International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 04 | April -2019 ISSN: 1847-9790 || p-ISSN: 2395-0126

SECURING CLOUD DATA UNDER KEY EXPOSURE

P.ARUNA
Assistant professor,
Department of Computer Science and Engineering
Sri Ramakrishna Engineering College ,Coimbatore
arunapalaniappan@srec.ac.in

SWEETHA G.R
Department of Computer Science and Engineering
sweethakumar20@gmail.com

POOJA BABURAJ
Department of computer science and Engineering
poojababuraj95@gmail.com

A.JANNATHULRISWANA
Department of Computer Science and Engineering
riswanakhan0@gmail.com

ABSTRACT

Recent news reveal a powerful attacker which breaks data confidentiality by acquiring cryptographic keys, by means of coercion or backdoors in cryptographic software. Once the encryption key is exposed, the only viable measure to preserve data confidentiality is to limit the attacker's access to the ciphertext. This may be achieved, for example, by spreading ciphertext blocks across servers in multiple administrative domains—thus assuming that the adversary cannot compromise all of them. Nevertheless, if data is encrypted with existing schemes, an adversary equipped with the encryption key, can still compromise a single server and decrypt the ciphertext blocks stored therein. In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the ciphertext blocks. To this end, we propose Bastion, a novel and efficient scheme that guarantees data confidentiality even if the encryption key is leaked and the adversary has access to almost all ciphertext blocks. We analyze the security of Bastion, and we evaluate its performance by means of a prototype implementation. We also discuss practical insights with respect to the integration of Bastion in commercial dispersed storage systems. Our evaluation results suggest that Bastion is well-suited for integration in existing systems since it incurs less than 5% overhead compared to existing semantically secure encryption modes.

INTRODUCTION

Recently, cloud computing has become an increasingly popular service for its flexibility and scalability, which motivates many organizations, institutions and companies to prefer to outsource data services to cloud platform. At the same time, much attention has been paid to cope with the special security and privacy problems in outsourced cloud. On one hand, to protect the data confidentiality, the data owner (DO) encrypt the sensitive information of his outsourced data, such as income level, health records, personal photos before the dataset is uploaded to the cloud . On the other hand, data owner may plan to rely on cloud platform for querying of the datasets stored in cloud, not just for storage and management. Therefore, a large amount of secure schemes have been proposed.

As a fundamental query operation in spatial and multimedia databases, k-nearest neighbors (k-NN) query aims at identifying k nearest points for a given query point in a dataset. In the past few years, researchers have proposed various methods to address the security and privacy problems of k-NN

query on encrypted cloud data. The general approach is to encrypt data by the data owner (DO) before outsourcing, the authorized query users (QUs) perform a complex series of encryption and decryption operations during query execution. For example, the work in proposes an asymmetric scalar-product-preserving encryption (ASPE) to preserve scalar product between the query vector and any vector for distance comparison, which is sufficient to find k-NN. Instead of finding exact nearest neighbour, Yao et al allow a cloud party to approximate it based on secure Voronoi diagram algorithm. Elmehdwi et al. propose a novel protocol over encrypted data based on a TwinCloud model and Paillier cryptosystem , which can calculate k-NN between data records and query records in a secure manner. However, all the above schemes have assumed that the query users are fully-trusted and have the access to the key for encrypting and decrypting outsourced data. It will bring about several problems in the real world. Firstly, cloud platform can totally break the outsourced database once the key is obtained from any compromised query user. It is obvious that each query user could be one of the lucrative targets for attackers. Secondly, data owner may have no enough trust on each query user in many applications which will limit the scope of these schemes. For instance, hospitals or institutes of medicine might contribute medical data for a disease classification study or a service available to doctors. Thus, doctors can search the k-NN cases with some similar physiological data to help treat patients. If using the above schemes, the doctors will encrypt the indices with the same key as the one that the data owner encrypts and decrypts the outsourced database. Obviously, it is not realistic, since the data owner do not want to release the medical data in the clear to each other or a cloud platform. Thirdly, once query users receive the key, their query processing will not be controlled by data owner any more, and it is difficult to revoke the access even they are deemed to be untrustworthy. In general, these schemes with key-sharing are still far from being practical in most instances.

LITERATURE REVIEW

We presented the securing cloud data under key exposure using data encryption which helps to establish The availability of fast and reliable Digital Identities is an essential ingredient for the successful implementation of the public-key infrastructure of the Internet. All digital identity schemes must include a method for revoking someones digital identity in the case that this identity is stolen before its expiration date. In this we extend this scheme by reducing the overall CA to Directory communication, while still maintaining the same tiny user to vendor communication. A partition may either expire or be renewed at the end of a time slot. This is done efficiently using hash chains.

LIMITATION OF THE PROJECT

A powerful attacker which breaks data confidentiality by acquiring cryptographic keys, by means of coercion or backdoors in cryptographic software

ADVANTAGES

Here we introduced a novel security definition that captures data confidentiality against the new adversary .

EXISTING SYSTEM

In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the ciphertext blocks. The adversary can acquire the key either by exploiting flaws or backdoors in the key-generation software, or by compromising the devices that store the keys of secret-sharing

PROPOSED SYSTEM

 We propose Bastion, an efficient scheme which ensures data confidentiality against an adversary that knows the encryption key and has access to a large fraction of the ciphertext blocks.
 We analyze the security of Bastion, and we show that it prevents leakage of any plaintext block as long as the adversary has access to the encryption key and to all but two ciphertext blocks.
 We evaluate the performance of Bastion analytically and empirically in comparison to a number of existing encryption techniques.
 Our results show that Bastion considerably improves (by more than 50%) the performance of existing AON encryption schemes, and only incurs a negligible overhead when compared to existing semantically secure encryption modes (e.g., the CTR encryption mode).
 We discuss practical insights with respect to the deployment of Bastion within existing storage systems, such as the HYDRAstor grid storage system

FUTURE ENHANCEMENT

 Though the above solution supports the differential privilege duplicate, it is inherently subject to brute force attacks launched by the public cloud server, which can recover files falling
 The main idea of our technique is that the novel encryption key generation algorithm.
For simplicity, we will use the hash functions to define the tag generation functions
and convergent keys in this section.

CONCLUSION

In this paper, we addressed the problem of securing data outsourced to the cloud
against an adversary which has access to the encryption key. For that purpose, we introduced
a novel security definition that captures data confidentiality against the new adversary. We
then proposed Bastion, a scheme which ensures the confidentiality of encrypted data even
when the adversary has the encryption key, and all but two ciphertext blocks. Bastion is most
suitable for settings where the ciphertext blocks are stored in multi-cloud storage systems. In
these settings, the adversary would need to acquire the encryption key, and to compromise all
servers, in order to recover any single block of plaintext. We analyzed the security of Bastion
and evaluated its performance in realistic settings. Bastion considerably improves (by more than 50%) the performance of existing primitives which offer comparable security under key exposure, and only incurs a negligible overhead (less than 5%) when compared to existing semantically secure encryption modes (e.g., the CTR encryption mode). Finally, we showed how Bastion can be practically integrated within existing dispersed storage systems.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology (CRYPTO'98). New York, NY, USA: Springer, 1998, pp. 137–152.

[2] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, S. Dietrich and R. Dhamija, Eds. Berlin, Germany: Springer, 2007, vol. 4886, pp. 247–259.

[3] F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography (PKC'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, vol. 2947, pp. 375–388.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput. Commun. Security (CCS'08), 2008, pp. 417–426.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557–557.

[7] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," Cryptology ePrint Archive, Rep. 2011/ 518, 2011 [online]. Available: http://eprint.iacr.org/2011/518.

[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Annu. ACM Symp. Theory Comput. (STOC'97), 1997, pp. 506–516.

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography (TCC'05), 2005, pp. 264–282.

[10] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, A. Smith, Ed. Berlin, Germany: Springer, 2012, vol. 7412, pp. 37–61.

[11] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.