Secure and Efficient Authentication System for Cloud Using Improved Hybrid Encryption Standard

*A. Hema Ambiha**

Abstract

Cloud computing (CC) is a virtualization technique that allows users to build and customise applications that run on the internet. Cloud technology is made up of a digital competence, a hard disc, a package application, and information. A trustworthy and dependable cloud storage service will be a great alternative for keeping data on the internet while being secure and stress-free. If security requirements are properly managed, many enterprises and government organisations will transit to cloud environments. The server for cloud storage systems, on the other hand, contains a significant amount of data. Data confidentiality is lost because data is kept for an extended length of time over the internet, allowing hackers to steal data from the storage system. Even when data is moved to the cloud, it retains data integrity (DI), which frequently disappoints cloud consumers. This article discusses about existing authentication and encryption systems in terms of user scenarios, distinguishing features, and limits. This research also looks at the benefits and drawbacks of authentication and data encryption strategies for CC services..

Keywords—Cloud Computing (CC), Security, Authentication, Data encryption, symmetric encryption, Asymmetric encryption, and Attribute based encryption.

I. INTRODUCTION

By merging the principles of grid computing, distributed computing, and utility computing, among others, CC combines various storage, computational, and software resources to form a vast pool of shared virtual resources [1]. It, like many other technical services, has given several benefits. It allowed for the storing of vast volumes of data, as well as the provision of many services. Furthermore, by distributing valuable resources across different users, this platform addressed the issue of scarce resources while cutting service costs [2]. CC is a service offered by data centres that is mostly based on virtualization technology [3]. By combining four fundamental characteristics, any platform may be turned into a CC platform: wide network connectivity, on-demand self-service, resource pooling, and quick elasticity. This innovation paves the way for reduced business startup by providing infrastructure as a service (IAAS), software as a service (SAAS), and platform as a service (PAAS) [4]. The fundamental benefit of the cloud is that it requires authentication before any user, organisation, or employee of a firm may access the data. Cost, attack vulnerability, a lack of control and flexibility, vendor lock-in, and, most significantly, security and privacy[5] are some of its drawbacks.

A company's security is critical for protecting its employees' data. Security is considered from the perspectives of data owner control, fine-grained access to stored data for protecting employee data from less privileged users [6]. As a result, protecting data stored in the cloud is critical; this can be accomplished by utilizing authentication, virtualization, and encryption, which help prevent unauthorized access. Public key encryption was a widespread technique in the early days of CC. This typical method does not achieve the desired outcomes because it only supports one-to-one encryption communication. Public key encryption has limited scalability. This paved the way for the development of more advanced techniques. In this paper, we will concentrate on data security (DS), which one of the most

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore
* Corresponding Author

pressing issues in cloud is computing. We also examine various security problems and the methods used to address those issues. Authentication and data encryption are thoroughly investigated.

II. BACKGROUND STUDY

Companies and cloud service providers have implemented solutions to prevent and mitigate the effects of the threats mentioned in the preceding section. This section will discuss some popular countermeasures, such as data encryption and authentication.

2.1 Authentication

Authentication is a critical component of every security system. It is a process of proving or showing something to be authentic, genuine, or valid, and it verifies the identity of a user or process. Before granting access to shared resources, an authentication process must be used to validate the user's identity. In the CC environment, several mechanisms are used to authenticate users, including username and password, single-factor, multi-factor, single sign-on (SSO), and biometric authentication. These methods are commonly used to improve the security of CC.

Marimuthu Karuppiah et al. [7] presented a key agreement-based secure mutual authentication method (AS) for cloud users. The system proved that the mutual authentication process was resistant to a variety of threats. The proposed work's security was examined using the Real-Or-Random (ROR) model, which confirmed that the model provided session key (SK) security. Furthermore, the model was compared to earlier state-of-the-art authentication frameworks. The results demonstrated that the scheme outperformed conventional schemes in terms of DS performance. Diksha Rangwani and Hari Om [8] introduced an Elliptical Curve Cryptography (ECC)-based secure user AS for the CC platform. The protocol was lightweight due to the usage of ECC as well as irreversible hash algorithms. According to the most recent formal and informal security evaluations based on AVISPA and BAN logic, the protocol was resistant to all malicious assaults. The protocol outperformed other similar protocols in a comparative performance comparison.

2.1.1 Two factor and Multifactor authentication

There has been some research towards two-factor and multifactor authenticationTwo-factor authentication (2FA) necessitates the use of two distinct types of authentication, whereas Multifactor Authentication (MFA) necessitates the use of at least two distinct types of authentication, if not more. Each level of assurance that the user attempting to access the account is permitted varies. SandeepKaur et al. [9] proposed a safe two-factor authentication architecture for the CC environment. When performing data transmission, the system used a one-way hash function and an efficient 2FA approach to authenticate cloud users. The proposed approach uses user IDs, passwords, and OTP verification protocols to authenticate users, protecting cloud data from attacks such as brute force, session and account hijacking, MITM, and replay. The results verified that the technique provided secure and efficient authentication between cloud users while also protecting users' sensitive data from a variety of attacks.

For cloud users using ECC, Hakjun Lee et al. [10] suggested a three-factor AS. To demonstrate the model's security efficacy, both formal and informal analyses were undertaken. Finally, the ECC model's performance was compared to that of other encryption methods, and the results demonstrated that ECC was superior to other encryption models in terms of security and encryption time. K. Mohana Prabha and P. Vidhya Saraswathi [11] presented the suppressed K-Anonymity Multi-Factor Authentication based Schmidt-Samoa Cryptography (SKMA-SC) algorithm to provide safe data access in CC. Cloud users were initially enrolled with the cloud server (CS) by supplying information such as one-time passwords, conditional qualities and tokens. The SKMA-SC authenticates users using the identities they gave during the registration process. The SKMA-SC permitted users to access data in the cloud after successful authentication by conducting the Schmidt-Samoa data encryption/decryption process. The results established that the suggested solution prevented illegal access to the environment and provided greater security to user data through the implementation of an efficient encryption scheme.

2.1.2 Biometric authentication

This authentication adds an extra degree of protection by certifying a user's true identity based on one or more biometric features. To improve cloud user security, Teena Joseph et al. [12] developed a multimodal biometric-based AS (MBAS). To authenticate the user, the system made advantage of multimodal biometrics features. Initially, users gave their biometrics in the form of an image, which was then preprocessed, normalized, and feature extracted. The secret key was formed by merging the retrieved features in two steps. By using MBAS, the approach provided safe access control in the CC platform and improved DS. Kashish A. Shakil et al. [13] introduced a biometric-based AS for the healthcare cloud, which uses behavioural biometric signature-based authentication to secure e-medical data access security. The authentication signature samples were learned in parallel using a Resilient Back propagation neural network employing the Hadoop Map Reduce architecture. A performance comparison with other cutting-edge algorithms shows that the system outperforms the existing systems.

2.2 Data Encryption

Data encryption aids to information security. Both data saved in the cloud and data sent are secure. While encryption prevents illegal data access, it cannot prevent data loss. There are numerous DS hazards to consider. The three essential features that must be ensured are data availability, confidentiality, and integrity. Several encryption techniques have been developed to safeguard cloud data. The following are some well-known encryption algorithms:

2.2.1 Symmetric encryption

The symmetric key cryptographic (SKC) model encrypts and decrypts the data using a single secret key. The generated secret key of the cryptographic model was shared between the sender and receiver before the decryption process. Some of the popularly used symmetric key cryptographic models to provide DS are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, IDEA, Rivest Cipher 4 (RC4), Rivest Cipher 5 (RC5), and Rivest Cipher 6 (RC6).

2.2.2 Asymmetric encryption

In asymmetric key encryption (AKE), the encryption procedure uses two types of keys, such as the private and public keys, to carry out encryption and decryption on the user data, unlike symmetric encryption, which employs the same secret key for both operations. Compared to the private key system, this is the most used model to provide higher security to the data in the network. Asymmetric encryptions, as some examples, include: Digital Signature Standard (DSS) and Rivest Shamir Adleman (RSA), which includes the Digital Signature Algorithm (DSA), and ECC.

Ijaz Ahmad Awan et al. [14] suggested an AES algorithm for the CC platform that improved data privacy and security for cloud users. The results revealed that the model performed the best in terms of various measures. The strategy reduced power use by 14.43%, delay by 15.67%, and network utilization by 11.53%, according to the data. As a result, when delivering computational cloud services, the framework increased security, lowered resource use, and reduced delay.Based on the Triple Data Encryption Standard (TDES),Mohan NaikRamachandra et al. [15] provided a solution for storing vast volumes of data in the cloud that was both efficient and safe. By raising the length of keys in DES, the disclosed TDES methodology provides a significantly simpler way for protecting against assaults and defending data privacy. The findings revealed that the TDES approach efficiently secured and protected vast amounts of healthcare data stored in the cloud. Furthermore, the TDES methodology took less time to encrypt and decode than the existing Intelligent Framework for Healthcare DS (IFHDS) method.

To improve DI in the CC context, Priyadharshini Kaliyamoorthy and Aroul Canessane Ramalingam [16] proposed Qusai modified levy fight distribution (QMLFD) for the RSA system. The data was safeguarded against unauthorized access by utilizing the RSA cryptosystem for secure key generation and data encryption. A quasi-based modified Levy battle distribution algorithm was used to select the key. As a result, the system presented an effective model for improving DI in CC by validating the DI of cloud-stored data. P. Chinnasamy et al. [17] suggested a hybrid cryptography model for the healthcare cloud to offer patient data security and integrity. By integrating ECC and Blowfish, the model exploited both symmetric and asymmetric methods. The hybrid system's efficiency was compared with the previous hybrid encryption models, demonstrating that the approach provided higher security and integrity to the patient data.

2.2.3 Attribute based encryption

ABE is a kind of public-key encryption model which uses attributes to determine the encrypted data or ciphertext (CT) and the user's secret key. The decryption of a CT is only possible in such a system if the user key's set of attributes matches the CT's attributes. Table 1 compares the advantages and disadvantages of traditional ABE techniques.

Table 1: Comparison of current existing works on attribute based encryption

Author Name and Ref. No	**Technique Used**	**Advantages**	**Drawbacks**
Hui Cui *et al.* [18]	Server aided Revocable ABE (SR-ABE)	The computational overheads of users in decrypting CT were significantly reduced by the SR-ABE framework, where the computation time for a user to decrypt a CT was independent of the number of attributes associated with the CT and the attribute keys.	Increased computational cost, because the server had to be online all the time to meet user decryption requests.
Yang Ming *et al.* [19]	Multi Authority ABE (MA-ABE)	Storage and computation cost efficient.	Although the system produced promising results, it did not demonstrate a high level of security.
Jiguo Li*et al.*	Key-Policy	Resistant to leakage	The KP - ABE

[20]	ABE (KP-ABE)	of auxiliary input.	approach produced better results, but it did not provide compromising security.
MariemBouchaala *et al.* [21]	Traceable, Revocable and Accountable Ciphertext-Policy ABE (TRAK-CPABE)	It was achieved lower computational time and decryption time.It was also secure and robustto all security patterns.	However, malicious users used their devices for decryption instead of secret keys. This implies that white-box traceability was not an effectual one.

III. METHODOLOGY

In the initial step of our proposed model, we present an efficient hashing-based authentication system and a cryptographic scheme called Improved Advance Encryption Standard for cloud data users to prevent their data from unauthorized access and provide better security to the data uploaded into the public cloud.

3.1 Elliptic curve cryptography (ECC)

ECC, a type of public-key cryptography uses the algebraic structure of elliptic curves over finite fields. When compared to other public-key algorithms, it provides strong security with very short key lengths, making it especially suited in confined situations such as mobile devices. and Internet of Things (IoT) devices.

The basic idea behind elliptic curve cryptography is to express a group structure on an elliptic curve and exploit the mathematical properties of this structure for cryptographic operations. The curve is defined by an equation of the form y^2 = x^3 + ax + b, where a and b are parameters that determine the shape of the curve. The points on the curve, along with a special "point at infinity," form an Abelian group under an operation called point addition.

In ECC, each participant generates a key pair consisting of a private key and a public key. The private key is generated using a random number, typically selected from a wide range, while the public key is framed from the private key using a mathematical operation termed as scalar multiplication. The scalar multiplication is a method of repeatedly adding the same point on the curve to itself at given number of times. as specified by the private key.

The complexity of solving the elliptic curve discrete logarithm problem (ECDLP), which is the underlying mathematical issue that forms the basis of the cryptographic operations, determines the security of ECC. According to the ECDLP it is computationally infeasible to determine the value of k at given a point P on the curve and the result of scalar multiplication kP (where k is an unknown integer).

ECC has a number of advantages over other public-key algorithms such as RSA. Initially, ECC provides equivalent security with shorter key lengths, resulting in faster computations and fewer resource needs. This makes it especially useful for devices with limited resources. Second, ECC provides strong security against both classical and quantum computer attacks. Unlike RSA, ECC's security is dependent on the difficulty of solving the ECDLP, which has not been proved to be vulnerable to quantum computers. Due to its efficiency and strong security properties, elliptic curve cryptography has become widely adopted in various applications, including secure communications protocols (e.g., TLS/SSL), digital signatures, key exchange protocols, and more.

3.2 Advanced Encryption Standard (AES)

AES is a data encryption specification that is a symmetric block cypher technique with a block/chunk size of 128 bits. It uses 128-, 192-, and 256-bit keys to translate these individual blocks. It encrypts these blocks and connects them to generate the cipher text.

The main idea behind the cryptography of AESareAES-128, AES-192 and AES-256: These are the three key lengths supported by AES. The numbers represent the size of the encryption key in bits. AES-256 provides the highest level of security among the three, but AES-128 and AES-192 are also considered highly secure.

Electronic Codebook (ECB) Mode: This is the easiest mode of operation for AES.Sinceeach block of plain textisse parately encrypted with the same key, some vulnerability canoccur. ECB mode does not provide any form of diffusion, which means that patterns in the plaintext can be apparent in the ciphertext.

Cipher Block Chaining (CBC) Mode: In CBC mode, each block of plaintext is XORed with the previous block of ciphertext before encryption. This ensures that identical blocks of plaintext produce different blocks of ciphertext.It also requires an initialization vector (IV) for the first block. CBC mode provides confidentiality and is resistant to some attacks, but it does not provide integrity or authentication.

Counter (CTR) Mode: CTR mode converts a block cipher into a stream cipher. It takes a counter as the input to the block cipher, and the output is XORed with the plaintext to produce the ciphertext. CTR mode allows encryption and decryption to run in parallel, making it suitable for high-performance applications. It also provides confidentiality but lacks integrity and authentication.

Galois/Counter Mode (GCM): GCM is an authenticated encryption mode which combines the Counter (CTR) mode with a universal hash function called Galois Field Multiplication. GCM provides confidentiality, integrity, and authentication in a single mode of operation. It is widely used for secure communication and storage.

XTS-AES: XTS-AES (XEX-based Tweaked CodeBook mode with CipherText Stealing) is q mode specifically designed for backing up data on storage devices such as hard drives and solid state drives. It provides confidentiality and protection against certain attacks, taking into account the block structure of the storage medium.

These are just a few methodologies and modes of operation that can be used with the Advanced Encryption Standard. The choice of methodology depends on the specific security requirements, performance considerations, and the context in

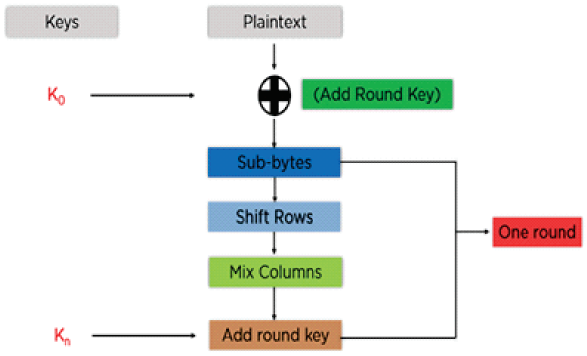

Figure1.Block structure

IV. PROPOSED WORK

4.1. Combining AES and ECC for Cloud Security:

To protect data confidentiality in the cloud, AES can be employed for symmetric encryption. Before data is transferred to the cloud, it is split into fixed-size blocks and encrypted using AES with a randomly generated session key. This key is securely exchanged using ECC-based key exchange protocols, ensuring the confidentiality of the session key itself.

4.4.1. Key Management:

ECC offers efficient key management in cloud environments. Shared cryptographic keys can be securely established between cloud users and providers using ECC-based algorithms such as Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Integrated Encryption Scheme (ECIES). These keys can then be used for AES encryption/decryption operations, providing a secure and efficient key management mechanism.

4.4.2. Authentication and Integrity:

ECC-based digital signatures, such as Elliptic Curve Digital Signature Algorithm (ECDSA), can enhance cloud security by providing authentication and integrity verification. Digital signatures generated using ECC ensure the authenticity of cloud resources, verifying that they have not been tampered with during transmission or storage. This prevents unauthorized access and detects any unauthorized modifications.

4.4.3. Hybrid Encryption:

A combination of symmetric AES encryption and ECC-based hybrid encryption can provide an additional layer of security for cloud data. In this approach, ECC is used for key exchange and AES for bulk data encryption. This hybrid encryption scheme harnesses the benefits of both algorithms, combining the efficiency of symmetric encryption with the strong security properties of ECC.

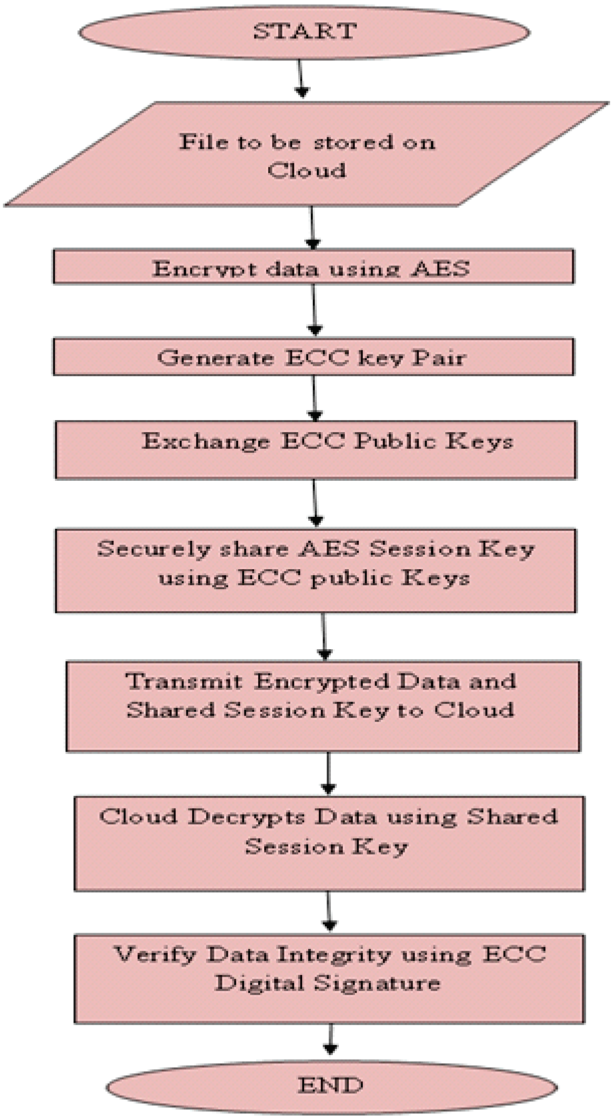
START
File to be stored on Cloud
Encrypt data using AES
Generate ECC key Pair
Exchange ECC Public Keys
Securely share AES Session Key using ECC public Keys
Transmit Encrypted Data and Shared Session Key to Cloud
Cloud Decrypts Data using Shared Session Key
Verify Data Integrity using ECC Digital Signature
END

Figure2.Flowchart

V. CONCLUSION

An efficient hashing-based authentication system and a cryptographic scheme called Improved Advance Encryption Standard for cloud data users is developed to prevent the data from unauthorized access and better security to the data uploaded into the public cloud is provided using the Improved AES.Securing sensitive data in the cloud is of utmost importance in today's digital landscape. By Combining the strengths of Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC), cloud security can be greatly improved.AES ensures data confidentiality, while ECC provides secure key exchange, authentication, integrity, and efficient key management. Adopting this powerful combination of encryption techniques helps safeguard data privacy, protect against unauthorized access, and fortify the overall security posture of cloud environments.

REFERENCES

[1] Pan Jun Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions", IEEE Access, vol. 7, pp. 147420-147452, 2019.

[2] Hamed Tabrizchi and Marjan Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions", The Journal of Supercomputing, vol. 76, pp. 9493-9532, 2020.

[3] Amr M. Sauber, Passent M. El-Kafrawy, Amr F. Shawish, Mohamed A. Amin and Ismail M. Hagag, "A new secure model for data protection over cloud computing", Computational Intelligence and Neuroscience, vol. 2021, pp. 1-11, 2021.

[4] Pan Jun Sun, "Security and privacy protection in cloud computing: Discussions and challenges", Journal of Network and Computer Applications, vol. 160, pp. 1-34, 2020.

[5] VishrutiKakkad, Meshwa Patel and Manan Shah, "Biometric authentication and image encryption for image security in cloud framework", Multiscale and Multidisciplinary Modeling, Experiments and Design, vol. 2, no. 4, pp. 1-6, 2019.

[6] Praveen S. Challagidad and Mahantesh N. Birje, "Efficient multi-authority access control using attribute-based encryption in cloud storage", Procedia Computer Science, vol. 167, pp. 840-849, 2020.

[7] MarimuthuKaruppiah, Ashok Kumar Das, Xiong Li, SaruKumari, Fan Wu, Shehzad Ashraf Chaudhry and Niranchana R, "Secure remote user mutual authentication scheme with key agreement for cloud environment", Mobile Networks and Applications, vol. 24, no. 11, pp. 1-18, 2018.

[8] DikshaRangwani and Hari Om, "A secure user authentication protocol based on ECC for cloud computing environment", Arabian Journal for Science and Engineering, vol. 46, pp. 3865-3888, 2021.

[9] Sandeep kaur, Gaganpreet kaur and Mohammad Shabaz, "A secure two-factor authentication framework in cloud computing", Security and Communication Networks, vol. 2022, pp. 1-9, 2022.

[10]Hakjun Lee, Dongwoo Kang, Youngsook Lee and Dongho Won, "Secure three-factor anonymous user authentication scheme for cloud computing environment", Wireless Communications and Mobile Computing, vol. 2021, pp. 1-20, 2021.

[11]MohanaPrabha K and VidhyaSaraswathi P, "Suppressed K-anonymity multi-factor authentication based schmidt-samoa cryptography for privacy preserved data access in cloud computing", Computer Communications, vol. 158, pp. 85-94, 2020.

[12]Teena Joseph, Kalaiselvan S. A, Aswathy S. U, Radhakrishnan R and Shamna A. R, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment", Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 2, pp. 1-9, 2020.

[13]Kashish A. Shakil, Farhana J. Zareen, Mansaf Alam and SuraiyaJabin, "BAMHealthCloud: A biometric authentication and data management system for healthcare

data in cloud", Journal of King Saud University – Computer and Information Sciences, vol. 32, no. 1, pp. 57-64, 2017.

[14]Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar and Allah Ditta, "Secure framework enhancing AES algorithm in cloud computing", Security and Communication Networks, vol. 2020, pp. 1-16, 2020.

[15]Mohan Naik Ramachandra, Madala SrinivasaRao, Wen Cheng Lai, Bidare Divakarachari Parameshachari, Jayachandra Ananda Babu and Kivudujogappa Lingappa Hemalatha, "An efficient and secure big data storage in cloud environment by using triple data encryption standard", Big Data and Cognitive Computing, vol. 6, no. 4, pp. 1-20, 2022.

[16]Priyadharshini Kaliyamoorthy and Aroul Canessane Ramalingam, "QMLFD Based RSA cryptosystem for enhancing data security in public cloud storage system", Wireless Personal Communications, vol. 122, no. 1, pp. 755-782, 2021.

[17]Chinnasamy P, Padmavathi S, Swathy R and Rakesh S, "Efficient data security using hybrid cryptography on cloud computing", Lecture Notes in Networks and Systems, Springer, pp. 537-547, 2021.

[18]Hui Cui, Tsz Hon Yuen, Robert H. Deng and Guilin Wang, "Server-aided revocable attribute-based encryption for cloud computing services", Concurrency and Computation Practice and Experience, vol. 32, no. 14, pp. 1-16, 2020.

[19]Yang Ming, Baokang He and Chenhao Wang, "Efficient revocable multi-authority attribute-based encryption for cloud storage", IEEE Access, vol. 9, pp. 42593-42603, 2021.

[20] Jiguo Li, Qihong Yu, Yichen Zhang and JianShen, "Key-policy attribute-based encryption against continual auxiliary input leakag", Information Sciences, vol. 470, pp. 175-188, 2018.

[21]MariemBouchaala, CherifGhazel and Leila AzzouzSaidane, "TRAK-CPABE: A novel traceable, revocable and accountable ciphertext-policy attribute-based encryption scheme in cloud computing", Journal of Information Security and Applications, vol. 61, pp. 1-13, 2021.