International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Cryptography in cloud: An in-depth investigation into encryption mechanisms for safeguarding cloud-based data

Malathi P [1,*], Suganthi Devi S [2] and Jospin Jeya J [3]

[1] *Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, India.*
[2] *Department of Computer Science and Engineering, Annamalai University, Tamilnadu. India*
[3] *Department of Computer Science and Engineering, SRM Institute of science and Technology, Ramapuram Campus. India*

International Journal of Science and Research Archive, 2024, 11(01), 1635–1645

Publication history: Received on 23 December 2023; revised on 06 February 2024; accepted on 08 February 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.1.0188

Abstract

Cloud computing is one of the most significant computing models, which provides easy access of resources. It is an alternative for costlier data framework and networking models. The services are provided to the data users based on their requirements. More industries are depending on the cloud, because of its fast computations and robust nature. However, there are several security concerns and threats in cloud storages. Moreover, large amounts of data are shared between people and organizations through the cloud. The data owner doesn't have control over the data in the cloud. To address the security and privacy issues in the cloud, this thesis aims at overcoming this trade-off, while considering security.

Keywords: Cloud Computing; Attribute Based Encryption; Advanced Encryption Standard; Networking Model

1. Introduction

In cloud computing, services such as data storage, databases and networking are delivered to the Data Users (DU's) through the internet by the service providers. Instead of storing the user's files on a local personal storage device, it is saved in a remote database. Cloud-based storage provides the ability to save the files on the remote database which is connected through the internet. If the electronic device has access to the internet, it can establish the entrance to the remote database and the software applications to operate it [1]. There is a serious problem concerned with privacy and security in cloud computing because the Cloud Service Provider (CSP) can access the data in the cloud at any time. CSP could inadvertently or deliberately alter or delete the data. CSP may share the data with third parties if required. Hence there is a possibility of unauthorized persons accessing the data. To avoid this, the Data Owner (DO) can encrypt the data and store the ciphertext in the cloud [2]. Though there are a number of cryptographic techniques available in the literature, the following techniques are used in the proposed work to develop new cryptographic algorithms. They are symmetric key cryptography, asymmetric key cryptography and Attribute Based Encryption techniques.

2. Cloud computing

The term "cloud" refers to a set of hardware, networks, applications, and interfaces that enables computing services. According to The National Institute of Standards and Technology, cloud computing [3] is defined as a ubiquitous, suitable, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or CSP interaction. There are five defining characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [4]. Cloud computing is a fast-developing computing method that substitutes static and expensive data models,

* Corresponding author: Malathi P

network patterns and software framework with adaptive reliable cloud-based models that are provided by third party service providers. Cloud computing applications or software act as front end, back end and cloud-based delivery. Front end matches to the client side and back-end matches to the resources used by servers. Through the internet, cloud computing delivers different services using some specific tools and applications like data storage, servers, databases, networking, and software instead of utilizing the data processing with limited resources in an organization. Cloud computing is used for sharing resources such as software, storage and hardware which are available in a data center to many data users.

3. Literature survey

This Section presents several cryptographic techniques in cloud computing that are developed for secure sharing of data. Because of scalability and pay-per-use, a growing number of businesses and individuals are beginning to use the cloud. Security and privacy issues are predominated in the cloud. Most of the existing traditional cryptographic techniques do not support fine grained access control.

Identity Based Encryption (IBE) was the first step towards ABE. There is no need to access the public key certificate by using IBE since the owner encrypts the message to an identity. This decreases the transmission overhead and makes certificate management easier [5]. Using the Trusted Third Party (TTP), the secret keys are generated based on the user's identity, such as email address and DOB. If TTP is compromised, the entire system is collapsed or hacked. User privacy is not preserved using IBE scheme. Sahai and Waters extended the new IBE scheme called Fuzzy Identity Based Encryption (FIBE), which considers identity as a collection of attributes.

Since the access control structure is connected to secret keys, encrypted data is transmitted. Access tree is defined by the data owner with the help of set of attributes. Monotonic access structure is constructed from the generated private key. The major drawback is data owner is unable to access the data. The security of the third party is important [6].

Expressive KP-ABE unauthorized data access from the cloud is tightly regulated. Increasing number of attributes increases the computing overhead. Waters [8] implemented the CP-ABE scheme, in which LSSS is used to express the access structure, which was previously addressed as a matrix over the attributes. The complexity of the access structure creates an impact on size of the ciphertext and it leads to computation overhead.

CP-ABE is developed in such a manner that the access structure and the encrypted data are not stored with cloud users with anonymous access policy. The key factor contains two random factors that support the cipher text elements and decryption process. Further, Multi-Authority CP-ABE [7] is developed with standard cipher text length for securing user data privacy, providing access control and standard cipher-text length. The model used hidden access policy, in which the attackers could not store the private data through the access model. Moreover, the number of encryption functions and decryption operations using bilinear pairing are pre-defined.

William [8] introduced the multi-authority ABE scheme that uses multiple authorities to resolve the issues of single authority is proposed. In most authority schemes, the various accounting authorities release different personal information of the users and thus the credentials are controlled by different authorities. In the above scenario, the hospital provides each user with confidential private information related to the “Physician and medical researcher” provides each user with a private key related to the “Medical Researcher”.

Hierarchical Attribute Based Encryption (HABE) is formed by combining the HIBE and CP-ABE. This scheme involves in developing multi-level processing for key generation. There is hierarchical key generation in HIBE schemes, and a flexible access control mechanism in CP-ABE schemes. The CP-ABE scheme is used in the HABE scheme for access control. CP-ABE helps to gain the fine-grained access control over the cloud data [9].

In Extended version of CP-ASBE, data are stored in hierarchical manner. The attributes are also stored in different hierarchical in Hierarchical Attribute-Set- Based Encryption (HASBE) . Because of hierarchical structure, the proposed scheme has the advantage of providing scalability, but also inherits flexibility and fine- grained access control from existing ASBE attributes.

The files are encrypted in a different hierarchical layer with different access levels. So that the storage and time are effectively consumed under some standard assumptions. The secret key is generated based on the different hierarchical levels of attributes. The scheme is not cost effective [9].

Certificate-Less-Proxy Re-Encryption (CL-PRE) model has been developed for sharing the data in secure manner in the group of devices in public Cloud. In that model, the data before sharing on Cloud is encrypted using the symmetric key. Consequently, the symmetric algorithm is used to provide security for data owner's public key. Both keys are provided to the cloud for re-encryption and decryption process. Moreover, the re-encryption is processed with the bilinear pairings, some computational complexities. For reducing the computational complexities in bilinear pairings, the authors [10] developed a mediated certificate-less model. The model framed key pair comprises public and private key for all the participating users in the Cloud and transmits the public-key to all devices. The process of decryption is initiated at the user side. In security point of view, the generated key is provided to multiple users. The decryption process is performed twice for acquiring the original content.

Personal Health Record (PHR) is shared in cloud and maintained by TTP or CSP. Since medical data are stored in cloud it leads to several security issues from the untrusted third-party servers. For ensuring security, the PHR's are encrypted. Multiple data owners are used to secure the data which is shared in cloud. Another model [11], Online PHR sharing model acquired the data access over cloud. But the model supported single owner scenarios. In, the risks on sharing data over cloud and the security measures were discussed for solving those issues. A novel security model by integrating symmetric key techniques and steganography is presented here. The authors deployed some symmetric key models to provide user-data block-wise security, such as, Advanced Encryption Standard, RC6 (Rivest Cipher 6) and Blowfish.

A new cloud service model called Encryption as a Service has been defined in [12] for solving the security risks between the cloud user and CSP. The simulation used for computation is Eucalyptus Private Cloud with MAC. The efficiency is measured with time of encryption and decryption, varying file sizes. Key management problems are given in future work. A novel model SecCloud is developed by combining computation auditing and secure storage model for assuring privacy with signature verification, probabilistic sampling model and batch verification. Moreover, computational overhead and effectiveness of model is measured. The computational cost is also measured with subsequent model evaluation, pairing time and multiplication time.

A valuable survey work is presented in the secure cloud storage models and cryptographic standards. The survey work begins with the cloud model, and cryptographic techniques such as ABE, searchable encryption, broadcast model, IBE, group encryption and so on. Those models are incorporated in cloud model to perform cryptographic executions. Furthermore, the authors of [13] developed a novel technique for solving the issues over lightweight cloud data storage. Additionally, the RSA algorithm is modified to produce large prime values. AES and modified RSA are combined to frame integrated security model to support data security.

An effective review work presented in discusses about the data storage and retrieval techniques in the cloud in secure manner. Considering the factors such as security model, model functionality and query efficiency, the different techniques for key word search are used. Since the secure data sharing is essential, user revocation and key sharing model are discussed. Additionally, the data sharing techniques such as proxy encryption, Sirius, etc are also discussed [14].

Secure multi-owner data sharing method is proposed. The RSA-CRT (RSA-Chinese Remainder Theorem) and index generation model are used. The user revocation list is used, keys are stored and managed by the authorized authorities. The scheme minimizes the storage overhead. The results are compared with wild-card fuzzy model. The work concludes by stating that the model is not efficient in handling multimedia files. A fine-grained data access model is presented for managing E-Health care records. The model user ABE based cipher text model and the model is evaluated with real-time data obtained from University of California, comprising 500-3000 patient records. Further, for supporting multiple senders and services, flexible search authorization model is developed in. The work also used fine grained data access control and synonym-based keyword searching technique based on bilinear pairing. Besides, the model provides assurance for data privacy and keywords without duplications. The work presented in formulates a model for secure cloud storage with AES and Fuzzy based keyword search model. Initially, the data is encrypted by the data owner and shared in the cloud. The following information is also stored on to the cloud: file, index and keyword. Finally, the fuzzy keyword is framed with the edit- distance technique and wild-card fuzzy method to retrieve the data.

Semantic keyword search model is proposed and explained in [15]. The work employs stemming model which is used to minimize the index dimensions. The efficiency of keyword search has been enhanced with the symbol-based tree model and the model is evaluated with the enron dataset based on factors such as stemming method, query processing and processing time. Another work in presents a secure keyword search model, in which the data are retrieved securely from cloud. Additionally, dual encryption is applied for enhancing data security. The data and keyword are encrypted with AES technique and outsourced to the cloud. The secret key of AES has been encoded using RSA and keyword

matching has been executed. The model is evaluated based on the time taken for encryption, decryption and storage overhead.

4. Summary

This chapter has discussed the various security factors, and methods for providing secure communications over cloud. It has been depicted from the above survey that there are several schemes for providing advanced security over the data transmission. Moreover, the previous works done for ABE, CP-ABE, single CPABE, Multi-Authority CP-ABE, ECC and HCC schemes are less secured. Still there is a requirement for tight security in the communication over cloud for ensuring the security of the shared data of owner through cloud environment.

5. Methodology

In survey, Elliptic Curve Cryptography (ECC) is discussed, which is a public-key cryptography is based on the algebraic structure of elliptic curves over finite fields. ECC requires a smaller key compared to some of the existing cryptographic techniques to provide equivalent security. The Diffie-Hellman key exchange is mainly used to establish a shared secret key that can be used for secure communication while exchanging data over a public network. It uses the elliptic curve points and gets the secret key, using the system security parameters. [13] proposed a new technology that improves the Diffie-Hellman algorithm and properties. The proposed scheme MA-CP-ABE is combined with Hyperbolic Curve Cryptography to enhance the data security in cloud. HCC is designed on a hyperbolic curve over a finite field. It has a solid Abel group structure whose order is diverse over a finite field.

6. Network model of ma-Cp-Abe with Hcc

In this section, Hyperbolic Curve Cryptography (HCC) is combined with MA-CP-ABE for enhancing the data security over the cloud. The network model of MA-CPABE with HCC contains the following elements:

- Data Owner (DO)
- Cloud Service Provider (CSP)
- Data User (DU)
- Attribute Authority (AA)
- Verification Authority (VA)

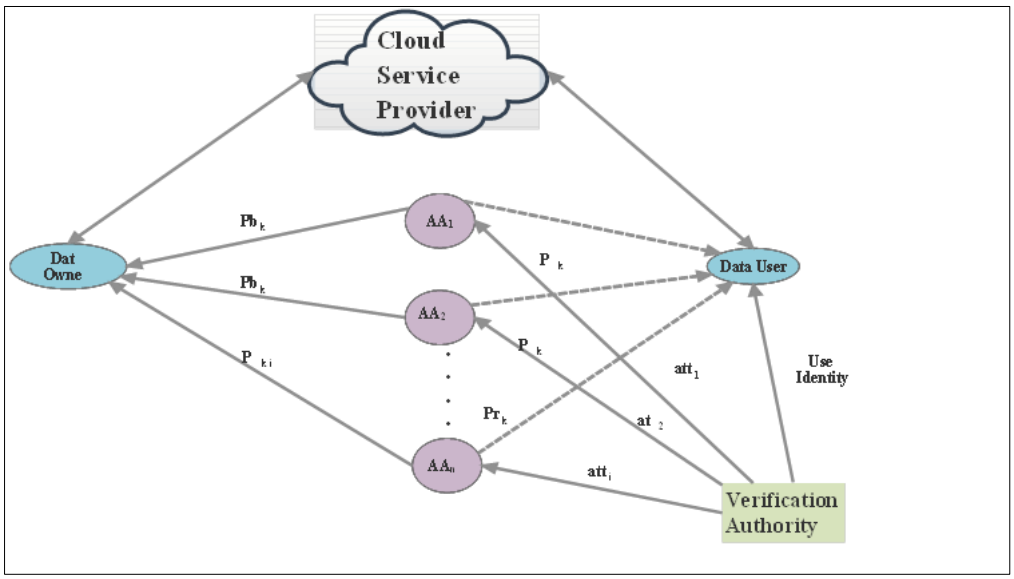

Figure 1 Network Model of MA-CP-ABE with HCC

The Data Owner is responsible for framing the attribute-based access policyand encrypting the data using MA-CP-ABE-HCC. The data or the message are assumedto be the hyperbolic curve points. The ciphertext is uploaded in the cloud by the data owner. The verification and the attribute authorities are responsible for the setup, key generation and key distribution process. When the data user wants to access the data inthe cloud, the attribute authority is responsible for

authenticating the data user based onthe attributes owned by the data user. The Data User downloads and decrypts the data only when the attributes match with the access policy framed by the data owner. The complete network model of MA-CP-ABE with HCC is presented in Figure 1.

7. Basic concepts

In this section, the basic system terminologies such as Multi-Authority Ciphertext Attribute Based Encryption (MA-CP-ABE), access structure, Hyperbolic Curve Cryptography and hyperbolic functions are presented.

7.1. Multi-Authority CP-ABE

In the proposed scheme, two authorities are assumed: the Attribute Authority (AA) and Verification Authority (VA). The Attribute Authority is responsible for the system setup and key generation. The Verification Authority is responsible for key generation and distribution and also provides fine grained access control.

7.2. Access Structure

A set $S \subseteq 2\ \{B1, \dots, Bn\}$ where 'B' is the group of attributes. The access tree contains non-empty sub-sets of $\{B1, \dots, Bn\}$ that is $S \subseteq 2\{B1, \dots, Bn\}$. The sets that are not presented in S are considered as authorized and the remaining are the un-authorized sets. Moreover, in the Attribute based encryption model, the access policy plays an important role in the process of key generation.

The access policy is generated based on the set of attributes and the boolean gates such as AND and OR. DO utilizes the access structure to develop the policy or the privilege based on the policy of the data attributes to provide access to the data that are shared over the paradigm. For instance, the boolean equation $A \vee (B \wedge C)$ denotes the data that can be utilized or decrypted when the user has the A or B and C.

8. Algorithm for MA-CP-ABE with HCC

In this model, MA-CP-ABE with HCC is effectively used for enhancing the data security and also for generating the public and secret key during the data transmission in the cloud.

Initialization

The coefficients for defining the vertices of the hyperbolic curve for the definite function (f) are:

Input

System security parameters

Output

B is a coordinate point on hyperbolic plane

The base point $(x0, y0)$ is fixed with large data order 'l' and the value is $Gl = T$. Select an integer 's', where $s < l$.

Compute

$B = Gs \bmod q$

In this model, HCC is effectively utilized for generating the public and secret key to secure the data communication on the cloud.

Encryption

Input

Coordinate points on the hyperbolic plane

Output

Encryption Points (X, Y)

Begin

Select the co-efficient for defining the hyperbolic curve with finite area function,

$$a2 - Fb2 = 1$$

Choose base point $G = (a0, b0)$ with large order 'l' that gives

$$Gl = E$$

Select an integer 'r', where, $r < l$ and Compute

$$D = Gr \; mod \; p$$

The public keys are generated by (G, D) and the private key is given as 'r' For encrypting the message 'M', Select secret integer 's'

Compute,

$$X = Gs \; mod \; n$$

$$Y = Ds \; M \; mod \; n$$

The generated cipher text (X, Y) is transmitted to cloud.

End For

End

The generated cipher text is sent to the cloud. When there is a data request from the data user, the authentication of the data user is verified by the authorities using MA-CP-ABE-HCC. Decryption of the data is done with the user's secret key based on the attributes. If the attribute does not match then the data user cannot download and decrypt the data from the cloud.

Decryption

The downloaded ciphertext (P, R) is decrypted by the data user, in which the receiver is required to perform the following operations.

Input: Encryption Points (X, Y)

Output: Decryption 'M'

Begin

Compute

$$L = Xr \; mod \; n$$

Recover

$$M = Y/L \; mod \; n$$

End

9. MA-CP-ABE based HCC

For performing the encryption with the HCC, the basic operations are explained in the following steps,

- A random integer 'k' is selected as the secret integer
- Derives
- $P = Gk \ mod \ n$
- $R = Bkw \ mod \ n$
- Computes the ciphertext (P, R)
- Transmits to the other end

In order to secure the data that are transmitted over the cloud platform, MA- CP-ABE is combined with HCC in this work. The data are given as, $d \rightarrow \{d1, d2, \ldots, dn\}$ by considering the attributes such as, $\{v1, v2, \ldots, vn\}$. The proposed model initially involves determining the user attributes and the attributes are needed to satisfy the public key 'X'. On obtaining the public key, the DU makes the request for the private key 'Y'. The data user is able to access the data that are stored over cloud, only when both the keys are obtained by them and verified by the authority. The system architecture of MA-CP-ABE with HCC is presented in Figure

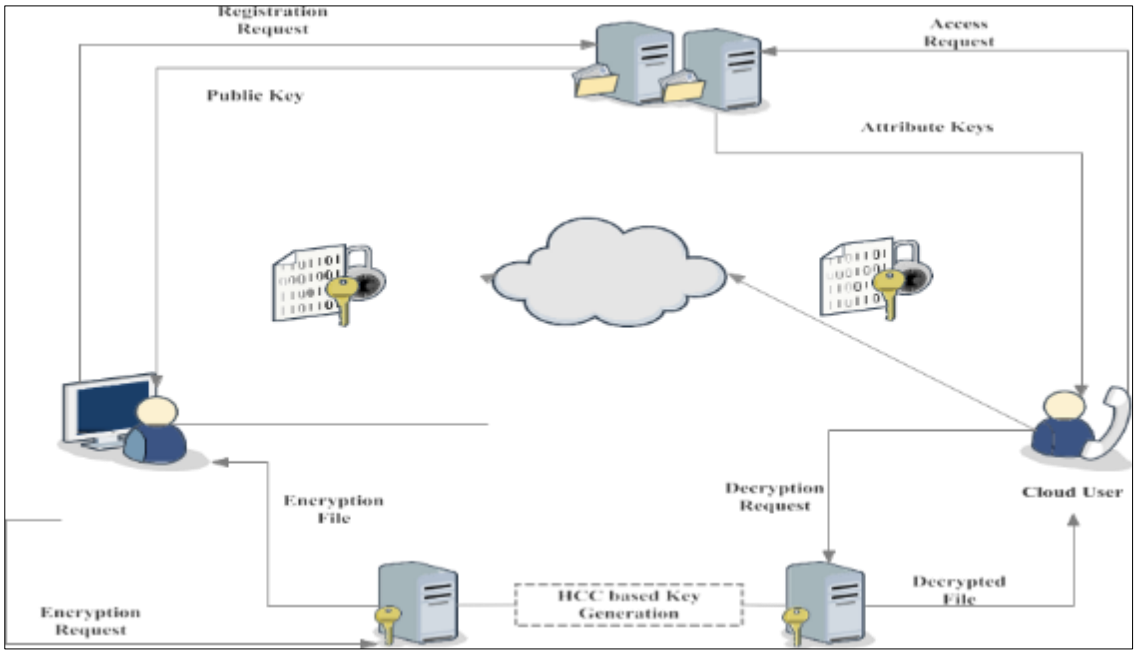

Figure 6 System Architecture of MA-CP-ABE with HCC

The attribute set is given as $AS = \{A1, A2, \ldots, Ai\}$.With this attribute set, the authority level is presented as$\{att1, att2, \ldots, atti\}$. Based on the encryption and decryption operations performed in the previous sections, the private and public keys for data security are generated. The public key and private keys are represented as $\{Pbk1, Pbk2, \ldots, Pbki\}$ and $\{Prk1, Prk2, \ldots, Prki\}$, respectively. Using the generated keys, the shared data is secured and then, using the private key, decryption is processed at the user end.

10. Performance analysis

MA-CP-ABE with HCC is implemented in Intel Pentium G620 CPU at 2.60GHz and 4 GB RAM using python 3.10, charm crypto 0.50 library on the Google Collaboratory and the results obtained are compared with the MA-FH-CP-ABE-ECC scheme. The experimental results represent the average values of 20 trials. The number of attributes is increased from 10 to 50.

11. Results and inference

This section presents the result analysis for the proposed cloud security scheme mainly focusing on the performance efficiency and model flexibility.

11.1. Performance Efficiency

In the scheme, the efficiency of a cryptography-based cloud security scheme is analyzed based on the amount of time to evaluate and the number of keys used in each level for securing the data. Hence, the following notations are considered for evaluating the performance.

- Tex is the time complexity for defining the modular exponentiation
- $Tmod$ defines the time complexity factor for modular multiplication
- Bit length is given as $|x|$.

It is assumed that the time complexity for performing modular operations is negotiable. Hence, the time complexity for performing the encryption and decryption is presented as,

$$\begin{cases} 2T_{ex} + T_{mod} \rightarrow Encryption \\ T_{ex} + T_{mod} \rightarrow Decryption \end{cases} \quad \ldots\ldots\ldots(12)$$

The communication cost of this scheme is considerably lesser than the proposed scheme, with the efficient implementations of the hyperbolic curve function MA-CP-ABE.

11.2. Flexibility

The proposed scheme contains flexible parameters of hyperbolic curves. The finite function of the HCC is divided based on several situations that can enhance the order selectivity of the model to ensure security.

The evaluations of the proposed MA-CP-ABE scheme with HCC are carried out based on the following metrics:

- Encryption Time
- Decryption Time

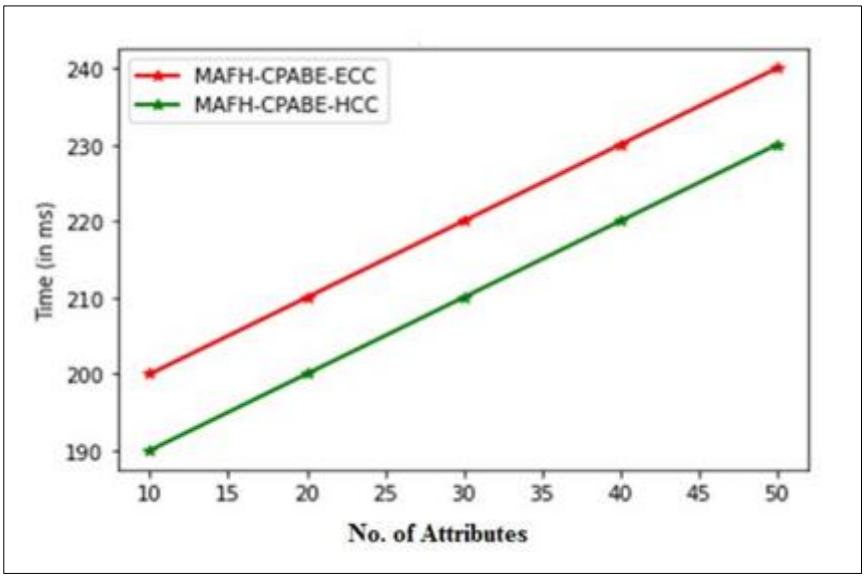

Figure 7 Encryption Time with varying number of Attributes

The encryption time is analyzed based on four modes of operations in securing the data over the cloud. It is also considered that the data count is given as $\{d1, d2, d3, d4\}$ and with four attributes as, $\{v1, v2, v3, v4\}$. The encryption

time results are analyzed for ECC based encryption, HCC based encryption, Attribute Based Encryption and encryption based on key size.

In Figure 7, the performance of the MA-CP-ABE with HCC based on user attributes is analyzed and the results are depicted. From Figure 7, it is also observed that the encryption time is gradually increasing with the number of attributes and approximately following a linear relationship with a number of attributes. It is observed from the results that the encryption time increases when the number of attributes increases. When compared to MA-CP-ABE-ECC, MA-CP-ABE-HCC takes lesser encryption time. The MA-CP-ABE-HCC scheme provides better efficiency by the encryption time than the existing schemes.

As in encryption, the next factor for evaluation is the decryption time based on user attributes shown Figure 8. From Figure 8, it is observed that the decryption time gradually increases with the number of attributes and approximately following a linear relationship with the number of attributes. The decryption time of the MA-CP- ABE-HCC scheme is less when compared to the MA-CP-ABE-ECC.

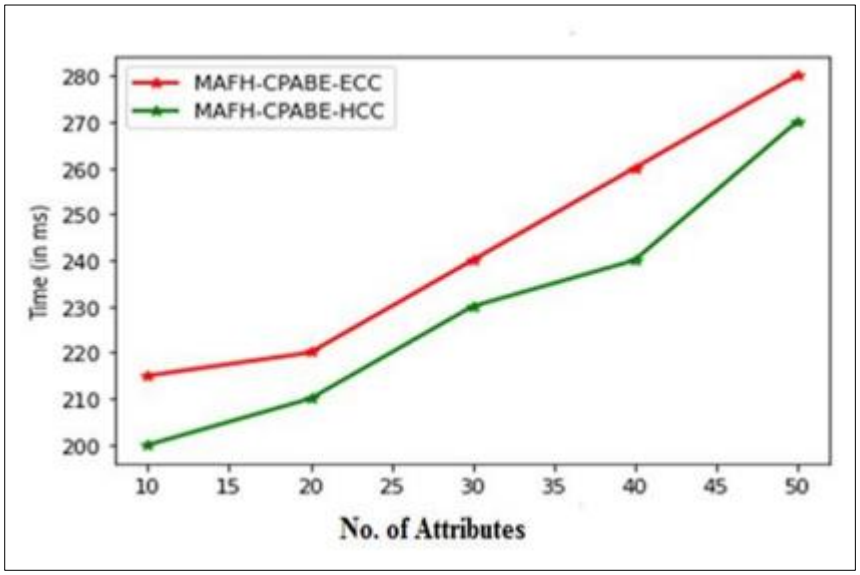

Figure 8 Decryption Time with varying number of Attributes

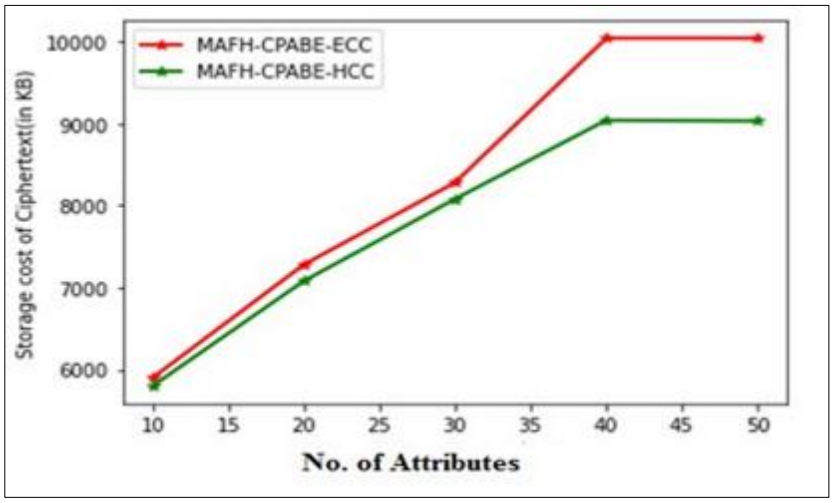

Figure 9 Storage cost with varying number of Attributes

The next factor to be considered for comparison is storage cost. For the storage cost of the ciphertext, the proposed MA-CP-ABE-HCC scheme consumes less storage than the existing scheme and it follows a linear relationship with the number of attributes as represented in Figure 9. MA-CP-ABE-HCC provides better results when the numbers of attributes is increased.

Further, the proposed schemes improve the efficiency in terms of the storage cost of ciphertext. The proposed schemes consume less storage cost when compared with the other existing schemes. The number of files taken into consideration is from 1 to 10. The file size varies from 1 Mb to 5 Mb. The number of attributes varies from 10 to 50. The number of attributes and number of files involved in determining the storage cost is compared and portrayed in Figure 10. It is observed that the security level based on the storage cost involved in the MA-CP-ABE-HCC is greater than the security level obtained by other schemes.

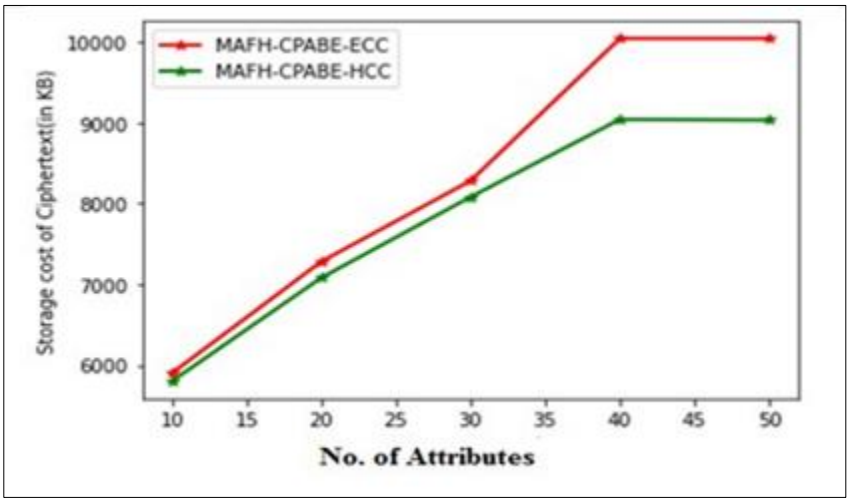

Figure 10 Comparison of Proposed Schemes for Storage Cost with varying number of files and attributes

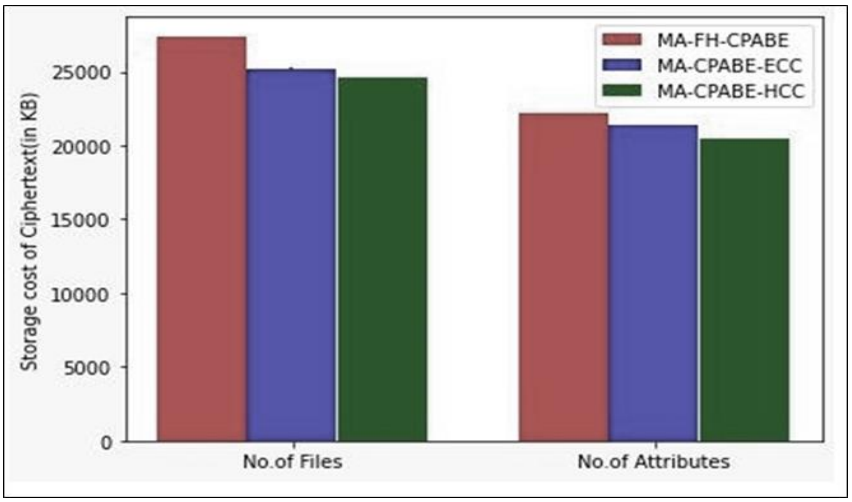

Figure 11 Comparison of Proposed Schemes for Key Generation Time with varying number of files and attributes

The key generation time is also compared based on the number of files and attributes as same as storage cost. Figure 11, shows that the proposed schemes are compared and the results are depicted. It is observed that the MA-CP-ABE-HCC scheme provides 97% of improved security rate. The proposed MA-CP-ABE-HCC scheme provides minimal processing time for encryption and decryption with a better rate of security. Figure 11 explicitly demonstrates that the ECC scheme provides 93% security rate and the HCC scheme provides 97% improved security rate

12. Conclusion

The Hyperbolic Curve Cryptosystem (HCC) is a general system of a key generation method, a decoding method and a signature verification method using a quadratic hyperbolic curve group. To enhance the security of the MA-CP-ABE scheme,the Hyperbolic Curve Cryptography is incorporated with the proposed scheme. The attributes are mapped with the points in the hyperbolic curve for key generation. The data is encrypted by the data owner using the hidden attribute data access structure. Theencrypted data is stored in the CSP. The data user downloads and decrypts the requireddata only when the user attribute matches with the set of attributes defined by the data owner. The simulation experiments

have been performed to evaluate the proposed MA-CP-ABE-HCC scheme. The encryption time and decryption time are observed with varying number of attributes. It is observed that the proposed scheme provides less processing time for both encryption and decryption compared to the existing systems. The simulation results have shown that the proposed scheme offers better performancein securing the shared data over the cloud.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl, Ricardo Puttini, and Zaigham Mahmood

[2] Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif

[3] Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)" by Michael J. Kavis

[4] Cloud Storage Forensics" by Darren Quick, Ben Martini, and Raymond Choo

[5] Cloud Native Infrastructure" by Justin Garrison and Kris Nova

[6] Cloud Storage Strategy: Harnessing the Power of the Cloud for Your Business" by Eric Vanderburg

[7] Google Cloud Storage: Professional Data Storage with Google Cloud Platform" by Anbazhagan Subbiah

[8] Cryptography and Network Security: Principles and Practice" by William Stallings

[9] Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif

[10] Cloud Security: A Comprehensive Guide to Secure Cloud Computing" by Ronald L. Krutz and Russell Dean Vines

[11] Securing the Cloud: Cloud Computer Security Techniques and Tactics" by Vic (J.R.) Winkler

[12] Data-Intensive Text Processing with MapReduce" by Jimmy Lin and Chris Dyer

[13] Foundations of Cryptography: Volume 2, Basic Applications" by Oded Goldreich

[14] Cloud Computing: Security Issues and Solutions" by Iaasak Abel Agboola

[15] Foundations of Cryptography: Volume 2, Basic Applications" by Oded Goldreich