Schemes for Securing Cloud Data when the Cryptographic Material is Exposed: A Review

Anagha Darokar[1], Dr. P. N. Chatur [2]

[1] M. Tech. Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) India
[2]Head, Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) India

---***---

Abstract - *Cloud storage is becoming one of the most attractive choices for individuals and enterprises to store their large scale data. It can avoid committing large capital of user for purchasing and managing hardware and software. Even if the benefits of cloud storage are tremendous, security concern become significant challenge for cloud storage. Key exposure is one of the serious security issues in cloud storage system. Once the key is exposed data confidentiality is lost. This review shows the different schemes that are useful to overcome the key exposure issue.*

Key Words: **Cloud Computing, Cryptography, Key Exposure, Erasure codes.**

1.INTRODUCTION

Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. By combining a set of existing and new techniques from research areas such as Service-Oriented Architectures and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. Along with this new paradigm, various business models are developed, which can be described by terminology of “X as a service” where X could be software, hardware, data storage, and etc. Successful examples are Amazon’s EC2 and S3, Google App Engine, and Microsoft Azure which provide users with scalable resources in the pay-as-you use fashion at relatively low prices. For example, Amazon’s S3 data storage service just charges $0.12 to $0.15 per gigabyte month. Instead of building their own infrastructures, users are able to save their investments significantly by migrating businesses into the cloud. With the increasing development of cloud computing technologies, it is not hard to imagine that in the near future more and more businesses will be moved into the cloud.

As promising as it is, cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users. Data confidential against cloud servers is hence frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security/privacy issue, but also of juristic concerns. For example, in healthcare application scenarios use and disclosure of protected health information should meet the requirements of Health Insurance Portability and Accountability Act, and keeping user data confidential against the storage servers is not just an option, but a requirement. [9]

Outsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. Sensitive data stored in the cloud must be protected from being read in the clear by a cloud provider that is honest but-curious. Day by day as the technology increases the attackers also become powerful such attackers break the data confidentiality by acquiring cryptographic key by unauthorized way. Once the key exposed data confidentiality is lost.

Key exposure is one serious security problem for cloud storage system. This review includes those security schemes which resolve the key exposure issue in some extends. Different types of encryption modes and techniques are available some of the are as follows

A. CPA-Encryption modes

These encryption modes provide the ind security but are only 1 CAKE (Ciphertext Access under Key Exposure) secure. That is, an adversary equipped with the encryption key must only fetch two ciphertext blocks to break data confidentiality.

B. CPA-Encryption and Secret-sharing

This encryption mode combine the CPA secure encryption modes and secret-sharing. If the file f is encrypted and then shared with an n-out-of-n secret-sharing scheme (denoted as “encrypt then-secret-share” in the following), then the construction is clearly (n − 1)CAKE secure and is also ind secure. However, secret-sharing the ciphertext comes at considerable storage costs; for example, each share would be as large as the file f using a perfect secret sharing scheme—which makes it impractical for storing large files. Secret-sharing the encryption key and dispersing its shares across the storage servers alongside the ciphertext is not secure against an ind-adversary. Indeed, if the adversary can access all the storage servers and download all ciphertext blocks, the adversary may as well download all key shares and compute the encryption key.

C. All-or-nothing Encryption

All-or-nothing is not an encryption scheme and does not require the decryptor to have any secret key. That is, an All-or-nothing Transform is not secure against an ind-adversary which can access all the ciphertext blocks. One alternative is to combine the use of All-or-nothing Transform with standard encryption. Rivest suggests to pre-process a message with an All-or-nothing Transform and then encrypt its output with an encryption mode. This paradigm is referred to in the literature as All-or-nothing encryption and provides (n−1) CAKE security. Existing All-or-nothing encryption schemes require at least two rounds of block cipher encryption with two different keys. At least one round is required for the actual All-or-nothing Transform that embeds the first encryption key in the pseudo-ciphertext. An additional round uses another encryption key that is kept secret to guarantee CPA-security. However, two encryption rounds constitute a considerable overhead when encrypting and decrypting large files. These solutions are either not satisfactory in terms of security or incur a large overhead when compared to Bastion and may not be suitable to store large files in a multi-cloud storage system.[10].

2. RELATED WORK

Ran Canetti, Cynthia Dwork, Moni Naor, Rafail Ostrovsky [1] present the deniable encryption scheme. An encryption scheme is deniable if the sender can generate 'fake random choices' that will make the ciphertext 'look like'an encryption of different cleartext, thus keeping the real cleartext private.

Marcos K. Aguilera, Ramaprabhu Janakiraman, Lihao Xu [2] proposed a protocol in which they describe the concept of Erasure Codes Efficiently for Storage of data in a distributed system. . Erasure codes enable users to distribute their data on a number of servers and recover it despite some servers failures. Erasure codes provide space-optimal data redundancy to protect against data loss. Erasure codes are powerful alternatives to replication for storage, as they provide better space efficiency and finer control over the redundancy level. The proposed protocol allow the use of highly-efficient erasure codes, i. e., codes with large n and k and small n-k.

Ronal L. Rivest [3] present new mode of encryption for block cipher called all-or-nothing encryption. This mode has the interesting property that one must decrypt the entire ciphertext into plaintext before one can determine even single message block. All-or-nothing encryption provide the protection against chosen plaintext attack and related message attack.

Anand Desai [4] present a scheme which combine All-or-nothing transform with an ordinary encryption mode. The main motivation is to have secure encryption mode that protecting against the exhaustive key search attack. The all-or-nothing encryption paradigm was suggested as means to achieve strongly non-separable encryption modes. It involves using an all-or-nothing transform as a pre-processing step to an ordinary encryption mode.

Jason K. Resch, James S. Plank [5] describe a new scheme which combine the All-or-nothing Transform with Reed-Solomon coding to achieve high security with low computational and storage cost.

Amos Beimel [6] present a survey on secret sharing scheme. A secret-sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. Secret-sharing schemes are important tools in cryptography and also used as a building box in protocols like general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer. Secret-sharing schemes are a tool used in many cryptographic protocols.

S. Micali and L. Reyzin [7] present leakage-resilient cryptography. Leakage-resilient cryptography aims at designing cryptographic primitives that can resist an adversary which learns partial information about the secret state of a system, e.g., through side-channels. Various models allow to reason about the "leaks" of real implementations of cryptographic primitives. All of these models, however, limit in some way the knowledge of the secret state of a system by the adversary.

Jia Yu and Huaqun Wang [8] present a cloud storage auding scheme with key exposure resilience. In proposed scheme the key exposure in one time period doesn't affect the security of cloud storage auditing in other time periods.

Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou [9] proposed a scheme which uniquely combining techniques of attribute-based encryption,proxy re-encryption, and lazy re-encryption for achieving secure,scalable, and fine-grained data access control in cloud computing. The proposed scheme can enable the data owner to delegate most of computational overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved.

Ghassan O. Karame, Claudio Soriente, Krzysztof Lichota, Srdjan Capkun [10] present a Bastion encryption scheme. This scheme gurantees data confidentiality even if the encryption key is leaked and the adversary has access to almost all ciphertext blocks. Bastion requires only one round of Encryption which make it well-suited to be integrated in existing dispersed storage system. Bastion only incurs a negligible performance deterioration (less than 5%) when compared to symmetric encryption schemes, and considerably improves the performance of existing All-or-nothing encryption schemes.

3. CONCLUSIONS

This paper addressed different cryptographic schemes that resolve the problem of key exposure. After reviewing all the above defined cryptographic schemes it can be concluded that Bastion is more efficient scheme than the All-or-nothing encryption scheme. Bastion require only one round of encryption and it incur a negligible percentage of overhead compared to other encryption scheme. In cloud storage auditing scheme the key exposure in one time period doesn't affect the security of cloud storage auditing in other time periods. In future we will propose a scheme which the combination of all-or-nothing and Bastion scheme that strongly overcome the key exposure problem and also reduces the overhead.

REFERENCES

[1] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable Encryption," in Proceedings of CRYPTO, 1997.

[2] M. K. Aguilera, R. Janakiraman, and L. Xu, "Using Erasure Codes Efficiently for Storage in a Distributed System," in International Conference on Dependable Systems and Networks (DSN), 2005, pp. 336–345.

[3] R. L. Rivest, "All-or-Nothing Encryption and the Package Transform," in International Workshop on Fast Software Encryption (FSE), 1997, pp. 210–218.

[4] A. Desai, "The security of all-or-nothing encryption: Protecting against exhaustive key search," in Advances in Cryptology (CRYPTO), 2000, pp. 359–375.

[5] J. K. Resch and J. S. Plank, "AONT-RS: Blending Security and Performance in Dispersed Storage Systems," in USENIX Conference on File and Storage Technologies (FAST), 2011, pp. 191–202.

[6] A. Beimel, "Secret-sharing schemes: A survey," in International Workshop on Coding and Cryptology (IWCC), 2011, pp. 11–46.

[7] S. Micali and L. Reyzin, "Physically observable cryptography (extended abstract)," in Theory of Cryptography Conference (TCC), 2004, pp. 278–296.

[8] Jia Yu and Huaqan Wang. "Strong Key-Exposure Resilient Auditing for Secure Cloud Storage," in IEEE Transaction on Information Forensics and Security, Vol., No., 2016.

[9] Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc.IEEE INFOCOM'10, pp. 534-542, 2010

[10] Ghassan O. Karame, Claudio Soriente, Krzysztof Lichota, Srdjan Capkun, "Securing Cloud Data under Key Exposure," IEEE Transaction on Cloud Computing 2017.

[11] Anup Mathew, "Survey Paper on Security & Privacy Issues in Cloud Storage Systems," EECE 571B, Term Survey Paper,April 2012.

[12] Y. Chen and R. Sion, "On Securing untrusted clouds with cryptography," In Processings of 9th annual ACM workshop on Privacy in the electronicsociety, pp.109-114, ACM WPES'10,2010

[13] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, Dept. of ECE, ILLinois Inst. Of Technology, "Ensuring data storage security in cloud computing," 17th International Workshop on Quality of Service,2009

[14] K. Yang and X. Jia, "Attributed-Based Access Control for MultiAuthority Systems in Cloud Storage," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 536-545, 2012.

[15] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers," Proc. IEEE Second Int'l Conf. Cloud Computing Technology and Science (CLOUDCOM '10), pp. 97-103, 2010

[16] P.K. Tysowski and M.A. Hasan, "Towards Secure Communication for Highly Scalable Mobile Applications in Cloud Computing Systems," Technical Report 33, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2011.

[17] Q. Liu, G. Wang, and J. Wu, "Clock-Based Proxy Re-Encryption Scheme in Unreliable Clouds," Proc. 41st Int'l Conf. Parallel Processing Workshops (ICPPW), pp. 304-305, Sept. 2012.

[18] P.K. Tysowski and M.A. Hasan, "Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds," Technical Report 13, Centre for Applied Cryptographic Research (CACR), Univ. of Waterloo, 2013.