IJMRSET

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.2022.0506088 |

Attribute Based Data Management in Crypt Cloud

Naveen Kumar K, Navabharathi V, Selvakanmani S

U.G Scholar, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

U.G Scholar, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

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

ABSTRACT: Enabling cryptographically enforced access controls for data hosted in untrusted cloud is attractive for many users and organizations. However, designing efficient cryptographically enforced dynamic access control system in the cloud is still challenging. In this paper, we propose Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Crypt-DAC revokes access permissions by delegating the cloud to update encrypted data. In Crypt-DAC, a file is encrypted by a symmetric key list which records a file key and a sequence of revocation keys. In each revocation, a dedicated administrator uploads a new revocation key to the cloud and requests it to encrypt the file with a new layer of encryption and update the encrypted key list accordingly. Crypt-DAC proposes three key techniques to constrain the size of key list and encryption layers. As a result, Crypt-DAC enforces dynamic access control that provides efficiency, as it does not require expensive decryption/reencryption and uploading/re-uploading of large data at the administrator side, and security, as it immediately revokes access permissions. We use formalization framework and system implementation to demonstrate the security and efficiency of our construction.

I. INTRODUCTION

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. An 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 Crypt-DAC enforces dynamic access control that provides efficiency, as it does not require expensive decryption, re encryption and uploading/re-uploading of large data at the administrator side, and security, as it immediately revokes access permissions.

II. LITERATURE SURVEY

Vipul Goyal, OmkantPandeyy, Amit Sahai, “Attribute-Based Encryption for Fine-Grained Access Control oF Encrypted Data”, 2006. User's private keys will consist of a group element for every leaf in the key's corresponding access tree. This will increase the efficiency of the scheme in terms of cipher text size, private key size, and computation time for decryption and encryption. For the decryption algorithm to do some type of exploration of the access tree relative to the cipher text attributes before it makes cryptographic computations.

Rafail Ostrovsky, Amit Sahai Brent Waters, “Attribute-Based Encryption with Non-Monotonic Access Structures”, 2007. The previous ABE schemes were limited to expressing only monotonic access structures.

This Scheme provides a proof of security. The access decisions depend upon attributes of the protected data and access policies assigned to users. Both the servers and their storage must be trusted and remain uncompromised

Sascha M¨uller and Stefan Katzenbeisser, "Hiding the Policy in Cryptographic Access Control", 2011. The cryptographic access control has received a lot of attention, mainly due to the availability of efficient Attribute-Based Encryption (ABE) schemes. ABE has a privacy problem: The access policies are sent in clear along with the cipher texts. It is also possible to automatically extract such policies from policies written in the Open Digital Rights Language (ODRL).

John Bethencourt, Amit Sahai, "Cipher text-Policy Attribute-Based Encryption", 2008. The cipher text policy attribute based encryption method allows enforcing such policies to employ a trusted server to store the data and mediate access control. By using these techniques, encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks

Dr.Ragesh G. K.a, Dr. K. Baskaranb, "Cryptographically Enforced Data Access Control in Personal Health Record Systems", 2016. The record systems provide many value-added features like viewing one's health related information, secure transmission and tracking of that information with the health service providers. The proposed scheme inherits flexibility, scalability and fine-grained patient centric data access control.

Xiaoguang Wang, Yong Qi, "Design and Implementation of Sec Pod, A Framework for Virtualization-based Security Systems", 2017. The OS kernel is difficult to the security so the fundamental weakness of those systems is that page tables, the data structures that control the memory protection, are not isolated from the vulnerable kernel, and thus subject to tampering. A practical and extensible framework for virtualization-based security systems that can provide both strong isolation and the compatibility with modern hardware.

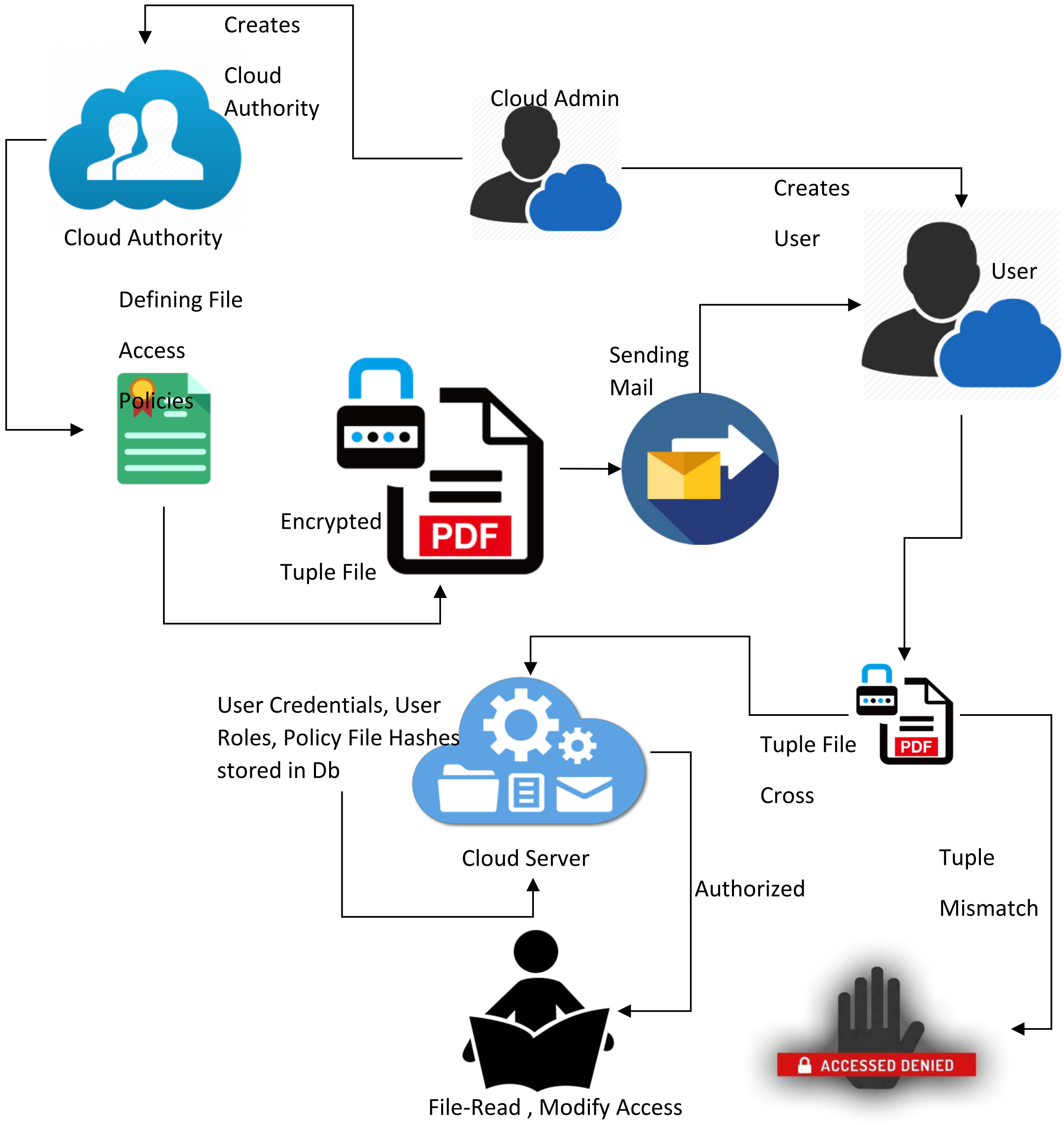
Xiaofeng Chen, Jin Li, Xinyi Huang, "New Publicly Verifiable Databases with Efficient Updates", 2014. The notion of verifiable database (VDB) enables a resource-constrained client to securely outsource a very large database to an untrusted server so that it could later retrieve a database record and update it by assigning a new value. The construction is not only public verifiable but also secure under the FAU attack.

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

| Volume 5, Issue 6, June 2022 |

| DOI:10.15680/IJMRSET.2022.0506088 |

III. PROPOSED SYSTEM



Role Creation

The roles will be created for employee and the cloud authority. The roles will be created based on their designation. The employee and the cloud authority will get added based on their designation and roles.

Admin File Upload

The admin will upload the file which is of two types. They are public and private files. The admin will add the news. If the file is public, it does not contain any access permission. If the file is private, then the tuples will get generated.

Tuple Generation

Here file permission keys are issued to the employees in the organization based on their experience and position to their registered. Senior Employees have all the permission to access the files (read, write, delete, & download). Freshers or trainee only having the permission to read the files. Some Employees have the permission to read and write. And some employees have all the permissions except deleting the data. If any Senior Employee leaks or shares their secret permission keys to their junior employees they will request to download or delete the Data Owners Data. Tuples are the encrypted PDF files which will be generated while the employee logs in. These tuples will get generated based on the roles of employee and the cloud authority.

User File Access

Authorized DUs are able to access (e.g. read, write, download, delete and decrypt) the outsourced data. While entering the password for re-encryption system, it will generate attribute set for their role in background validate that the user has all rights to access the data. If the attributes set is not matched to the Data Owners policy files they will be claimed as guilty. If we ask them, we will find who leaked the key to the junior employees. If any employee does an illegal access of files without any permission, they will be warned for 3 times. If they continue the access, they will get captured by the camera and send as a notification to the admin.

IV. RESULT

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. This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, Crypt-DAC, a cryptographically enforced dynamic access control system on untrusted cloud. Crypt-DAC delegates the cloud to update encrypted files in permission revocations. Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority

V. CONCLUSION AND FUTURE SCOPE

In this work, we have present Crypt-DAC, a cryptographically enforced dynamic access control system on un-trusted cloud. To overcome the onion encryption, we propose Tuple for security purpose. Every time user should upload the tuple file while accessing the cloud files. If the tuple verification is success, you can access the files otherwise admin sent you a warning message three times and then admin will block you at the same time camera will capture your face and sent to admin.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption, in IEEE S&P, 2007.

[2] X. Wang, Y. Qi, and Z. Wang, Design and Implementation of SecPod: A Framework for Virtualization-based Security Systems, IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, 2019.

[3] J. Ren, Y. Qi, Y. Dai, X. Wang, and Y. Shi, AppSec: A Safe Execution Environment for Security Sensitive Applications, in ACM VEE, 2015.

[4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, Bounded ciphertext policy attribute based encryption, in ICALP, 2008.

[5] V. Goyal, O. Pandey, A. Sahai, and B.Waters, Attribute-based encryption for fine-grained access control of encrypted data, in ACM CCS, 2006.

[6] J. Katz, A. Sahai, and B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, in EUROCRYPT, 2008.

[7] S. Muller and S. Katzenbeisser, Hiding the policy in cryptographic access control, in STM, 2011.

[8] R. Ostrovsky, A. Sahai, and B. Waters, Attribute-based encryption with non-monotonic access structures, in ACM CCS, 2007.

[9] A. Sahai, and B. Waters, Fuzzy identity-based encryption, in EUROCRYPT, 2005.

[10] T. Ring, Cloud computing hit by celebgate, http://www.scmagazineuk. com/cloudcomputing-hit-by-celebgate/article/370815/, 2015.

[11] X. Jin, R. Krishnan, and R. S. Sandhu, A unified attribute-based access control model covering DAC, MAC and RBAC, in DDBSec, 2012.

[12] W. C. Garrison III, A. Shull, S. Myers, and, A. J. Lee, On the Practicality of Cryptographically Enforcing Dynamic Access Control Policies in the Cloud, in IEEE S&P, 2016.

[13] R. S. Sandhu, Rationale for the RBAC96 family of access control models, in ACM Workshop on RBAC, 1995.

[14] T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, Secure and Efficient Cloud Data Deduplication With Randomized Tag, IEEE Trasactions on Information Forensics and Security, vol. 12, no. 3, 2017.

[15] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, Plutus: Scalable Secure File Sharing on Untrusted Storage, in USENIX FAST, 2003.

[16] J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, Verifiable Auditing for Outsourced Database in Cloud Computing, IEEE Transactions on Computers, vol. 64, no. 11, 2015.

[17] J. Wang, X. Chen, J. Li, J. Zhao, and J. Shen, Towards achieving flexible and verifiable search for outsourced database in cloud computing, Future Generation Computer Systems, vol. 67, 2017.

[18] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, New Publicly Verifiable Databases with Efficient Updates, IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, 2015.

[19] T. Jiang, X. Chen, and J. Ma, Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation, IEEE Transactions on Computers, vol. 65, no. 8, 2016.

[20] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM Journal on Computing, vol. 32, no. 3, 2003.

BIOGRAPHY

Naveen Kumar K is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on attribute based dynamic cloud access control.

Navabharathi V is a B.E. final year student in the department of Computer Science and Engineering from Velammal Institute of Technology, Panchetti. His current research focuses on attribute based dynamic cloud access control.

Dr.S.Selvakanmani, M.E.,Ph.D., is HOD of Computer Science and Engineering Department in VelammalInstitue of Technology, Panchetti.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor
7.54

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com