National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

Online Data Sharing Using Secure Key Aggregate Cryptosystem on Cloud

Supriya M*[1], Pushpalatha R[2]
*[1]M.Tech in CS&E, VTU PG Centre, Mysuru, Karnataka, India
[2]Assistant Professor, DoS in CS&E, VTU PG Centre, Mysuru, Karnataka, India

ABSTRACT

Sharing of data in cloud is widely used now a day. Cloud is used for storing data and applications on servers and accessing them through internet. Online data sharing for improved productivity and efficiency is one of the primary requirements today for any organization. In cloud, data is stored on single machine and this stored data shared among multiple users by different machines. To store and for sharing data securely cryptosystem is used. The data owner encrypt the data before it is upload to the cloud and then data decryption is done when user want to access it. In the existing system owner needs to generate individual key to the individual user. To overcome this problem in proposed system we generate an aggregate key and broadcast.

Keywords: Cloud, cryptosystem, encrypt, internet, decryption

I. INTRODUCTION

Outsourcing of data is increasingly demanded in enterprise settings. In outsourcing of data, there are chances of stolen data from virtual machine. On separate virtual machine is used to access the data of cloud stored on single physical machine. Proposed system supports KAC scheme, which contains various security levels. In availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner. When the user is not perfectly happy with trusting the security of the virtual machine. The shared data in cloud servers, however usually contains user's sensitive information such as personal profile, financial data health records etc…and needs to be well protected. Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed encryption. The main aim of cryptography is to take care of data secure from attacker. Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, with storage size more than 25GB (or a few dollars for more than 1TB).Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any corner of the world.

II. RELATED WORKS

2.1 Spice–simple privacy-preserving identity-management for cloud environment:

According to Sherman SM Chow, Yi-Jun He Identity security and privacy have been regarded as one of

the top seven cloud security threats. There are a few identity management solutions proposed recently trying to tackle these problems. However, none of these can satisfy all desirable properties. In particular, unlinkability ensures that none of the cloud service providers (CSPs), even if they collude, can link the transactions of the same user. On the other hand, delegatable authentication is unique to the cloud platform, in which several CSPs may join together to provide a packaged service, with one of them being the source provider which interacts with the clients and performs authentication while the others will be transparent to the clients. Note that CSPs may have different authentication mechanisms that rely on different attributes. Moreover, each CSP is limited to see only the attributes that it concerns. This paper presents SPICE – the first digital identity management system that can satisfy these properties in addition to other desirable properties.

2.2 Dynamic secure cloud storage with provenance:

According to Sherman SM Chow, Cheng-Kang Chu One concern in using cloud storage is that the sensitive data should be confidential to the servers which are outside the trust domain of data owners. Another issue is that the user may want to preserve his/her anonymity in the sharing or accessing of the data (such as in Web 2.0 applications). To fully enjoy the benefits of cloud storage, we need a confidential data sharing mechanism which is fine-grained (one can specify who can access which classes of his/her encrypted files), dynamic (the total number of users is not fixed in the setup, and any new user can decrypt previously encrypted messages), scalable (space requirement does not depend on the number of decryptors), accountable (anonymity can be revoked if necessary) and secure (trust level is minimized).This paper addresses the problem of building a secure cloud storage system which supports dynamic users and data provenance. Previous system is based on specific constructions and does not offer all of the aforementioned desirable properties. Most importantly, dynamic user is not supported. We study the various features offered by cryptographic anonymous authentication and encryption mechanisms; and instantiate our design with verifier-local revocable group signature and identity-based broadcast encryption with constant size cipher texts and private keys.

III. PROBLEMS DEFINITION

In a shared-tenancy cloud-computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Data in a target VM could be stolen by instantiating another VM coresident with the target one. Regarding availability of files, there are a series of cryptographic schemes, which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data anonymity.

IV. SYSTEM ANALYSIS

A. Existing System

Current technology for secure online data sharing comes in two major flavors - trusting a third party auditor, or using the user's own key to encrypt her data while preserving anonymity. This system is popularly known as the key-aggregate cryptosystem (KAC), and derives its roots from the seminal work on broadcast encryption by Boneh et.al.. KAC may essentially be considered as a dual notion of broadcast encryption. In broadcast encryption, a single cipher text is broadcast among multiple users, each of whom may decrypt the same using their own individual private keys. In KAC, a single aggregate key is distributed among multiple users and may be used to decrypt cipher texts encrypted with respect to different classes.

B. Proposed System

In this paper, we attempt to build precisely such a data sharing framework that is provably secure and at the same time, efficiently implementable. In this

paper, we propose an efficiently implementable version of the basic key-aggregate cryptosystem (KAC) using asymmetric bilinear pairings. We propose a CCA-secure fully collusion resistant construction for the basic KAC scheme with low overhead cipher texts and aggregate keys. We demonstrate how the basic KAC framework may be efficiently extended and combined with broadcast encryption schemes for distributing the aggregate key among an arbitrary number of data users in a real-life data-sharing environment. The extension has a secure channel requirement of O (m + m0) for m data users and m0 data owners. In addition, the extended construction continues to have the same overhead for the public parameters, cipher texts and aggregate keys, and does not require any secure storage for the aggregate keys, which are publicly broadcast.

V. SYSTEM ARCHITECTURE

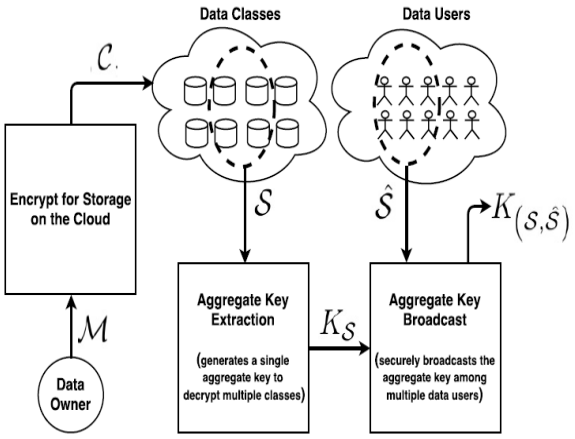

Figure 1. System Architecture

Data owner:

1.First the Data owners register with the respective Registration form.

2. Data owner can login only using secrete key sent by cloud.

3. Data owner upload their files with cloud in an encrypted format.

Data User:

1. Data users also register with the respective registration form.

2. Data users also can login only using secrete key sent by cloud.

3. Data users can search uploaded files by using file key or file name.

4. Users can download requested files from cloud by using third party generated private key and aggregate keys.

Cloud:

1. Cloud can view the owner and user details.

2. Cloud can also view user's file request.

3. It request third party to send corresponding file to the user.

TPA:

1. It will send private and aggregate keys to user's mail id.

2. It shows all file details.

VI. CONCLUSION

In this paper, we addressed an important issue of secure data sharing on untrusted storage. We have proposed an efficiently implementable version of the basic key aggregate cryptosystem in with low overhead cipher texts and aggregate keys using asymmetric bilinear pairings. We have proved our construction to be fully collusion resistant and semantically secure against a non-adaptive adversary under appropriate security assumptions. We have then demonstrated how this construction may be modified to achieve CCA-secure construction, which is, to the best of our knowledge, the first CCA secure KAC construction in the cryptographic literature. We have further demonstrated how the basic KAC framework may be efficiently extended and generalized for securely broadcasting the aggregate key among multiple data users in a real-life data-sharing environment.

VII. REFERENCES

1. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for secure cloud storage. Cryptology ePrint Archive, Report 2009/579, 2009.
2. Sherman SM Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou, and Robert H Deng. Dynamic secure cloud storage with provenance. In Cryptography and Security: From Theory to Applications, pages 442–464. Springer, 2012.
3. Erik C Shallman. Up in the air: Clarifying cloud storage protections. Intell. Prop. L. Bull., 19:49, 2014.
4. Cheng-Kang Chu, Sherman SM Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions on, 25(2):468–477, 2014.
5. Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Advances in Cryptology–CRYPTO 2005, pages 258–275. Springer, 2005.
6. D Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Veri?ably Encrypted Signatures from Bilinear Maps," in ProceedingsofAdvancesinCryptology-EUROCRYPT'03, ser.LNCS, vol. 2656. Springer, 2003, pp. 416–432.
7. M J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.
8. J Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
9. F Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.
10. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.