IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003197

Attribute Based Data Management in Crypt Cloud

Mohammed Feroz S, Naresh Balaji D, Vignesh s, Mr. Retheesh D

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTARCT: 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. Cipher text 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 Crypt Cloud. We also present the security analysis and further demonstrate the utility of our system via experiments.Data owners will store their data in public cloud along with encryption and particular set of attributes to access control on the cloud data.Cloud owners have all rights to download and delete their data whenever they want While uploading the data into public cloud they will assign some attribute set to their data.

KEYWORDS: Cipher text Policy attribute based encryption,security analysis, secure cloud

I. INTRODUCTION

Cloud Computing provides us means of accessing the applications as utilities over the Internet.It allows us to create, configure, and customize the applications online. The term Cloud refers to a Network or Internet**.** In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, VPN.Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud. Cloud Computing refers to manipulating**,** configuring**,** and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

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. These attributes will be stored in the policy files in a cloud. If any user leaks their unique decryption key to the any malicious user data owners wants to trace by sending audit request to auditor and auditor will process the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003197

data owners request and concludes that who is the guilty.

II. LITERATURE SURVEY

Project Title: Attribute Based Data Sharing with Attribute Revocation

Author Name:Shucheng, YuCong Wang, Kui Ren

Year of publishing: 2010
Abstract:
Cipher text-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure. Beside this basic property, practical applications usually have other requirements. In this paper we focus on an important issue of attribute revocation which is cumbersome for CP-ABE schemes. In particular, we re-solve this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available. As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort. We achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy servers. Formal analysis shows that our proposed scheme is provably secure against chosen cipher text attacks. In ad- dictions, we show that our technique can also be applicable to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart.

Project Title: Cloud data integrity checking with an identity-based auditing mechanism from RSA

Author Name:Yong Yua, Liang Xuea, Man Ho Aub, Willy Susilo, Jianbing Ni, Yafang Zhanga, Athanasios V. Vasilakos, Jian Shene

Year of publishing: 3 March 2016
Abstract:
Cloud data auditing is extremely essential for securing cloud storage since it enables cloud users to verify the integrity of their outsourced data efficiently. The computation overheads on both the cloud server and the verifier can be significantly reduced by making use of data auditing because there is no necessity to retrieve the entire file but rather just use a spot checking technique. A number of cloud data auditing schemes have been proposed recently, but a majority of the proposals are based on Public Key Infrastructure (PKI). There are some drawbacks in these protocols: (1) It is mandatory to verify the validity of public key certificates before using any public key, which makes the verifier incur expensive computation cost. (2) Complex certificate management makes the whole protocol inefficient. To address the key management issues in cloud data auditing, in this paper, we propose ID-CDIC, an identity-based cloud data integrity checking protocol which can eliminate the complex certificate management in traditional cloud data integrity checking protocols. The proposed concrete construction from RSA signature can support variable-sized file blocks and public auditing. In addition, we provide a formal security model for ID-CDIC and prove the security of our construction under the RSA assumption with large public exponents in the random oracle model. We demonstrate the performance of our proposal by developing a prototype of the protocol. Implementation results show that the proposed ID-CDIC protocol is very practical and adoptable in real life.
Project Title: Leveraging software defined networking for security policy enforcement

Author Name:iaqiangLiu,YongLi,HuandongWang, DepengJin, LiSu, LieguangZeng, ThanosVasilakos
Year of publishing: 21August2015
Abstract:
Network operators employ a variety of security policies for protecting the data and services. However, deploying these policies intraditional network is complicated and security vulner able due to the distributed network control and lack of standard control protocol. Software defined network provide sanideal paradigm to address these challenges by separating control plane and d tap lane, and exploiting the logically centralized control. In this paper, we focus on taking the advantage of software-defined networking for security policies enforcement. We propose at wo layer Open Flows witch topology designed to implement security policies, which considers the limitation off low table size in a single switch, the complexity of configuring security policies to these switches, and load balance among these switches. Furthermore, we introduce a safe way to update the configuration of these switches one by one for better load balance

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003197

when traffic distribution changes. Specifically, we model the update process as a path in a graph, in which each no derepresents a security policy satisfied configuration, and each edge represents a single step of safely update. Based on this model, we design a heuristic algorithm to find an optimal update path in real time. Simulations of the update schemes how that our proposed algorithm is effective and robust under an extensive range of conditions.

Project Title: SeDaSC: Secure Data Sharing in Clouds

Author Name:Mazhar Ali, Revathi Dhamotharan Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos Keqin Li, Albert Y. Zomaya
Year of publishing: 20 April 2015
Abstract:
Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. In case of group-shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive re encryption; 4) insider threat security; and 5) forward and backward access control. The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations. We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be encouraging and show that SeDaSC has the potential to be effectively used for secure data sharing in the cloud.

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.

IV. EXPERIMENTAL RESULTS

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

V. 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 3, March 2021 ||

DOI:10.15680/IJIRSET.2021.1003197

stronger notion (compared to white-box traceability), in CryptCloud. One of our future works is to consider the black-box traceability and auditing.

VI. FUTURE ENHANCEMENT

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.

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]Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.
[3]Michael Armbrust, Armando Fox, R ean 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 -2014,pages 53-70,2004
[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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details