.pone.0207543 PMID:30496194

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review. *Security and Communication Networks*, 1–9.

Tembhare, A., Sibi Chakkaravarthy, S., Sangeetha, D., Vaidehi, V., & Venkata Rathnam, M. (2019). Role-based policy to maintain privacy of patient health records in cloud. *The Journal of Supercomputing, 11227*, 1-16.

Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., & Alem, L. (2014). A platform for secure monitoring and sharing of generic health data in the Cloud. *Future Generation Computer Systems, Elsevier*, *35*, 102–113. doi:10.1016/j.future.2013.09.011

Tran, D. H., Nguyen, H. L., & Zha, W. (2011). Towards security in sharing data on cloud based social networks. *8th IEEE International conference on information, communications and signal processing*, 1–5. doi:10.1109/ICICS.2011.6173582

Tu, S., Niu, S., Li, H., Xiao-ming, Y., & Li, M. (2012). Fine-grained access control and revocation for sharing data on clouds. *26th international parallel and distributed processing symposium workshops and PhD forum,* 2146–2155. doi:10.1109/IPDPSW.2012.265

Wang, C., & Luo, J. (2013). An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length. *Mathematical Problems in Engineering*, 1–7.

Yang, Y., & Zhang, Y. (2011). A Generic Scheme for Secure Data Sharing in Cloud. *40th IEEE International Conference on Parallel Processing Workshops*, 145-153. doi:10.1109/ICPPW.2011.51

Zhou, D., Yan, Z., Fu, Y., & Yao, Z. (2018). A survey on network data collection. *Journal of Network and Computer Applications, Elsevier*, *116*, 9–23. doi:10.1016/j.jnca.2018.05.004

Rajendra Kumar Dwivedi is Assistant Professor in the Department of Information Technology and Computer Applications at Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.), India. He joined this institute in 2009. He received his B. Tech Degree in 2004 from Pt Ravishanker Shukla University, Raipur and M.Tech. from Indian Institute of Technology, Roorkee in 2015. Currently, he is pursuing his Ph.D. from Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.). Before joining MMM Engineering College (under state government of U.P.), he worked in K.V. Lansdowne U.K. (under central government of India). He has supervised a large number of M. Tech. students. He has published a large number of research papers in various international and national journals and conferences of high repute (h-index=9, i-10 index=9, citations=241). He is a member of IEEE and also life member of Institution of Engineers (India). His main research interests lie in Wireless sensor networks, Network security, Cloud computing and Machine learning.

Rakesh Kumar is Professor in the Department of Computer Science and Engineering at Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.), India. He received his B. Tech. Degree in 1990 from MMM Engineering College, Gorakhpur and M.E. from SGS Institute of Technology and Science, Indore in 1994. He did his Ph.D. from Indian Institute of Technology, Roorkee in 2011. Before joining MMM Engineering College, he worked in HBTI Kanpur and BIET Jhansi. He was also the principal investigator of a major research project sanctioned from University Grant Commission, New Delhi, India. Dr. Kumar has supervised a large number of M. Tech. Dissertations and guiding several Ph.D. students. He has published a large number of research papers in various international and national journals and conferences of high repute (h-index=13, i-10 index=19, citations=687). He is a member of IEEE, life member of CSI, ISTE and also a Fellow of IETE and Institution of Engineers (India). His main interests lie in mobile ad hoc network, MANET- Internet integration, Sensor network, Network security, Cloud computing and Machine learning.

Rajkumar Buyya is a Redmond Barry Distinguished Professor and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at the University of Melbourne, Australia. He is also serving as the founding CEO of Manjrasoft, a spin-off company of the University, commercializing its innovations in Cloud Computing. He served as a Future Fellow of the Australian Research Council during 2012-2016. He has authored over 625 publications and seven text books including "Mastering Cloud Computing" published by McGraw Hill, China Machine Press, and Morgan Kaufmann for Indian, Chinese and international markets respectively. He also edited several books including "Cloud Computing: Principles and Paradigms" (Wiley Press, USA, Feb 2011). He is one of the highly cited authors in computer science and software engineering worldwide (h-index=145, i-10 index=609, g-index=307, 111924+ citations). "A Scientometric Analysis of Cloud Computing Literature" by German scientists ranked Dr. Buyya as the World's Top-Cited (#1) Author and the World's Most-Productive (#1) Author in Cloud Computing. Dr. Buyya is recognized as a "Web of Science Highly Cited Researcher" for three consecutive years since 2016, a Fellow of IEEE, and Scopus Researcher of the Year 2017 with Excellence in Innovative Research Award by Elsevier and recently (2019) received "Lifetime Achievement Awards" from two Indian universities for his outstanding contributions to Cloud computing and distributed systems. Software technologies for Grid and Cloud computing developed under Dr. Buyya's leadership have gained rapid acceptance and are in use at several academic institutions and commercial enterprises in 40 countries around the world. Dr. Buyya has led the establishment and development of key community activities, including serving as foundation Chair of the IEEE Technical Committee on Scalable Computing and five IEEE/ACM conferences. These contributions and international research leadership of Dr. Buyya are recognized through the award of "2009 IEEE Medal for Excellence in Scalable Computing" from the IEEE Computer Society TCSC. Manjrasoft's Aneka Cloud technology developed under his leadership has received "2010 Frost & Sullivan New Product Innovation Award". Recently, Dr. Buyya received "Mahatma Gandhi Award" along with Gold Medals for his outstanding and extraordinary achievements in Information Technology field and services rendered to promote greater friendship and India-International cooperation. He served as the founding Editor-in-Chief of the IEEE Transactions on Cloud Computing. He is currently serving as Co-Editor-in-Chief of Journal of Software: Practice and Experience, which was established ~50 years ago. For further information on Dr.Buyya, please visit his cyberhome: www.buyya.com.