International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 30th June 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-06

Title: **CLOUD STORAGE SYSTEM WITH ATTRIBUTE-BASED ENCRYPTION FOR MULTI-AUTHORITY DATA ACCESS CONTROL**

Volume 09, Issue 06, Pages: 135-141

Paper Authors

ALURU SUSHMA, C.BALAJI

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CLOUD STORAGE SYSTEM WITH ATTRIBUTE-BASED ENCRYPTION FOR MULTI-AUTHORITY DATA ACCESS CONTROL

ALURU SUSHMA, C.BALAJI

PG SCHOLAR.DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE, AP, INDIA
ASSOCIATE PROFESSOR, DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE,, AP, INDIA

ABSTRACT: Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights), due to the intrinsic "all-or-nothing" decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi-trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as CryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

1. 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 [3]. 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 [51]. Ciphertext-Policy Attribute-Based Encryption (CPABE) [15] 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 UniversityofTexasatSanAntonio)andindividuals(e.g.,students,facultymembers and visiting scholars of the university) can first specify access policyoverattributesofapotentialclouduser.Authorizedcloudusersthenaregrantedaccesscredentials (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. As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access control over the data. Generally speaking, the existing CP-ABE based cloud storage systems fail to consider the case

where access credential is misused. For instance, a university deploys a CPABE based cloud storage system to outsource encrypted student data to cloud under some access policies that are compliant with the relevant data sharing and privacy legislation (e.g., the federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act of 1992 (HIPAA)). 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","seniormanager","finan cialofficer", "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). 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 ofstudentinformationinplainformatforillicitfi nancialIsitalsopossibleforustorevokethecom promised 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? 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 remains. Therefore, we posit that adopting an accountable authority approach to mitigate the access credential escrow problem is the preferred strategy. Seeking to mitigate accesscredentialmisuse,wepropose CryptCloud+, an accountable authority and revocable CPABEbasedcloudstoragesystemwithwhite-boxtraceability 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 whitebox traceability and auditing) that are fully secure in the standardmodel,referredtoasATER-CP-ABEandATIR-CPABE, respectively. Based on the two systems, we present the construction of CryptCloud+ that provides the following features. 1) Traceability of malicious cloud users. Users who leak their access credentials can be traced and identified. 2) Accountable authority. A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for

damages and breach of contract). 3) Auditing. An auditor can determine if a (suspected) cloud user is guilty in leaking his/her access credential. 4) "Almost" zero storage requirement for tracing. We use a Paillierlikeencryptionasanextractablecommitmentintracingmaliciouscloudusersandmorepractically, we do not need to maintain an identity table of users for tracing (unlike the approach used in [27]). 5) Malicious cloud users revocation. Access credentials for individual traced and further determined to be "compromised" can be revoked. We design two mechanisms to revoke the "traitor(s)" effectively. The ATER-CP-ABE provides an explicitly revocation mechanism where a revocation list is specified explicitly into the algorithm Encrypt, while the ATIRCP-ABE offers an implicitly revocation where the encryption does not need to know the revocation list but a key update operation is required periodically. This paper extends our earlier work (a conference version in [35]), as follows.

1) We present a formal framework model of the proposed system, designed for practical cloud storage system deployment.

2) We address a weakness in the auditing procedure of the conference version. Specifically, a malicious user may change tid of his secret key in the conference version, and the auditing procedure will fail in this case. As a mitigation, we revise the key generation algorithm and add an audit list to detect if the tid is changed.

3) We enhance the functionality of the construction (w.r.t. AAT-CP-ABE) proposed in the conference version and further present two enhanced constructions, namely ATER-CP-ABE and ATIR-CP-ABE. These constructions allow us to effectively revoke the malicious users explicitly or implicitly. We also present the new definitions, technique and related materials of ATER-CP-ABE and ATIR-CP-ABE.

4) Based on the new ATER-CP-ABE and ATIR-CPABE, we present CryptCloud+ which is an effective and practical solution for secure cloud storage. 5) We provide general extensions (of our system) on the large universe, the multi-use, and the prime-order setting cases, so that the solution introduced in this paper is more scalable in real-world applications.

6) We comprehensively evaluate the efficiency of the proposed ATER-CP-ABE and ATIR-CP-ABE via experiments.

2. EXISTING SYSTEM

Li et al. introduce the notion of accountable CP-ABE to prevent unauthorized key distribution among colluded users. In a later work [22], a user accountable multi-authority CP-ABE system is proposed. Liu et al. also proposed white-box and black-box traceability 1 CP-ABE systems supporting policy expressiveness in any monotone access structures. Ning et al. propose several practical CP-ABE systems with white-box traceability and black-box traceability. Deng et al. [11] provide a tracing mechanism of CP-ABE to find the leaked access credentials in cloud storage system. Sahai et al. [40] define the problem of revocable storage and provide a fully secure construction for ABE based on ciphertext delegation. Yang et al. [49] propose a revocable multi-authority CP-ABE system that achieves both forward and backward security. More recently, Yang et al. [50] propose an attribute updating method to achieve the dynamic change on attribute (such as revoking previous attribute and re-granting previously revoked attribute). There is less security on outsourced data due to lack of Verification Based on Hash code.There is no more security in the data access.

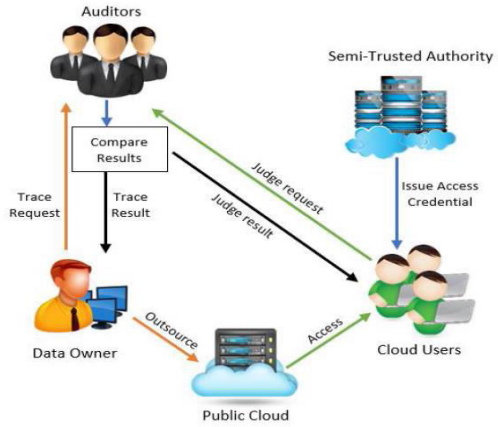
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3. PROPOSED SYSTEM

The proposed system presents a formal framework model of the proposed system, designed for practical cloud storage system deployment. The system addresses a weakness in the auditing procedure of the conference version. Specifically, a malicious user may change tid of his secret key in the conference version, and the auditing procedure will fail in this case. As a mitigation, we revise the key generation algorithm and add an audit list to detect if the tid is changed.The system enhances the functionality of the construction (w.r.t. AAT-CP-ABE) proposed in the conference version and further present two enhanced constructions, namely ATER-CP-ABE and ATIR-CP-ABE. These constructions allow us to effectively revoke the malicious users explicitly or implicitly. We also present the new definitions, technique and related materials of ATER-CP-ABE and ATIR-CP-ABE. Based on the new ATER-CP-ABE and ATIR-CPABE, we present CryptCloud+ which is an effective and practical solution for secure cloud storage. The system provides general extensions (of our system) on the large universe, the multi-use, and the prime-order setting cases, so that the solution introduced in this paper is more scalable in real-world applications. The system comprehensively evaluates the efficiency of the proposed ATER-CP-ABE and ATIR-CP-ABE via experiments.

Traceability of malicious cloud users. Users who leak their access credentials can be traced and identified. Accountable authority. A semi-trusted authority, who (without proper authorization) generates and further distributes access credentials to unauthorized user(s), can be identified. This allows further actions to be undertaken (e.g. criminal investigation or civil litigation for damages and breach of contract). Auditing. An auditor can determine if a (suspected) Cloud

4. ARCHITECTURE



5. IMPLEMENTATION

Data Owner

In this module, the data owner performs operations such as Attackers, Upload File, View Files, Send Trace Request and Trace Files, Delete Files, Transactions

Data User

In this module, he logs in by using his/her user name and password. After Login receiver will perform operations like View my Profile, View Files , Search Files, Search Ratio, Top K Search, Request Search Access Issue Credentials

Auditor

In this module, the sector can do following operations View Files, View Trace Request and Give Permission

Semi Trusted Authority

In this module, the sector can do following operations Request Search Issue Credentials

Public Cloud

The Cloud manages a server to provide data storage service and can also do the following operations such as View Users and Authorize, View Owners and Authorize ,View Files, View File Transactions, View Top Searched Files, View Attackers , View

Search Model, View Time Delay, View Throughput

6. CONCLUSION AND FUTURE WORK

In this work, we have addressed the challenge of credential leakageinCP-ABEbasedcloudstoragesystembydesigning 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. Furthermore, AU is assumed to be fully trusted in CryptCloud+. However, in practice, it may not be the case. Is there any way to reduce trust from AU? Intuitively, one method is to employ multiple AUs. This is similar to the technique used in threshold schemes. But it will require additional communication and deployment cost and meanwhile, the problem of collusion among AUs remains. Another potential approach is to employ secure multi-party computation in the presence of malicious adversaries. However, the efficiency is also a bottleneck. Designing efficient multi-party computation and decentralizing trust among AUs (while maintaining the same level of security and efficiency) is also a part of our future work. We use Paillier-like encryption to serve as an extractable commitment to achieve white-box traceability. From an abstract view point, any extractable commitment may be employed to achieve white-box traceability in theory. To improve the efficiency of tracing, we may make use of a more light-weight (pairing-suitable) extractable commitment. Also, the trace algorithm in CryptCloud+ needs to take the master secret key as input to achieve white-box traceability of malicious cloud users. Intuitively, the proposed CryptCloud+ is private traceable5. Private traceability only allows the tracing algorithm to be run by the system administrator itself, while partial/full public traceability enables the administrator, authorized users and even anyone without the secret information of the system to fulfill the trace. Our future work will include extending CryptCloud+ to provide "partial" and fully public traceability without compromising on performance.

REFERENCES

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

[2] MazharAli,SameeU.Khan,andAthanasiosV. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.

[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

[4] Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

[5] Amos Beimel. Secure schemes for

secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[6] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.
[7] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.
[8] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.
[9] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.
[10] Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.
[11] Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.
[12] Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.
5. As noted in [36], there three types of traceability, namely: private traceability, partial public traceability and fully public traceability.
1939-1374 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/ publications/rights/index.html for more information.
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2791538, IEEE Transactions on Services Computing
13
[13] Vipul Goyal. Reducing trust in the PKG in identity based cryptosystems. InAdvancesinCryptology-CRYPTO2007,pages430–447. Springer, 2007.
[14] Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.
[15] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. InProceedingsofthe13thACMconferenceonComputer and communications security, pages 89–98. ACM, 2006.
[16] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: perspectives and challenges. Wireless Networks, 20(8):2481–2501, 2014.
[17] Allison Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Advances in Cryptology–EUROCRYPT 2012, pages 318–335. Springer, 2012.
[18] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Advances in Cryptology–EUROCRYPT 2010, pages 62–91. Springer, 2010.
[19] Allison Lewko and Brent Waters. New

proof methods for attribute-based encryption: Achieving full security through selective techniques. In Advances in Cryptology–CRYPTO 2012, pages 180–198. Springer, 2012. [20] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. KSFOABE: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Trans. Services Computing, 10(5):715–725, 2017.

[21] JiguoLi,WeiYao,YichenZhang,HuilingQian, andJinguangHan. Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Trans. Services Computing, 10(5):785–796, 2017.

[22] Jin Li, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, Duncan S Wong, and Dongqing Xie. Multi-authority ciphertext-policy attribute-basedencryptionwithaccountability. InProceedingsofthe 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, pages 386–390. ACM, 2011.

[23] Jin Li, Kui Ren, and Kwangjo Kim. A2be: Accountable attributebased encryption for abuse free access control. IACR Cryptology ePrint Archive, 2009:118, 2009.

[24] Jiaqiang Liu, Yong Li, Huandong Wang, Depeng Jin, Li Su, Lieguang Zeng, and Thanos Vasilakos. Leveraging softwaredefined networking for security policy enforcement. Inf. Sci., 327:288–299, 2016.

[25] QiangLiu,HaoZhang,JiafuWan,andXinChen. Anaccesscontrol model for resource sharing based on the role-based access control intendedformulti-domainmanufacturinginternetofthings. IEEE Access, 5:7001–7011, 2017.

[26] Zhen Liu, Zhenfu Cao, and Duncan S Wong. Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 475–486. ACM, 2013.

[27] Zhen Liu, Zhenfu Cao, and Duncan S Wong. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Transactions on Information Forensics and Security, 8(1):76–88, 2013.

[28] Ben Lynn et al. The pairing-based cryptography library. Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.