International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

Access Control based Scheme for effective cloud data access with secured policy with Equality Test

Gunda Mamatha, Department of CSE, Malla Reddy College of Engineering & Technology, Telangana - 500014
D Chandra Sekhar Reddy, Associate Professor, Department of CSE, Malla Reddy College of Engineering & Technology, Telangana - 500014

Abstract -With the rapid use of large data, how to control access to large amounts of large data becomes a very difficult problem, especially when large data is stored in the cloud. We propose an effective and well-obtained system based on the control of access to big data with the policy of protection of privacy thanks to the Equality Test. where all the attributes are hidden in the access policy, not just the values of the attributes. We also designed a new Bloom attribute filter to evaluate if the attribute is in the access policy. The Encryption Text Policy attribute based on equality-based encryption (CP-ABE with equality test) is a promising encryption technique that allows Data-Providers to encrypt data within specified access rules for certain attributes of recipients of data and only allows attributes to comply with access rules to decrypt data. In CP-ABE with the equality test, the access policy is attached to the encrypted text in the form of a simple text, which can also filter some private information about Data-Providers. Existing methods only partially hide attribute values in access rules, while attribute names are not yet protected. In particular, in the proposed system, we hide the entire attribute (instead of only its values) in the access rules and we will not filter any privacy information in the access control policy with quality control, and we will protect against text attacks without the selected format using the equality test.

Index Terms—Big Data; Access Control; Privacy-preserving Policy; Attribute Bloom Filter; LSSS Access Structure

1. INTRODUCTION

In the era of big data, a huge amount of data can be generated quickly from various sources (e.g., smart phones, sensors, machines, social networks, etc.). Towards these big data, conventional computer systems are not competent to store and process these data. Due to the flexible and elastic computing resources, cloud computing is a natural fit for storing and processing big data [1], [2]. With cloud computing, Data-Providers store their data into the cloud, and rely on the cloud server to share their data to other users (data consumers). In order to only share Data-Providers' data to authorized users, it is necessary to design access control

mechanisms according to the requirements of Data-Providers. When outsourcing data into the cloud, Data-Providers lose the physical control of their data. Moreover, cloud service providers are not fully-trusted by Data-Providers, which make the access control more challenging. For example, if the traditional access control mechanisms (e.g., Access Control Lists) are applied, the cloud server becomes the judge to evaluate the access policy and make access decision. Thus, Data-Providers may worry that the cloud server may make wrong access decision intentionally or unintentionally, and disclose their data to some unauthorized users. In order to enable Data-Providers to control the access of their own data, some attribute-based access control schemes [3]–[5] are proposed by leveraging attribute-based encryption [6], [7]. In attribute-based access control, Data-Providers first define access policies for their data and encrypt the data under these access policies. Only the users whose attributes can satisfy the access policy are eligible to decrypt the data. Although the existing attribute-based access control schemes can deal with the attribute revocation problem [3]– [5], they all suffer from one problem: the access policy mayleak privacy. This is because the access policy is associated with the encrypted data in plaintext form. From the plaintext of access policy, the adversaries may obtain some privacy information about the end-user. For example, Alice encrypts her data to enable the "Psychology Doctor" to access. So, the access policy may contain the attributes "Psychology" and "Doctor". If anyone sees this data, although he/she may not be able to decrypt the data, he/she still can guess that Alice may suffer from some psychological problems, which leaks the privacy of Alice. To prevent the privacy leakage from the access policy, astraight forward method is to hide the attributes in the access policy. However, when the attributes are hidden, not only the unauthorized users but also the authorized users cannot know which attributes are involved in the access policy, which makes the decryption a challenging problem. Due to this reason, existing methods [8]–[12] do not hide or anonymize the attributes. Instead, they only hide the values of each attribute by using wildcards [8], [9], Hidden Vector Encryption [10], and Inner Product Encryption [11], [12]. Hiding the values of attributes can somehow protect user privacy, but the attribute name may also leak private information. Moreover, most of these partially hidden policy schemes only support specific policy structures (e.g., AND-gates on multi-valued attributes). In this paper, we aim to hide the whole attribute instead of only partially hiding the attribute values. Moreover, we do not restrict our method to some specific access structures. The basic idea is to express the access policy in LSSS access structure (M;r) where M is a policy matrix and r matches each row Mi of the matrix M to an attribute [6], and hide the attributes by simply removing the attribute matching function r. Without the attribute matching function r, it is necessary to design an attribute localization algorithm to evaluate whether an attribute is in the access policy and if so find the correct position in the access policy. To this end, we further

build a novel Attribute Bloom Filter to locate the attributes to the anonymous access policy, which can save a lot of storage overhead and computation cost especially for large attribute universe. Our contributions are summarized as follows.

1) We propose an access control scheme for big data with privacy-preserving policy, where the whole attributes are hidden in the access policy rather than only the values of the attributes.

2) We also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.

3) We further give the security proof and performance evaluation of our proposed scheme, which demonstrate that our scheme can preserve the privacy from any LSSS access policy without employing much overhead.

2. LITERATURE SURVEY

Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage

In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Enabling Access Control scheme with Efficient Attribute Revocation and Policy Updating in Smart Grid

In this paper, we propose a fine-grained access control scheme (FAC) with efficient attribute revocation and policy updating in smart grid. Specifically, by introducing the concept of Third-party Auditor (TPA), the proposed FAC achieves efficient attribute revocation. Also, we design an efficient policy updating algorithm by outsourcing the computational task to a cloud server. Moreover, we give security analysis and conduct experiments to demonstrate that the FAC is both secure and efficient compared with existing ABE-based approaches.

Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach

In this paper, we focus on how to securely share video contents to a certain group of people during a particular time period in cloud-based multimedia systems, and propose a cryptographic approach, a provably secure time-domain attribute-based access control (TAAC) scheme, to secure the cloud-based video content sharing. Specifically, we first propose a provably secure time-domain attribute-based

encryption scheme by embedding the time into both the ciphertexts and the keys, such that only users who hold sufficient attributes in a specific time slot can decrypt the video contents. We also propose an efficient attribute updating method to achieve the dynamic change of users' attributes, including granting new attributes, revoking previous attributes, and regranting previously revoked attributes. We further discuss on how to control those video contents that can be commonly accessed in multiple time slots and how to make special queries on video contents generated in previous time slots. The security analysis and performance evaluation show that TAAC is provably secure in generic group model and efficient in practice.

Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority

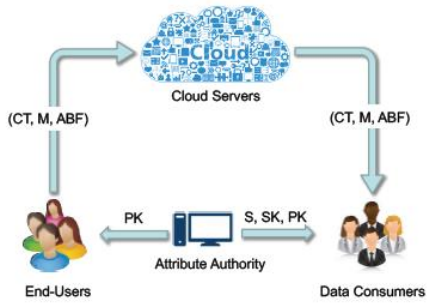
This paper presents a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encrypter can encrypt a message such that a user could only decrypt if he has at least d_k of the given attributes about the message for at least $t + 1$, $t \leq n/2$ honest authorities of all the n attribute authorities in the proposed scheme. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme and be further extended to a proactive MA-ABE scheme.

Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures

We propose attribute-based encryption schemes where encryptor-specified access structures (also called ciphertext policies) are hidden. By using our schemes, an encryptor can encrypt data with a hidden access structure. A decryptor obtains her secret key associated with her attributes from a trusted authority in advance and if the attributes associated with the decryptor's secret key do not satisfy the access structure associated with the encrypted data, the decryptor cannot decrypt the data or guess even what access structure was specified by the encryptor. We prove security of our construction based on the Decisional Bilinear Diffie-Hellman assumption and the Decision Linear assumption. In our security notion, even the legitimate decryptor cannot obtain the information about the access structure associated with the encrypted data more than the fact that she can decrypt the data.

3. SYSTEM ANALYSIS:

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019



System Architecture

EXISTING SYSTEM:

In order to enable Data-Providers to control the access of their own data stored on untrusted remote servers (e.g., cloud servers), encryption-based access control is an effective method, where data are encrypted by Data-Providers and only authorized users are given decryption keys. This can also prevent the data security during the transmission over wireless networks which are vulnerable to many threats. However; traditional public key encryption methods are not suitable for data encryption because it may produce multiple copies of ciphertext for the same data when there are many data consumers in the system. In order to cope with this issue, some attribute-based access control schemes are proposed by leveraging attribute-based encryption which only produces one copy of ciphertext for each data and does not need to know how many intended data consumers during the data encryption. Moreover, once the cloud data are encrypted, some searchable encryption algorithms are proposed to support search on encrypted cloud data.

DISADVANTAGES:

- Existing methods which only partially hide the attribute values in the access policies
- Data-Providers may worry that the cloud server may make wrong access decision intentionally or unintentionally, and disclose their data to some unauthorized users.
- Attribute-based access control schemes can deal with the attribute revocation problem; they all suffer from one problem: the access policy may leak privacy. This is because the access policy is associated with the encrypted data in plaintext form.

PROPOSED SYSTEM:

1. We propose an efficient and fine-gained big data access control scheme with privacy-preserving policy, where the whole attributes are hidden in the access policy rather than only the values of the attributes.

2) We also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.

3) We further give the security proof and performance evaluation of our proposed scheme, which demonstrate that our scheme can preserve the privacy from any LSSS

access policy without employing much overhead.

ADVANTAGES:

- We have proposed an efficient and fine-grained data access control scheme for big data, where the access policy will not leak any privacy information.
- our method can hide the whole attribute(rather than only its values) in the access policies
- Our scheme is selectively secure against chosen plaintext attacks.

IMPLEMENTATION

MODULES:

The system consists of five entities, namely

1. **Cloud Servers**
2. **Attribute Authority**
3. **Data-Providers,**
4. **Data Consumers**

Cloud Servers Cloud Servers are employed to store, share and process big data in the system. The cloud servers are managed by cloud service providers, who are not in the same trust domain as Data-Providers. Thus, cloud servers cannot be trusted by Data-Providers to enforce the access policy and make access decisions. We also assume that the cloud server cannot collude with any Data-Providers or Data Consumers.

Attribute Authority The attribute authority manages all the attributes in the system and assigns attributes chosen from the attribute space to Data-Providers. It is also a key generation center, where the public parameters are generated. It also grants different access privileges to Data-Providers by issuing secret keys according to their attributes. The attribute authority is assumed to be fully trusted in the system.

End-user Data-Providers are the data owners/producers who outsource their data into the cloud. They also would like to control the access of their data by encrypting the data with CP-ABE. Data-Providers are assumed to be honest in the system.

Data Consumers Data consumers request the data from cloud servers. Only when their attributes can satisfy the access policies of the data, data consumers can decrypt the data. However, data consumers may try to collude together to access some data that are not accessible individually.

4. OUTPUT RESULTS:

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

Fig 4.1:Home Page

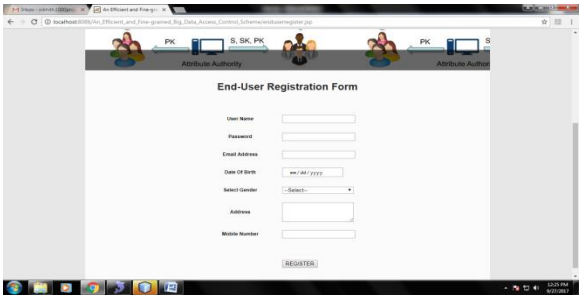


Fig 4.2: Data-Providers registration

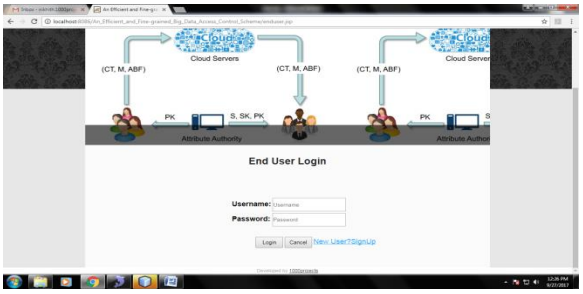


Fig 4.3: Data-Providers Login Page

Fig 4.4: Data-Providers Home page

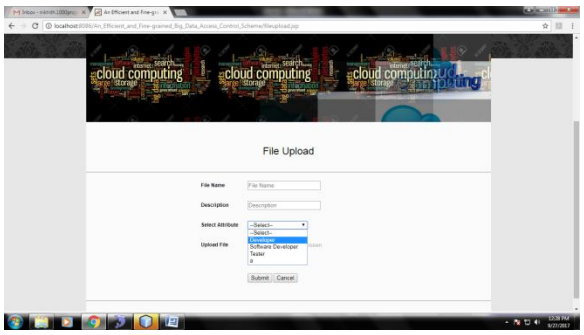


Fig 4.5: File Upload Page

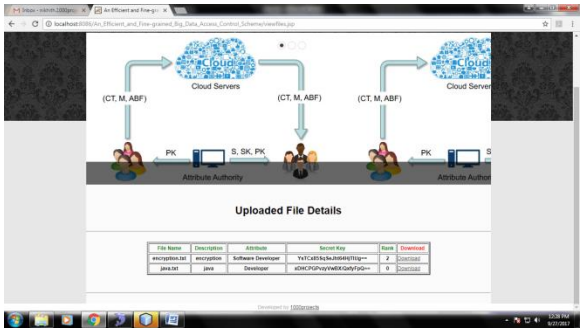


Fig 4.6: View Uploaded File Details Page

5. CONCLUSION

In this paper, we have proposed an access control scheme for big data with Equality test, where the access policy will not leak any privacy information. Different from the existing methods which only partially hide the attribute values in the access policies, our method can hide the whole attribute (rather than only its values) in the access policies. However, this may lead to great challenges and difficulties for legal data consumers to decrypt data. To cope with this problem, we have also designed an attribute localization algorithm to evaluate whether an attribute is in the access policy. In order to improve the efficiency, a novel Attribute Bloom Filter has been designed to locate the precise row numbers of attributes in the

access matrix. We have also demonstrated that our scheme is selectively secure against chosen plaintext attacks. Moreover, we have implemented the ABF by using Murmur Hash and the access control scheme to show that our scheme can preserve the privacy from any LSSS access policy without employing much overhead. In our future work, we will focus on how to deal with the offline attribute guessing attack that check the guessing "attribute strings" by continually querying the ABF.

REFERENCES

[1] C. Dong, L. Chen, and Z. Wen, "When private set intersection meets big data: an efficient and scalable protocol," in Proc. of CCS'13. ACM, 2013, pp. 789–800.

[2] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient andprivacy-preserving computing in big data era," IEEE Network, vol. 28no. 4, pp. 46–50, 2014.

[3] K. Yang and X. Jia, "Expressive, efficient, and revocable data accesscontrol for multi-authority cloud storage," IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.

[4] H. Li, D. Liu, K. Alharbi, S. Zhang, and X. Lin, "Enabling fine-grainedaccess control with efficient attribute revocation and policy updatingin smart grid," KSII Transactions on Internet and Information Systems(TIIS), vol. 9, no. 4, pp. 1404–1423, 2015.

[5] K. Yang, Z. Liu, X. Jia, and X. S. Shen, "Time-domain attribute-basedaccess control for cloud-based video content sharing: A cryptographicapproach," IEEE Trans. on Multimedia (to appear), February 2016.

[6] B. Waters, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. of PKC'11. Berlin,Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," in Proc. OfINDOCRYPT'08. Springer, 2008, pp. 426–436.

[8] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Applied cryptography and network security. Springer, 2008, pp. 111–129.

[9] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in Information Security. Springer,2009, pp. 347–362.

[10] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypteddata," in Theory of cryptography. Springer, 2007, pp. 535–554.

[11] J. Katz, A. Sahai, and B. Waters, "Predicateencryption supportingdisjunctions, polynomial equations, and inner products," in

Advancesin Cryptology–EUROCRYPT'08. Springer, 2008, pp. 146–162.

[12] J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding cpabe,"in Information Security Practice and Experience. Springer, 2011pp. 24–39.

[13] L. Lei, Z. Zhong, K. Zheng, J. Chen, and H. Meng, "Challenges on wireless heterogeneous networks for mobile cloud computing," IEEEWireless Communications, vol. 20, no. 3, pp. 34–44, 2013.

[14] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang,"Big data-driven optimization for mobile networks toward 5g," IEEENetwork, vol. 30, no. 1, pp. 44–51, 2016.

[15] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: a qoeorientedframework," IEEE Network, vol. 30, no. 1, pp. 52–57, 2016.

[16] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when qoe meets qop," IEEEWireless Communications, vol. 22, no. 4, pp. 74–80, 2015.