



Efficient Unpredictable Multi Authority Attribute based Encryption

Rohini S¹, Gini R²

¹ Student, Department of MCA, Narayanaguru College of Engineering, Anna University.

² Asst. Professor, Department of MCA, Narayanaguru College of Engineering, Anna University.

ABSTRACT

Data access control is an effective way to ensure data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Attribute-based encryption (ABE) is usually adopted for cloud storage, both for its achievement of fine grained access control over data, and for its guarantee of data confidentiality. Single-authority Attribute-Based Encryption (SA-ABE) has its obvious drawback in that only one attribute authority can assign the users' attributes, enabling the data to be shared only within the management domain of the attribute authority, while rendering multiple attribute authorities unable to share the data. On the other hand, multi-authority attribute-based encryption (MA-ABE) has its advantages over SA-ABE. It can not only satisfy the need for the fine-grained access control and confidentiality of data, but also make the data shared among different multiple attribute authorities. In this paper, on the basis of the cryptography, an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage is proposed. Multi-authority attribute-based encryption was very suitable for data access control in a cloud storage environment. However, efficient user revocation in multi-authority attribute based encryption remains a challenging problem that prevents it from practical applications. A multi-authority attribute-based encryption scheme with efficient revocation was proposed with proved statically secure and revocable in the random oracle model.

Keywords: Cloud Platform, Encryption, Decryption, Revocation, Security.

1 Introduction

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are divided into three main categories or types of cloud computing: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Cloud storage is an application pattern of cloud computing to store massive data, so more and more individuals and organizations shift their data from local computers to cloud. However, this new paradigm poses a serious threat to the privacy of their owners, since the data might be accessed and analyzed by the cloud server providers for illegal or monetary purposes. To solve this problem, people have figured out a variety of approaches. One common way is to resort to the traditional public key encryption technology to encrypt data, but the data owners fail to have fine-grained access to their data flexibly. It used to be considered one of the most promising technologies for cloud storage, since it ensures the data owners to enjoy no



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

interactive and fine-grained control over encrypted data. Since then, many single-authority attribute-based encryption (SA-ABE) schemes have been put forward. In these schemes, it is required that only one trusted attribute authority administers the attributes and distributes the corresponding secret keys of attributes to the data consumers. This mechanism may not meet the practical requirements in cloud storage, when data consumers' attributes are distributed by multiple different attribute authorities. For example, when a data owner intends to share the data with a targeted data consumer holding the attribute "Professor" from a university and the attribute "Engineer" from a research institution, obviously SA-ABE scheme cannot be applied to this scenario. To deal with this problem, many researchers turn to multi-authority attribute-based encryption (MA-ABE), so that secret keys of attributes are issued to data consumers with the corresponding privileges for different attribute authorities respectively. There exist two kinds of multi-authority ABE schemes, namely centralized multi-authority ABE and decentralized multi authority ABE. When the key is distributed by central authority, we can consider it as centralized multi authority ABE scheme. When the key is distributed by attribute authority, we can consider it as decentralized multi-authority ABE scheme.

From the perspective of practical application, the following challenges should be solved before applying MA-ABE in cloud storage system. One of the major challenges is the highly computational overhead, since the existing MA-ABE schemes are all based on the expensive bilinear pairing operations, hinders the further development of MA-ABE schemes on the resource-constrained devices. The other challenge is the attribute revocable, since multiple data consumers may share the same attribute, and each data consumers may possess multiple different attributes, result in that revocation for anyone attribute may influence the other data consumers in the cloud storage system. Although encrypting the data is a method to solve this problem, it will generate high computation cost. Another technology is to introduce a timestamp into every attribute, but it is not achieved immediate revocation.

This paper involves the construction of an efficient RMA-ABE scheme for cloud storage. Our main contributes are an efficient RMA-ABE scheme is proposed for cloud storage, so that bilinear pairing operations will be no longer needed. In the proposed scheme, we use the linear secret sharing schemes (LSSS) to boost the expressiveness of access policy and add version key to attribute to realize immediate attribute revocation. Second, the security analysis indicates that under the decisional Diffie-Hellman (DDH) assumption, the proposed RMA-ABE scheme achieves in distinguishability against the chosen plaintext attack (IND-CPA), and satisfies collision resistant and forward secrecy. Finally, the performance evaluation of the scheme indicates benefits of decreasing the computation Cost and occupies less storage overhead than other schemes.

2 Recent Works

Identity-Based Encryption, Amit Sahai and Brent Waters [2005] [1] in this paper they introduced a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as a set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω , to decrypt a ciphertext encrypted with



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

an identity, ω ', if and only if the identities ω and ω' are close to each other as measured by the “set overlap” distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term “attribute-based encryption”. In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

Attribute--Based Encryption for Fine-Grained Access Control of Encrypted Data, Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters [2006] [2] in this paper more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). Thus it provides a low accuracy system and therefore provides less security, they developed a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. In many mission-critical applications, fine-grained data access control is a must as illegal access to the sensitive data may cause disastrous results and/or be prohibited by the law. They demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

[3] Ciphertext-Policy Attribute-Based Encryption, John Bethencourt, Amit Sahai and Brent Waters [2007] in this paper distributed systems, a user should only be able to access data if a user posse a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

[4] FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

Networks, Hucheng Yu, Kui Ren and Wenjing Lou [2011] distributed sensor data storage and retrieval have gained increasing popularity in recent years for supporting various applications. While distributed architecture enjoys a more robust and fault-tolerant wireless sensor network (WSN), such architecture also poses a number of security challenges especially when applied in mission critical applications such as battlefield and e-healthcare. First, as sensor data are stored and maintained by individual sensors and unattended sensors are easily subject to strong attacks such as physical compromise, it is significantly harder to ensure data security. Second, in many mission-critical applications, fine-grained data access control is a must as illegal access to the sensitive data may cause disastrous results and/or be prohibited by the law. Last but not least, sensor nodes usually are resource-constrained, which limits the direct adoption of expensive cryptographic primitives. To address the above challenges, we propose, in this paper, a distributed data access control scheme that is able to enforce fine-grained access control over sensor data and is resilient against strong attacks such as sensor compromise and user colluding. Here the proposed scheme exploits a novel cryptographic primitive called attribute-based encryption (ABE), tailors, and adapts it for WSNs with respect to both performance and security requirements. The feasibility of the scheme is demonstrated by experiments on real sensor platforms. To our best knowledge, this paper is the first to realize distributed fine-grained data access control for WSNs.

[5] HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing, Zhiguo Wan, Jun'e Liu and Robert H. Deng [2013]. Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute based encryption (CP-ABE) scheme by Bethencourt and analyse its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

3 Proposed Work

The proposed RMA-ABE scheme embraces five entities: central authority (CA), attribute authorities (AAs), cloud service provider (CSP), data owner (DO) and data consumer (DC).



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

CA: CA, as central authority, is responsible for initializing the system public parameters, verifying and registering the DCs' and AAs' identities and the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. AAs: AA, an independent attribute authority, which is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. The function of AA is generating public keys and secret keys, and distributing secret keys of attributes to data consumers. In addition, when one or more attributes are revoked, AA operates the update key generation algorithm for non-revoked data consumers. CSP: CSP is responsible for data storage. When an attribute is revoked, CSP will provide data access service to data consumers and perform ciphertext update algorithm to help data owners update their ciphertext. DO: DO performs such operations as defining the access structure over attributes from one or more AAs, encrypting according to the access structure, and uploading encrypted data to the CSP. DC: DC has access to ciphertexts from CSP, and requests their secret keys from corresponding AAs. Only if the DC's attribute set meets the access structure, DC decrypts the ciphertexts successfully with his secret keys. The proposed RMA-ABE scheme is composed of such five phases as: the system initialization, the secret key generation, the data encryption, the data decryption, and the attribute revocation.

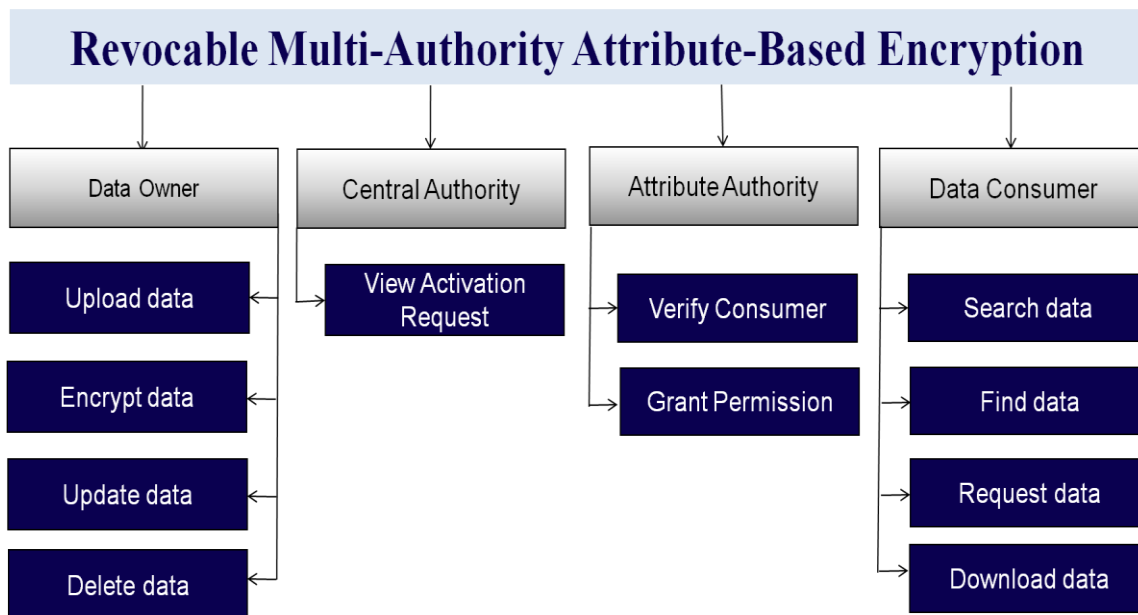


Figure 1: Proposed block Diagram

3.1 Revocable Multi Authority Attribute Based Encryption Scheme Implementation

3.1.1 System Initialization

1. CA Setup (λ) $\rightarrow$ PP. This Central Authority is implemented by Central Authority. It takes as input a security parameter λ , outputs public system parameters PP.
2. DCReg (info DC) $\rightarrow$ uid. Central Authority carries out the algorithm, using the Data Consumer's information info DC (e.g., name, birthday etc.) as input, and the identity uid



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

as output.

3. AAReg (info AA) $\rightarrow$ aid. Central Authority performs the algorithm, with AA's information info AA as input, and identity aid as output.
4. AA Setup (PP, S_{aid}) $\rightarrow$ APK_{aid} , ASK_{aid} , $\{VK_{xaid}, PK_{xaid}\}_{xaid \in S_{aid}}$. Attribute authority executes the algorithm, where the system public parameters PP and the attribute set S_{aid} managed by AA aid are used as input, and the outputs are the public and secret key pairs (APK_{aid} , ASK_{aid}) of AA_{aid} , version keys and the public keys of the attributes $\{VK_{xaid}, PK_{xaid}\}_{xaid \in S_{aid}}$ where the attribute set S_{aid} is managed by AA_{aid} .

3.1.2 Secret Key Generation

$SKey\ Gen(ASK_{aid}, S_{uid,aid}, \{VK_{xaid}\}_{xaid \in S_{uid,aid}}) \rightarrow SK_{uid,aid}$. AA performs the algorithm by entering secret key ASK_{aid} of AA_{aid} , the DC's attributes set $S_{uid, aid}$ and the corresponding version keys $\{VK_{xaid}\}_{xaid \in S_{uid,aid}}$ to generate secret key $SK_{uid,aid}$ for the DC.

$$SK_{uid, aid} = \{K_{uid, aid} = \alpha_{aid} / \beta_{aid} + 1 / \beta_{aid}\} \quad (1)$$

3.1.3 Data Encryption

To encrypt the data m under an access structure (M, ρ) , where M is a matrix with l rows and n columns and ρ is a function, associating each row M_i of M with attribute $\rho(i)$, Data Owner does as follows:

1. Data Owner selects two random vectors $\lambda E = (s, y_2, y_3, \dots, y_l)$, $\omega E = (0, z_2, z_3, \dots, z_l)$ and computes $\lambda_i = M_i \lambda$, $\omega_i = M_i \cdot E \omega$ for all $i = [1, l]$.
2. Data Owner selects a random value $s \in \mathbb{Z}_q$ and calculates $C_0 = m + s P_{aidk} \in \mathbb{I}A_{aidk}P$, where IA expresses the set of attribute authorities related to (M, ρ) .
3. Data Owner computes $C_{1,i} = \lambda_i P + \omega_i PK_{\rho(i)}$, $C_{2,i} = \omega_i \beta_{aidk} P$, $C_{3,i} = s \beta_{aidk} P$ for all $i = [1, l]$. The ciphertext is

$$CT = \{C_0, (C_{1,i}, C_{2,i}, C_{3,i}) \mid i = [1, l]\} \quad (2)$$

3.1.4 Data Decryption

This phase is composed of $Decrypt(CT, \{SK_{uid,aidk}\}_{aidk \in IA}) \rightarrow m$. DC executes the algorithm by entering ciphertext CT , and the secret keys $\{SK_{uid,aidk}\}_{aidk \in IA}$ related to the set IA , to output the data m .

3.1.5 Attribute Revocation

If an attribute x_{aid} is revoked from DC with identity uid , the phase of attribute revoked is as follows:

1. $UKeyGen(ASK_{aid}; x_{aid}, VK_{xaid}) \rightarrow VK_{xaid}; UK_{xaid}$. The key generation is executed by the corresponding AA_{aid0} administering the revoked attribute x_{aid} . It takes as input the secret key ASK_{aid} of AA_{aid} , the version key VK_{xaid} of the revoked attribute and the revoked attribute x_{aid} , outputs the new version key fVK_{xaid} and the update key UK_{xaid} .
2. $SKUpdate(SK_{uid,aid}; UK_{xaid}) \rightarrow SK_{uid,aid}$. The updation is executed by the non-revoked



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

Data Consumer. Its inputs are the current secret key $SK_{uid;aid}$, the update key UK_{xaid} , and its output is the new secret key $SK_{uid;aid}$.

3. CTUpdate (CT; UK_{xaid}) $\rightarrow$ CT. The Ciphertext updation is run by the Cloud Service Provider. Its inputs are the current ciphertext, the update key UK_{xaid} and its output is the new ciphertext.

4 Result and Discussion

The paper work provides a public key and a secret key. Encrypt: The inputs of the Encrypt algorithm are a message, an access matrix, the global parameters and the public keys of the pertinent authorities. The output of the algorithm is the ciphertext. Key Gen: A key is created for the (identity, attribute) pair. The CAs issue identity-related keys to users but do not involve in any attribute-related operations. The AAs issue attribute-related keys to users. Each AA manages a different attribute domain, and operates independently from other AAs. A party may easily join the system as an AA by registering itself to the CAs and publishing its attribute-related parameters. The expressiveness, efficiency and security are comparable greater than other schemes. Therefore no authority can independently decrypt any ciphertext.

	MA-ABE	MA-CP-ABE	Ours RMA-ABE
Standard Model	✓	✗	✓
Multi-Authority	✗	✓	✓
Prevent Decryption by Individual Authority	✗	Partially	✓
Size of Ciphertext	$2l + 2$	$3l + 1$	$2l + 2$
Size of Secret key	$ S + 2$	$ S $	$ S + D(K + 2)$
Pairing Computation of Decryption	$2 I + 1$	$2 I $	$2 I + 1$
Size of Public key	$ U + 3$	$2 U $	$ U + 3 + D$

Figure 2: Performance comparison

Finally all the file verification and authorization process completes by the Central Authority and as well as other attribute authorities for the particular user who requests the key for downloading a particular file can get the key and successfully download the files.



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

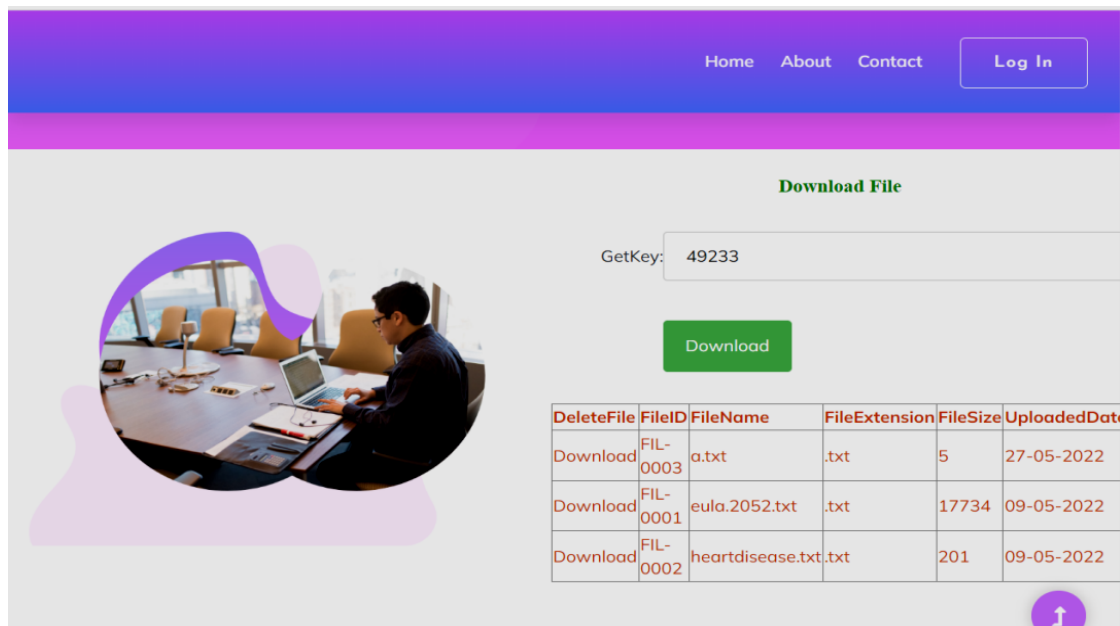


Figure 3: Downloading files using the key

5 Conclusion

This paper proposes an efficient RMA-ABE system for cloud storage, which is on the basis of the elliptic curve cryptography. The proposed scheme will not need any bilinear pairing operations any more. The version key is introduced into the attribute to achieve the attribute revocation. Security proof demonstrates that the proposed scheme enjoys the confidentiality. Finally, the performance evaluation of the scheme indicates following benefits, of reducing the Computation Cost, requires less storage overhead than other schemes. In addition, by using the unique identity uid tied to the secret keys of attributes, collusion resistant is realized. It is showed in the performance analysis that the proposed scheme is high-efficiency in storage as well as computation cost.

References

1. Yu Shucheng; Kui Ren; Wenjing Lou, Year: 2011, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," IEEE Transactions on Parallel Distributed System, Vol: 22, no: 4, pp. 673686.
2. Wan Zhiguo; Robert H. Deng, Year: 2012, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics Security, Vol: 7, no: 2, pp. 743754.
3. Bethencourt John; Amit Sahai; Brent Waters, Year: 2007, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Transactions on Symposium Security and Privacy, pp. 321–334.
4. Yang Kan; Xiaohua Jia; Kui Ren, Year: 2015, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Transactions on Parallel Distributed System, Vol: 26, no:



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

12, pp. 3461–3470.

5. Li Jiguo; Xiaonan Lin; Yichen Zhang; Jinguang Han, Year: 2017, “KSF-OABE: Outsourced attribute based encryption with keyword search function for cloud storage,” IEEE Transactions on Services Computing, Vol: 10, no: 5, pp. 715–725.

6. Li Jiguo; Wei Yao; Jinguang Han; Yichen Zhang; Jian Shen, Year: 2018, “User collision avoidance CP-ABE with efficient attribute revocation for cloud storage,” IEEE Transactions on Systems Journal, Vol: 12, no: 2, pp. 1767– 1777.

7. Wang Yong; Biwen Chen; Lei Li; Qiang Ma; Huicong Li; Debiao He, Year: 2020, “Efficient and secure ciphertext policy attribute-based encryption without pairing for cloud assisted smart grid,” IEEE Access, Vol: 8, pp. 40704–40713.

8. Ding Sheng; Chen Li; Hui Li, Year: 2018, “A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT,” IEEE Access, Vol: 6, pp. 27336–27345.

9. Guo Rui; Huixia Shi; Qinglong Zhao; Dong Zheng, Year: 2018, "Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems," in IEEE Access, Vol: 6, pp. 11676-11686.

10. Guo Rui; Huixian Shi; Qinglan Zhao; Dong Zheng, Year: 2017, "Immediate Attribute Revocation in Decentralized Attribute-Based Encryption Access Control," 2017 IEEE Trustcom/BigDataSE/ICSS, pp. 33-40.

11. Dolev Shlomi; Niv Gilboa; Marina Kopeetsky, Year: 2012, "Permanent Revocation in Attribute Based Broadcast Encryption," IEEE International Conference on Cyber Security, pp. 203-208.

12. Zhang Wei; ZhiShuo Zhang; YI WU, Year: 2020, "Multi-Authority Attribute Based Encryption With Policy-hidden and Accountability," IEEE International Conference on Space-Air-Ground Computing (SAGC), pp. 95-96.

13. Liu Yuan; Licheng Wang; Lixiang Li; Xixi Yan, Year: 2019, "Secure and Efficient Multi-Authority Attribute-Based Encryption Scheme from Lattices," in IEEE Access, Vol: 7, pp. 3665-3674.

14. Huang Kaiqing, Year: 2012, "Secure Efficient Revocable Large Universe Multi-Authority Attribute-Based Encryption for Cloud-Aided IoT," in IEEE Access, Vol: 9, pp. 53576-53588.

15. Shao Jiaye; Yanqin Zhu; Qijin Ji, Year: 2017, "Privacy-preserving online/offline and outsourced multi-authority attribute-based encryption," IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), pp. 285-291.

16. Miao Yinbin; Robert H. Deng; Ximeng Liu; Kim-Kwang Raymond Choo; Hongjun Wu; Hongwei Li, Year: 2021, "Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data," in IEEE Transactions on Dependable and Secure Computing, Vol: 18, no: 4, pp. 1667-1680.

17. Hur Junbeom; Dong Kun Noh, Year: 2011, "Attribute-Based Access Control with Efficient



Article Title: Efficient Unpredictable Multi Authority Attribute based Encryption

Revocation in Data Outsourcing Systems," in IEEE Transactions on Parallel and Distributed Systems, Vol: 22, no: 7, pp. 1214-1221.

18. Ibrahim Mostafa; Mostafa GM Mostafa; Sherif H. Nour El-Din; Rania Elgohary; Hossam Faheem, Year: 2021, "A Robust Generic Multi-Authority Attributes Management System for Cloud Storage Services," in IEEE Transactions on Cloud Computing, Vol: 9, no: 2, pp. 435-446.

19. Pussewalage Harsha Sandaruwan Gardiyawasam; Vladimir Oleshchuk, Year: 2023, "A Delegatable Attribute Based Encryption Scheme for a Collaborative E-Health Cloud," in IEEE Transactions on Services Computing, Vol: 16, no: 2, pp. 787-801.

20. Jiang Yu; Xiao long Xu; Fu Xiao, Year: 2022, "Attribute-Based Encryption with Blockchain Protection Scheme for Electronic Health Records," in IEEE Transactions on Network and Service Management, Vol: 19, no: 4, pp. 3884-3895.