SECURING CLOUD SERVICES USING REVOCABLE IDENTITY BASED ENCRYPTION

[1]Ujjwal Srivastava, [2]Sanjana M Singh, [3]Swetabh Sonal, [4]NV Bharat Varma, [5]Basavaraj Jakkali
[1,2,3,4] Pursuing B.E in Computer Science & Engineering, BMSCE, Bengaluru, India
[5] Associate Professor Dept. of CSE, BMSCE, Bengaluru, India.

Abstract— Cloud computing provides a flexible and convenient way for data sharing bringing various benefits for both the society and individuals. A natural resistance exists for users to directly outsource the data to the cloud since the data often contain important information. Thus, it is necessary to place access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static which means that when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, a notion was proposed which was known as revocable storage identity-based encryption. It can provide the forward/backward security of cipher-text by introducing the functionalities of user revocation and cipher-text update simultaneously. The performance comparisons indicate that the proposed scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

Index Terms—Authorization, forward/backward secrecy, cipher-text, auditor, cryptosystems .

I. INTRODUCTION

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud, Microsoft's Azure and Amazon's S3, can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society. It also suffers from several security threats, which are the primary concerns of cloud users. Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. A natural solution to conquer the aforementioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE).

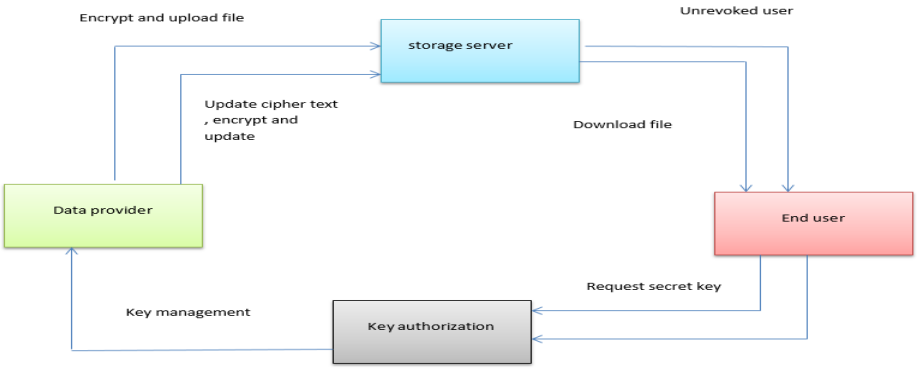
II. LITERATURE SURVEY

Firstly, we learnt that using Cloud Storage, users can remotely store their data and enjoy the on-demand applications and services from a shared pool of configurable computing resources, without the burden of local data storage. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a task, especially for users with constrained computing resources. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to an external auditor to check the integrity of outsourced data and be worry-free. To securely introduce an effective external auditor, the auditing process should bring in no new breaches of user data privacy, and introduce no additional online burden to user. In this paper, we learnt that a secure cloud storage system supporting privacy-preserving public auditing. We also learnt that data distribution is not at all easier with the progress of cloud computing, and an exact examination on the shared data offers a collection of profits both to the public and individuals. Data distribution with a huge number of applicants must get into account numerous issues, counting effectiveness, data integrity and confidentiality of data owner. The expensive certificate authentication in the conventional public key surroundings becomes a restricted access for this solution to be scalable. Data sharing is an important functionality in cloud storage. In this article, we study how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size cipher texts such that efficient formulation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential.

III. PROPOSED SYSTEM

Our proposed system consists of a data provider who generally uploads his data on the cloud server which could be accessed by the end user. A key authorizer exists which generates the key for the user. The data owner can upload the data as well as view the files uploaded by him. The end user can request for a key to access the file. The key authorizer can generate the key for the user and can view the potential attackers. This system can provide an external auditor without the influence of the end user or the cloud server itself. This system provides forward as well as the backward secrecy by making the data owner, key authorizer and the cloud server independent. If the user enters a wrong key, he/she would be under revocation while downloading the file. He would be considered an attacker. A user cannot log in under revocation. We used DES algorithm for encryption-decryption of data and try to make it more secure using various possibilities.

ARCHITECTURE DIAGRAM



IV. CONCLUSION

The notion of identity based encryption is being proposed to protect the data security by including external audit of users. As a proof of concept, we are going to simulate a prototype of a web server on an available public cloud service provider. We are also going to conduct several experiments on the prototype and analyze the security standard of the prototype

V. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no.

[2] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[3] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010. 8. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[8] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[9] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[10] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[11] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

I. 13.A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

II. 14. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.

III. 15. S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

IV. 16. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

AUTHOR PROFILE:

Basavaraj Jakkali is an Associate Professor in the Department of Computer Science & Engineering at BMS College of Engineering. He has completed his Post Graduation from Visvesvaraya Technological University (VTU), Belgaum, in 2002. His areas of interest include Computer Organization, Microprocessors, Theory of Computation, Operating Systems, System Software and Network Security.

Ujjwal Srivastava is Pursuing B.E in Computer Science & Engineering, BMSCE, Bengaluru.

Sanjana M Singh is Pursuing B.E in Computer Science & Engineering, BMSCE, Bengaluru.

Swetabh Sonal is Pursuing B.E in Computer Science & Engineering, BMSCE, Bengaluru.

NV Bharat Varma is Pursuing B.E in Computer Science & Engineering, BMSCE, Bengaluru.