Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

Fortification for Cloud Data Pilfering: using Attribute-based Encryption

Karthik A Patil
School of Computer Science and Engineering
REVA University Bengaluru, India

Nithin Mohandas
School of Computer Science and Engineering
REVA University Bengaluru, India

Pavan Swamy Hiremath
School of Computer Science and Engineering
REVA University Bengaluru, India

Biradar Vikas Mohanrao
School of Computer Science and Engineering
REVA University Bengaluru, India

Prof. Shruthi G
Assistant Professor
School of Computer Science and Engineering
REVA University
Bengaluru, India

***Abstract*— Cloud Storage provides the information owner to host endemic information into the cloud that can be accessed by the cloud users. There are many benefits to use cloud storage namely for substantial readiness, substantial authenticity, fleeting implementation, and durability. Since the cloud depository is steered by the Cloud Service Providers (CSP), the traditional methods like Client/Server mock-ups are not satisfactory for the cloud depository. So many IT industries use the CP-ABE, Cypher-Policy Text Attribute based Encryption technique to bring forth the certainty to the information stored in the cloud depository. But in this technique, the authority is centralized i.e., Single-Authority Access Control. Single-authority access control is used to generate unique and undisclosed keys for permissibility verified users that makes the users to wait for an epoch, to get their undisclosed keys to access the data from the cloud. To overcome this problem, to achieve surge the coherence of the system we are proposing decentralized technique i.e., Multi-Authority Access control system using ABE, Attribute Based Encryption.**

Keywords—Cypher-Policy Text Attribute based Encryption, Multi- Authority Access control system.

I. INTRODUCTION

Most of us knowingly or unknowingly use cloud computing in our daily activities. Cloud storage and cloud computing have become a part of our lives. Large industries, various organizations and institutions use cloud computing at various levels which has led to a tremendous growth of cloud storage systems and cloud service providers. Providing security is one among a few major concerns involved with cloud storage systems, this is usually handled by an access control.

An access control handles, manages, regulates and monitors permissions or access to data stored by a owner. It provides users the control to restrict unauthorized access and helps in maintaining a proper workflow. Handling an ingress governance in large scale public cloud storage systems is a very challenging task. The current security mechanism adopted in such a system is known as Ciphertext-Policy Attribute Based Encryption (CP-ABE). This mechanism provides flexibility and security to the cloud storage to which it is a part of. The drawback of such a system is that it makes use of single attribute authority.

A single attribute authority must handle the verification of a data user and the distribution of a secret key simultaneously which is very time consuming. This results in users being stuck in a long waiting queue to receive their secret keys, which leads to a system with less efficiency. To solve this problem another method which involves multi mastery ingress governance plan of actions has been put forward, but they are not so efficient in improving the overall performance of the system.

In our proposed system, we put forward a unique access control mechanism to overcome the problems present in the systems using single and multi- authority access control schemes which provides very effective and efficient data access control. Our proposed scheme also includes an auditing mechanism and a revocation method as well. Our framework consists of multiple accredit masteries to delegate the work of verifying user's permissibility, it also includes a centralized authority which generates and distributes the secret keys to already verified legitimate users. To improvise the security, we have instilled an auditing mechanism to identify a malfunction in the verification process and a revocation mechanism.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

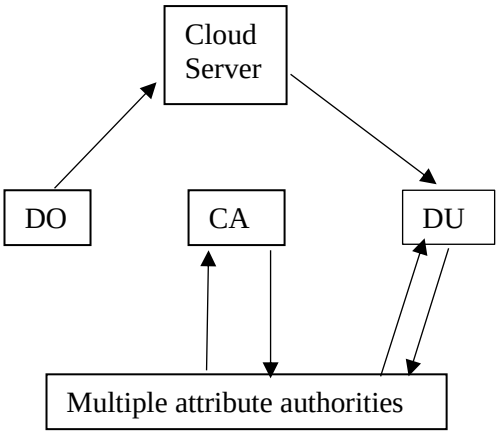

Figure 1: Architectural Design

II. RELATED WORK

As we are living in the age of Big Data, the computational developments and efficiencies are growing faster day by day, hence the security provides to these data are at utmost importance [6], [2] there are many projects which have led to successful inventions in cloud access control that specifically includes assignment-based, characteristic-based, consumption-mastery-based schemes. The privacy and security of the users' information which is deposited in the cloud is a major concern and this has hindered the wide adoption of public clouds [4], [5]. To fend off the unaccredited set-ups from acquiring the delicate information, a banal quick fix is to inscribe information and then transmit the ciphered information into the cloud [1], [7]. Nevertheless, the customary public key encryption and identity-based encryption (IBE) [8] is incapable of being arrogated. The rationale being that they only set the seal on the information ciphered is unraveled by one and only one end user, thus the pliability and malleability of ingress sway is dwindled. [10] (RB-MTAC) replica can regulate the specification of the user and endemic acceptable characters by the of user recognition governance and attain information and scheme separation by the way of well-organized administration of occupant ingress integrity, have in view to ameliorate multiuser soundness and seclusion in cloud. Cyphertext-Policy combined with accredit-based encryption is said to be an efficient to have a control over the access of data [10]. CP-ABE plan of action was initially put forward by Bethencourt et al. in [11], but this plan of action was manifested reliable only in the all-encompassing classification replica. In our put forward plan of action, and user can retrieve the data only if he/she has the necessary attribute keys with reference to the defined ingress stratagem. In addition to this, our proposed system includes the properties of constant-size ciphertext, it requires a compact reckoning-tariff as well. It supports attribute-level revocation and authorizes information possessor to perform user proportion renovation.

III. IMPLEMENTATION

We have divided our system model into five different modules as shown in figure 1. The five modules are:

1) Central Authority
2) Attribute Authorities
3) Cloud Server
4) Data Owner
5) Data User/Consumer

1. Central Authority

The central authority acts as an administrator of the system. Its responsibilities include initiating public key for all accredit in the accredit set and setting up the methodology parameters. In the commencing stage, it prov0069des an UID and an AID to all user and an accredit mastery respectively. Once the user sends a key request, the CA engenders confidential keys for the user on the essence of multiple accredits obtained verified by AA. The CA has the capability to identify which AA has malfunctioned and granted access to unauthorized attributes.

2. Attribute Authorities

The responsibilities of attribute authorities is to perform verification of the user and the generation of attribute key for the verified user. We are proposing multiple accredit masteries which can exchange the responsibilities of verifying the user and each AA can perform this independently for all the users. Each AA once selected, will substantiate the permissibility of the user using authentication protocols and it engender an attribute key. This attribute key is used in CA to generate secret keys.

3. Cloud Server

It anticipates a cloud storage tenet for all the data holders to stock and exchange endemic information. The data stored is encrypted using symmetric encryption algorithm. The information stocked in the cloud can be downloaded and modified by verified users having appropriate attribute keys.

4. Data Owner

Data owner as shown in figure 2, is the one who has the authority to define access policies which includes the permissions to access the data. Initially, the data owner ciphers endemic information using a symmetric encryption algorithm, next the data holder defines an ingress stratagem based on an accredit set and ciphers the symmetric key according to the stratagem defined and the public keys obtained from the CA. Finally, the data owner uploads the complete data that includes encrypted data and encrypted symmetric key (Cipher Text) to the cloud where it is stored.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

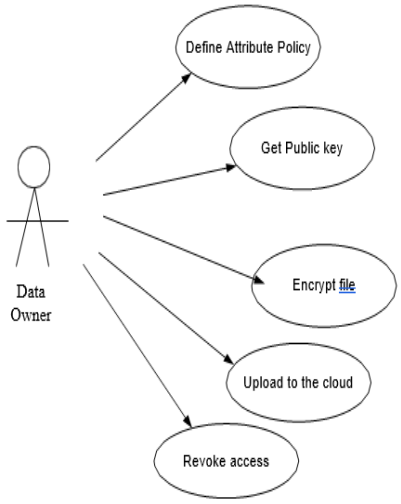

Figure 2: Data Owner

5. Data User

A data user as shown in figure 3, is associated with a unique identity known as UID by central authority. The data user possesses a set of accredits along with a confidential key correlated with endemic accredit set. A data user can access, modify, and download any ciphered information available in the cloud by decrypting the data file. The user can interpret the file consisting the required information only if he/she satisfies all the conditions mentioned in the ingress stratagem defined by the owner.

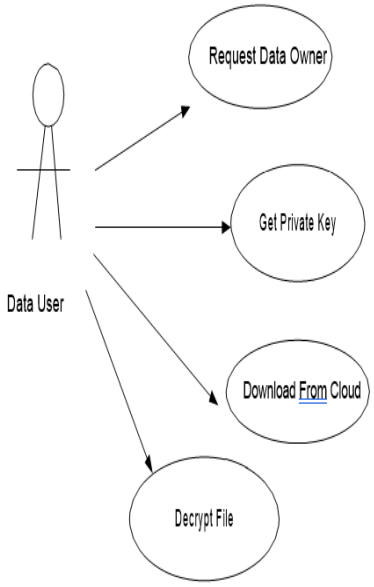

Figure 3: Data User

The non-functional requirements of our system model are:

1. Portability: The complete program is matured using Java, which paves the way for the program to be implemented on any machine having JDK and JVM.
2. Ease of use: The design of front end is very simple so that the user can interact easily.
3. Modularity: The proposed system is divided into five modules to increase flexibility.
4. Robustness: This program has been matured in such a way that the comprehensive fulfilment of the program is enhanced, and the user can look forward to the outcomes inside a bounded time with greatest applicability and exactness.

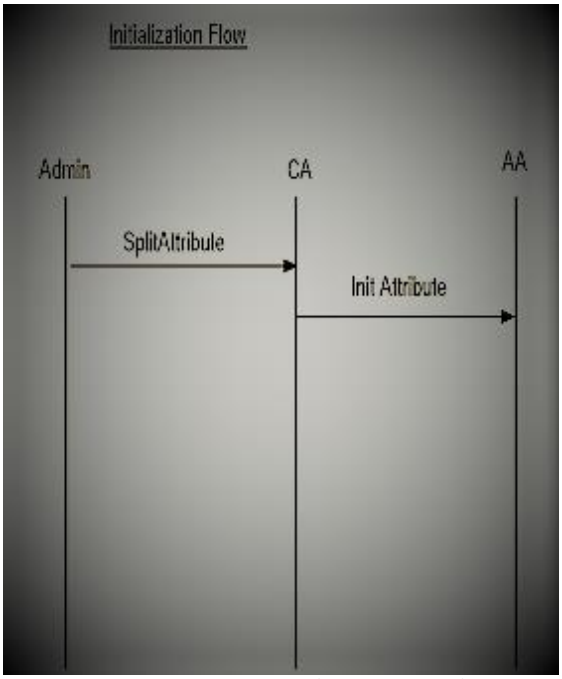

Figure 4: Sequence diagram for initialization flow

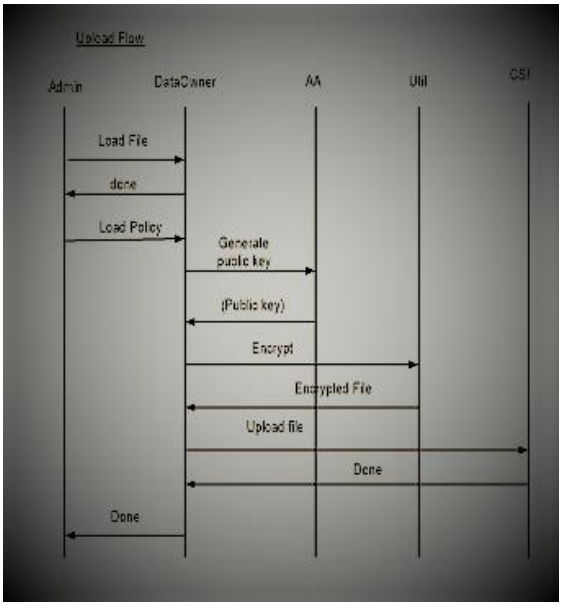

Figure 5: Sequence diagram for upload flow

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

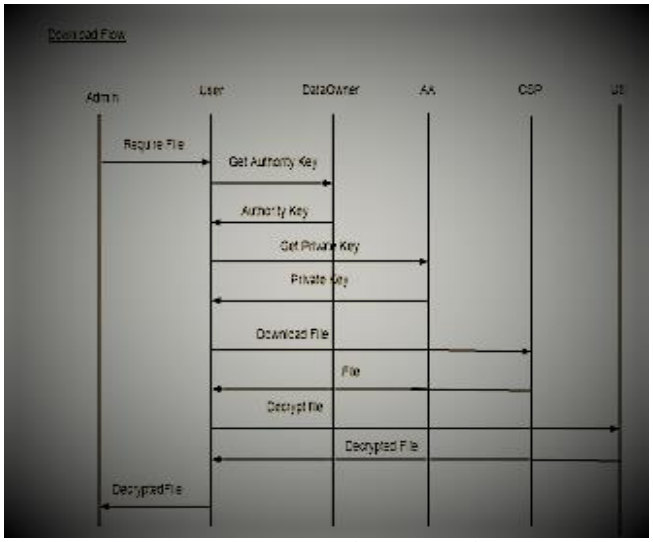

Figure 6: Sequence diagram for download flow

IV. RESULTS

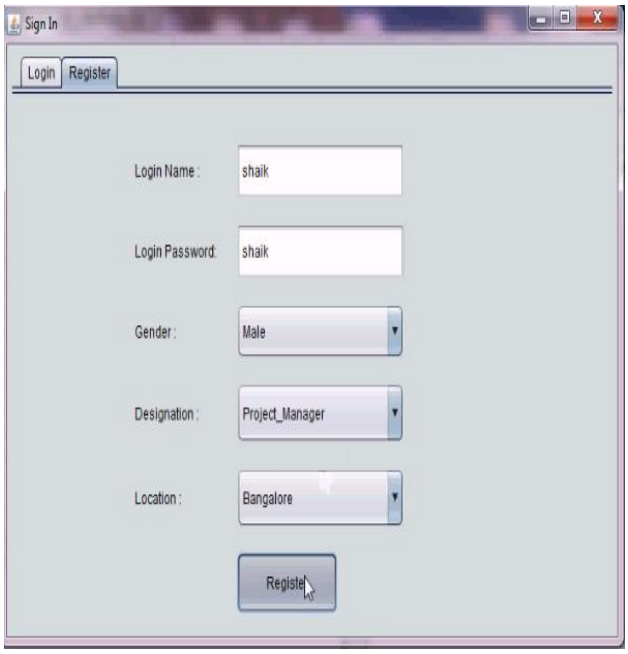

Figure 7: Registration Page

Registration page is the initial page where each desired user shall require registering by filling in the blanks as shown in fig:7, such as Login Name, Login Password, Gender, Description and Location. Only registered users can be able to successfully login using his/her login credentials as a data owner or a data user.

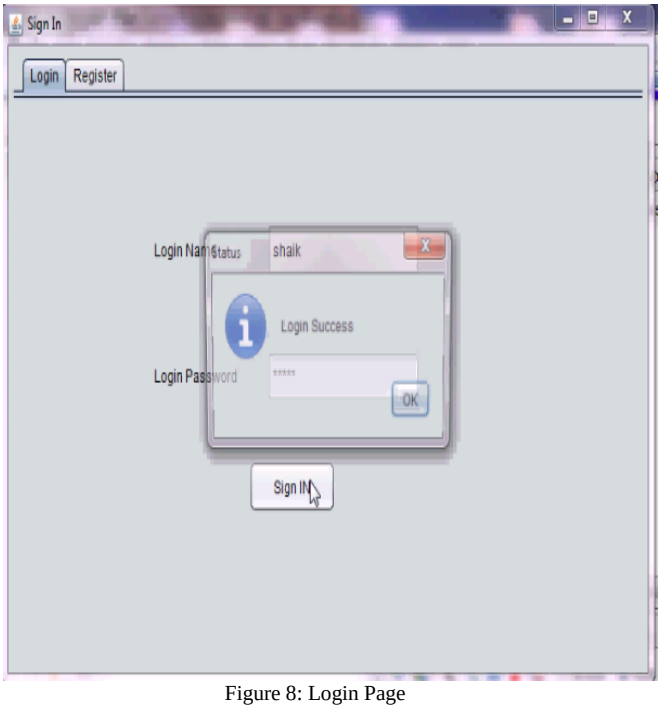

Figure 8: Login Page

Login page appears in the data owner's portal and data user's portal. The data owner and the data user need to specify the right login name and login password they had specified during registration.

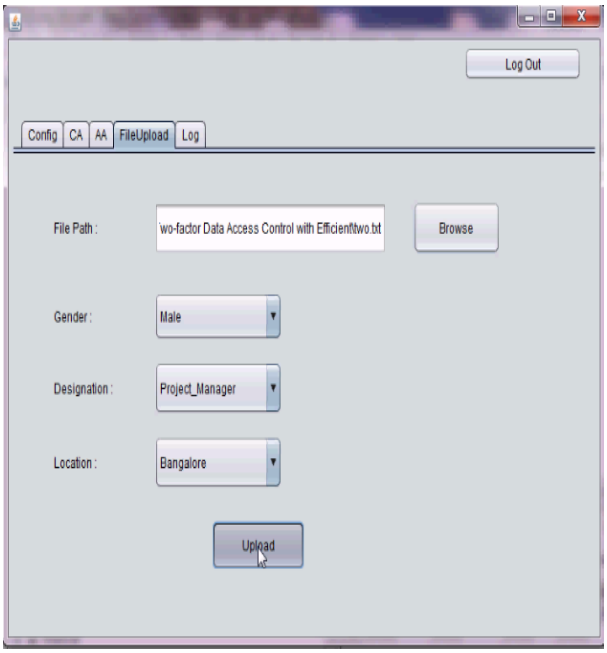

Figure 9: File Transfer

The file can be uploaded by browsing from the system by the data owner. Gender, description, and location are the attributes which could be assigned in a unique combination, only with which the data user could retrieve the file. The file is encrypted using RSA algorithm.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

Figure 10: Record of the processes

The data user must register first (if not registered previously), once registered then he/she has to login using the appropriate attributes. Once the user legitimacy is verified, the secret key is generated using which the file is decrypted. The file is downloaded from the cloud storage and can be viewed, modified, and updated.

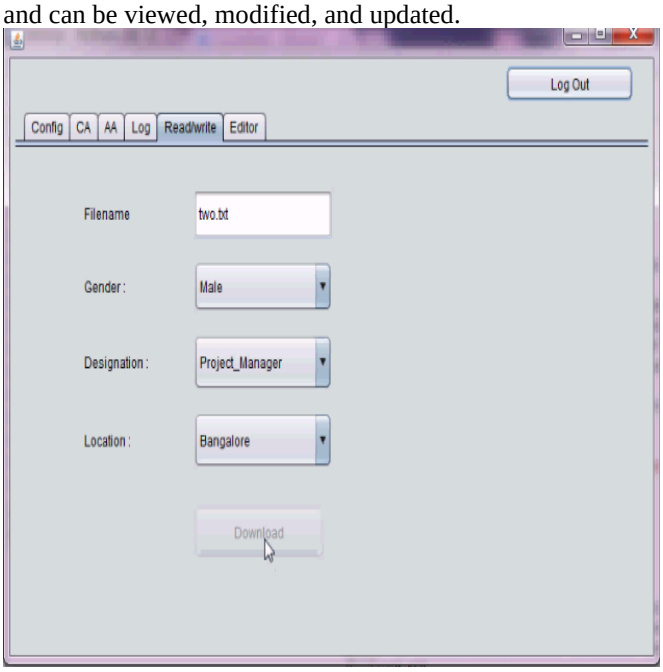

Figure 11: File Access Request Page

The legitimacy of the user is verified by checking the combination of the attributes specified for the specific file name. Once the user legitimacy is verified, the secret key is generated using which the file is decrypted. The file is downloaded from the cloud storage and can be viewed, modified, and updated.

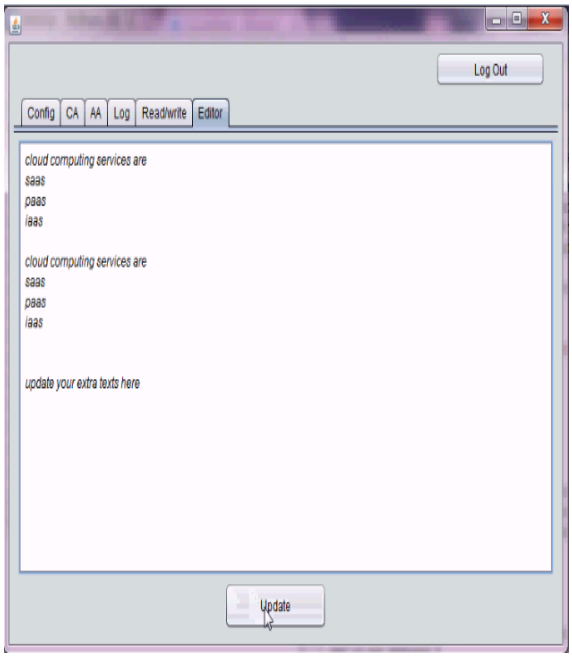

Figure 12: Decrypted File

The above image shows the decrypted file after been downloaded from the cloud into the data user's system. This file offers both read and write operations to the user.

V. CONCLUSION

Our proposed system signifies a new information ingress authority system using multiple attributes of authority for the cloud storage system. Our proposed system contributes two-factor protection procedure to hike the concealment of the information. To access or recuperate the information, every user is needed to have all the adequate accredit keys concerned with ingress stratagem and endorsement key. As we have proposed earlier, both the cryptograph text size and the numerous twin effectiveness in interpretation are persistent, that reduces the transmission aloft and the cost of the set-up. Additionally, we have put forward that users can also revoke or modify the data uploaded by the data owner using accredit-based information ingress governance system.

VI. REFERENCES

[1] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, ''*Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach,*'' IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[2] K. Yu, S. Eum, T. Kurita, Q. Hua, T. Sato, H. Nakazato, T. Asami, and P. Kafle, ''*Information-centric networking: Research and standardization status,*'' IEEE Access, vol. 7, pp. 126164–126176, 2019.

[3] X. Qi, Y. Su, K. Yu, J. Li, Q. Hua, Z. Wen, J. Lopez, and T. Sato, ''*Design and performance evaluation of content-oriented communication system for IoT network: A case study of named node networking for real- time video streaming system,*'' IEEE Access, vol. 7, pp. 88138–88149, 2019.

[4] J. Huang, D. M. Nicol, R. Bobba, and J. H. Huh, ''*A framework integrating attribute-based policies into role-based access control,*'' in Proc. 17th ACM Symp. Access Control Models Technol. (SACMAT). New York, NY, USA: ACM, 2012, pp. 187–196.

[5] T. Tavizi, M. Shajari, and P. Dodangeh, ''*A usage control-based architecture for cloud environments,*'' in Proc. IEEE 26th Int.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

Parallel Distrib. Process. Symp. Workshops PhD Forum, May 2012, pp. 1534–1539.

[6] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, and M. Wang, ''*Fog-Computing- Enabled cognitive network function virtualization for an information- centric future Internet,*'' IEEE Commune. Mag., vol. 57, no. 7, pp. 48–54, Jul. 2019.

[7] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, and M. Wen, ''*MBID: Micro- blockchain- based geographical dynamic intrusion detection for V2X,*'' IEEE Commune. Mag., vol. 57, no. 10, pp. 77–83, Oct. 2019.

[8] X.-Y. Li, Y. Shi, Y. Guo, and W. Ma, ''*Multi-tenancy-based access control in cloud,*'' in Proc. Int. Conf. Compute. Intell. Softw. Eng., Dec. 2010, pp. 1–4.

[9] S.-J. Yang, P.-C. Lai, and J. Lin, ''*Design role-based multi-tenancy access control scheme for cloud services,*'' in Proc. Int. Symp. Biometrics Secure. Technol., Jul. 2013, pp. 273–279.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-based encryption for fine- grained access control of encrypted data,*" in Proc. 13th ACM Conf. Compute. Commun. Secur. (CCS), 2016, pp. 89–98.

[11] J. Bethencourt, A. Sahai, and B. Waters, "*Ciphertext-policyattribute-based encryption,*" in Proc. IEEE Symp. Secur. Privacy (S&P), May 2016, pp. 321–334.