e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 5, Issue 6, June 2022

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.54

International Journal Of Multidisciplinary Research In Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506082 |

Attribute Based Data Management in Crypt Cloud

Mr. Lakshmi Narayanan, Navuluri Sree Valli Chandana, M.Muni pravalika

Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: Data owners will store their data in public cloud along with encryption and particular set of attributes to access control on the cloud data. While uploading the data into public cloud they will assign some attribute set to their data. If any authorized cloud user wants to download their data, they should enter that particular attribute set to perform further actions on data owner's data. A cloud user wants to register their details under cloud organization to access the data owner's data. Users want to submit their details as attributes along with their designation. Based on the user details Semi-Trusted Authority generates decryption keys to get control on owner's data. A user can perform a lot of operations over the cloud data. If the user wants to read the cloud data, he needs to be entering some read related attributes, and if he wants to write the data, he needs to be entering write related attributes. Foe each and every action user in an organization would be verified with their unique attribute set. These attributes would be shared by the admins to the authorized users in cloud organization.

I. INTRODUCTION

The prevalence of cloud computing may indirectly incur vulnerability to the confidentiality of outsourced data and the privacy of cloud users. A particular challenge here is on how to guarantee that only authorized users can gain access to the data, which has been outsourced to cloud, at anywhere and anytime. One naive solution is to employ encryption technique on the data prior to uploading to cloud.

However, the solution limits further data sharing and processing. This is so because a data owner needs to download the encrypted data from cloud and further re-encrypt them for sharing (suppose the data owner has no local copies of the data). A fine-grained access control over encrypted data is desirable in the context of cloud computing.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) may be an effective solution to guarantee the confidentiality of data and provide fine-grained access control here. In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user. Authorized cloud users then are granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data. The official in charge at the organization (e.g., university's security manager) initializes the system parameters and issues access credentials for all users (e.g., students, faculty members, and visiting scholars). Each employee is assigned with several attributes (e.g., "administrator", "senior manager", "financial officer", "tenured faculty", "tenure-track faculty", "non-tenure-track faculty", "instructors", "adjunct", "visitor", and/or "students"). Only the employees with attributes satisfying the decryption policy of the outsourced data are able to gain access to the student data stored in cloud (e.g., student admission materials).As we may have known, the leakage of any sensitive student information stored in cloud could result in a range of consequences for the organization and individuals (e.g., litigation, loss of competitive advantage, and criminal charges).In addition to the above questions, we have one more which is related to key generation authority. A cloud user's access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could we guarantee that this particular authority will not (re-)distribute the generated access credentials to others? For example, the organization security official leaks a lecturer Alice's key to an outsider Bob (who is not the employee of the university). One potential answer to the question is to employ multiple authorities. Nevertheless, this incurs additional cost in communication and infrastructure deployment and meanwhile, the problem of malicious collusion among authorities remain. Therefore, we posit that adopting an accountable authority approach to mitigate the access credential escrow problem is the preferred strategy. Seeking to mitigate access credential misuse, we propose accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing. To the best of our knowledge, this is the first practical solution to secure fine-grained access control over encrypted data in cloud. Specifically, in our work, we first present a CP-ABE based cloud storage framework. Using this (generic) framework, we propose two accountable authority and revocable CP-ABE systems (with white-box traceability and auditing) that are fully secure in the standard model, referred to as ATER-CP-ABE and ATIR-CP-ABE, respectively. Based on the two systems, we present the construction of Crypt Cloud.

II. EXISTING SYSTEM

In existing system, the CP-ABE may help us prevent security breach from outside attackers. But when an insider of the organization is suspected to commit the "crimes" related to the redistribution of decryption rights and the circulation of user information in plain format for illicit financial gains, how could we conclusively determine that the insider is guilty? Is it also possible for us to revoke the compromised access privileges? In addition to the above questions, we have one more which is related to key generation authority. A cloud user's access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could we guarantee that this particular authority will not (re-)distribute the generated access credentials to others.

III. PROPOSED SYSTEM

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing (referred to as Crypt Cloud+). This is the first CP-
ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, Crypt Cloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority.

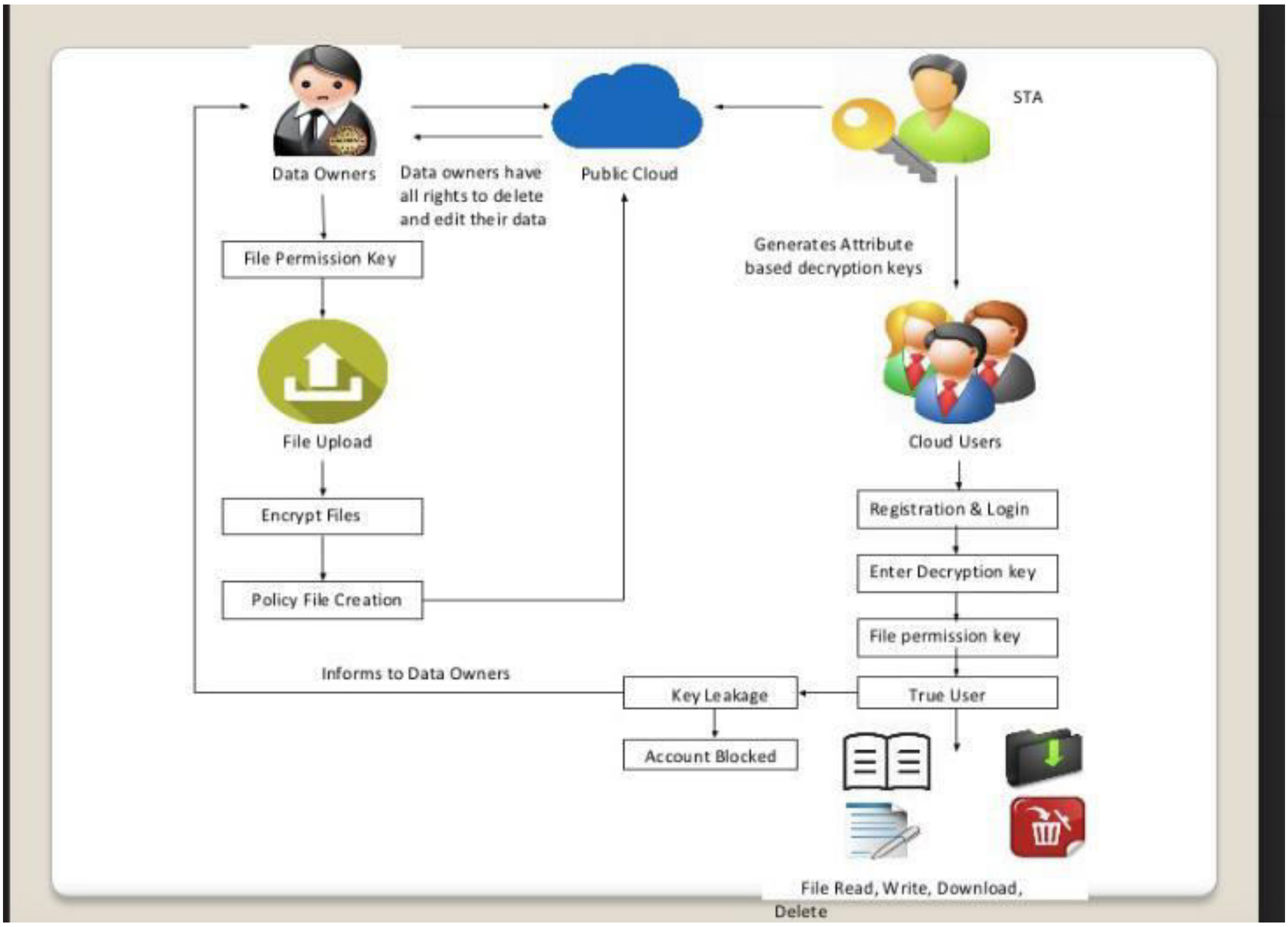
AIM:
The main aim of this project is to provide integrity of an organization data which is in public cloud.

OBJECTIVE:
Data owners will store their data in public cloud along with encryption and particular set of attributes to access control on the cloud data. While uploading the data into public cloud they will assign some attribute set to their data. If any authorized cloud user wants to download their data, they should enter that particular attribute set to perform further actions on data owner's data. A cloud user wants to register their details under cloud organization to access the data owner's data. Users want to submit their details as attributes along with their designation. Based on the user details Semi-Trusted Authority generates decryption keys to get control on owner's data. A user can perform a lot of operations over the cloud data. If the user wants to read the cloud data, he needs to be entering some read related attributes, and if he wants to write the data, he needs to be entering write related attributes.

PROBLEM STATEMENT:
Data owners will store their data in public cloud along with encryption and set of attributes to access control on the cloud data. While uploading the data into public cloud they will assign some attribute set to their data. A cloud user wants to register their details under cloud organization to access the data owner's data. Users want to submit their details as attributes along with their designation. Based on the user details Semi-Trusted Authority generates decryption keys to get on owner's data. A user can perform a lot of operations over the cloud data. If the user wants to read the cloud data, he needs to be entering some read related attributes, and if he wants to write the data, he needs to be entering write related attributes.

Algorithm
Binary search
Binary search is a fast search algorithm with run-time complexity of O (log n). ... For this algorithm to work properly, the data collection should be in the sorted form. Binary search looks for a particular item by comparing the middle most item of the collection. If a match occurs, then the index of item is returned.

ARCHITECTURE DIAGRAM:



IV. CONCLUSION

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable CryptCloud which supports white-box traceability and auditing (referred to as CryptCloud+). This is the first CP-ABE based. cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, CryptCloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority. We note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in. CryptCloud. One of our future works is to consider the black-box traceability and auditing.

REFERENCES

[1] M. Ali, et al., "SeDaSC: Secure data sharing in clouds," IEEE Syst.J., vol. 11, no. 2, pp. 395–404, Jun. 2017.
[2] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud com-puting: Opportunities and challenges," Inf. Sci., vol. 305, pp. 357–383, 2015.
[3] M. Armbrust, et al., "A view of cloud computing," Commun. ACM,vol. 53, no. 4, pp. 50–58, 2010.
[4] N. Attrapadung and H. Imai, "Attribute-based encryption sup-porting direct/indirect revocation modes," in Proc. IMA Int. Conf. Cryptography Coding, 2009, pp. 278–300.
[5] A. Beimel, "Secure schemes for secret sharing and key distribu-tion," PhD thesis, Israel Inst. Technol., Faculty of computer science, Technion, Haifa, Israel, 1996.
[6] M. Bellare and O. Goldreich, "On defining proofs of knowledge,"in Proc. Annu. Int. Cryptology Conf., 1992, pp. 390–420.

[7] D. Boneh and X. Boyen, “Short signatures without random oracles,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, pp. 56–73.
[8] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, “IoT-based big data storage systems in cloud computing: Perspectives and challenges,”IEEE Internet Things J., vol. 4, no. 1, pp. 75–87, Feb. 2017.
[9] J. Chen, R. Gay, and H. Wee, “Improved dual system ABE in prime-order groups via predicate encodings,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2015, pp. 595–624.
[10] A. De Caro and V. Iovino, “jPBC: Java pairing based cryptography,”in Proc. IEEE Symp. Comput. Commun., 2011, pp. 850–855.
[11] H. Deng, et al., “Who is touching my cloud,” in Proc. Eur. Symp.Res. Comput. Secur., 2014, pp. 362–379.
[12] Z. Fu, F. Huang, X. Sun, A. Vasilakos, and C.-N. Yang, “Enablingsemantic search based on conceptual graphs over encrypted out-sourced data,” IEEE Trans. Serv. Comput., 2016, doi:10.1109/TSC.2016.2622697.
[13] V. Goyal, “Reducing trust in the PKG in identity based cryptosystems,” in Proc. Annu. Int. Cryptology Conf., 2007, pp. 430–447.
[14] V. Goyal, S. Lu, A. Sahai, and B. Waters, “Black-box accountableauthority identity-based encryption,” in Proc. 15th ACM Conf.Comput. Commun. Secur., 2008, pp. 427-436.
[15] 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. Comput. Commun. Secur., 2006, pp. 89–98.
[16] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: Perspectives and challenges,” Wireless Netw., vol. 20, no. 8, pp. 2481–2501, 2014.
[17] A. Lewko, “Tools for simulating features of composite order bilin-ear groups in the prime order setting,” in Proc. Annu. Int. Conf.Theory Appl. Cryptographic Techn., 2012, pp. 318–335.
[18] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters,“Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2010, pp. 62–91.
[19] A. Lewko and B. Waters, “New proof methods for attribute-based encryption: Achieving full security through selective techniques,” in Proc. Annu. Int. Cryptology Conf., 2012, pp. 180–198.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com