ISSN 2278-3091

Volume 7, No.3, May- June 2018

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01732018.pdf

https://doi.org/10.30534/ijatcse/2018/01732018

A Survey of : Securing Cloud Data under Key Exposure

Goodubaigari Amrulla [1], Murlidher Mourya [2], Rajasekhar Reddy Sanikommu[3] and Abdul Ahad Afroz [4]

[1] Assistant Professor Deportment of CSE,
DRK College of Engineering and Technology, JNTU Hyderabad, Telgana, India. amrushafi12@gmail.com
[2] Assistant Professor Deportment of CSE,
Vardhaman College of Engineering, JNTU Hyderabad, Telgana, India. murli_cool9@yahoo.com
[3] Assistant Professor Deportment of CSE,
DRK College of Engineering and Technology, JNTU Hyderabad, Telgana, India. reddysonikommu@gmail.com
[4] Assistant Professor Deportment of CSE,
Sree Dattha Institute of Engineering and Science, JNTU Hyderabad, Telgana, India. abdulahadafroz!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 cipher text. This may be achieved, for example, by spreading cipher text 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 cipher text 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 cipher text 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 cipher text 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.

Key words: Key exposure, Data Confidentiality, dispersed storage

1. INTRODUCTION

Most of the organizations now-a-days use cloud technologies, With the increase in the use of cloud technologies there can be a security and privacy issue of accessing personal and confidential information over the Internet. The recent and continuing data breaches highlight the need for more secure cloud storage systems. While it is generally agreed that encryption is necessary, cloud providers often perform the encryption and maintain the private keys instead of the data owners. That is, the cloud can read any data it desired, providing no privacy to its users. The storage of private keys and encrypted data by the cloud provider is also problematic in case of data breach. Hence, researchers have actively been exploring solutions for secure storage on private and public clouds where private keys remain in the hands of data owners. This scheme is very reliable and easy to implement also scalable, that means we can easily add and remove documents in the corpus. Makin some small changes to the scheme we can lower the storage cost at a very low cost and we can defend the cloud providers with statistical knowledge.

1.1 Existing system

If the encryption key is exposed, the only viable means to guarantee confidentiality is to limit the adversary's access to the cipher text, e.g., by spreading it across multiple administrative domains, in the hope that the adversary cannot compromise all of them. However, even if the data is encrypted and dispersed across different administrative domains, an adversary equipped with the appropriate keying material can compromise a server in one domain and decrypt cipher text blocks stored therein. Ramp schemes constitute a trade-off between the security guarantees of secret sharing and the efficiency of information dispersal algorithms. A ramp scheme achieves higher "code rates" than secret sharing and features two thresholds t1, t2. At least t2 shares are required to reconstruct the secret and less than t1 shares provide no information about the secret; a number of shares between t1 and t2 leak "some" information. Resch et al. combine AONT and information dispersal to provide both fault-tolerance and data secrecy, in the context of distributed storage systems. In existing system, however, an adversary which knows the encryption key can decrypt data stored on single servers.

In this paper, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the cipher text 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 (e.g., at the user-side or in the cloud). As far as we are aware, this adversary invalidates the security of mos cryptographic solutions, including those that protect encryption keys by means of secret-sharing (since these keys can be leaked as soon as they are generated).

1.2 Disadvantages of Existing System:

- Existing AON encryption schemes, however, require *at least* two rounds of block cipher encryptions on the data: one preprocessing round to create the AONT, followed by another round for the actual encryption. Notice that these rounds are sequential, and cannot be parallelized.
- This results in considerable—often unacceptable—overhead to encrypt and decrypt large files.
- On the other hand, Bastion requires only one round of encryption—which makes it well-suited to be integrated in existing dispersed storage systems.
- powerful attacker which breaks data confidentiality by acquiring cryptographic keys, by means of coercion or backdoors in cryptographic software

1.3 Proposed 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 cipher text 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 (e.g., at the user-side or in the cloud). To counter such an adversary, we propose Bastion, a novel and efficient scheme which ensures that plaintext data cannot be recovered as long as the adversary has access to at most all but *two* cipher text blocks, even when the encryption key is exposed.

Bastion achieves this by combining the use of standard encryption functions with an efficient linear transform. In this sense, Bastion shares similarities with the notion of all-or-nothing transform. An AONT is not an encryption by itself, but can be used as a pre-processing step before encrypting the data with a block cipher. This encryption paradigm called AON encryption was mainly intended to slow down brute-force attacks on the encryption key. However, AON encryption can also preserve data confidentiality in case the encryption key is exposed, as long as the adversary has access to at most all but one cipher text blocks.

1.4 Advantages of Proposed System:

- We evaluate the performance of Bastion in comparison with a number of existing encryption schemes. Our results show that Bastion only incurs a negligible performance deterioration (less than 5%) when compared to symmetric encryption schemes, and considerably improves the performance of existing AON encryption schemes.
- 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 cipher text 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 cipher text 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 HYDRA store grid storage system.
- we introduced a novel security definition that captures data confidentiality against the new adversary

2. MODULES:

The system consists of modules and threat modules.

- Public Key and Secret Key
- File Storage
- Generate time period key
- Indexing of files
- View files and download files
- Auditor Public key

Public Key & Secret Key:

In this Module public key is generated for authentication for the user to provide the user specification logging.

The secret key is the confidential generated for each candidate during registration

File Storage

The File Storage module the file stored for the further usage of the consumer and the file is provided the option to view and Download based on the time period keys.

Generate time period key;

The time period key is generated such to use the file or to perform operation on it based on time

Indexing of the files

The indexing of the files is specified such that to view the download or to generate key or to download or perform the operation on the file**.**

View and Download files.

The files can be viewed or download based on the time period key authentication of the user.

Auditor Public Key.

The auditor public key is generated to perform all the operation with a single key on all the modules

3. METHODOLOGY

Data security can be defined as the confidentiality and integrity of data processed by the organization. In scenarios where the data owner has no control over the detailed architecture and management controls, such as outsourcing, assuming an increased risk of data security. We mitigate the risks by knowing the element:

- organization structure that properly values, protects and uses data, both in planning as well as the provision of services.
- strong and clear accountability procedures, recognizing that the data owner (organizational unit) is the best place to understand and address the risks to their information, including personal data
- measures taken on the level of security of archived data, creating confidentiality, data security and sharing .
- establish a clear policy to be simple to understand and use.
- provide a consistent and universal framework for safety training .

4. AIM

The aim of this paper is to investigate how to reduce the damage of the client's key exposure in cloud storage auditing.

5. SCOPE

The scope of this paper tends to formalize the definition and the security model of auditing protocol with key-exposure resilience and propose.

6. SYSTEM ARCHITECTURE:

Our attacker model. We assume an adversary which can acquire all the cryptographic secret material, and can compromise a large fraction (up to all but one) of the storage servers[1].

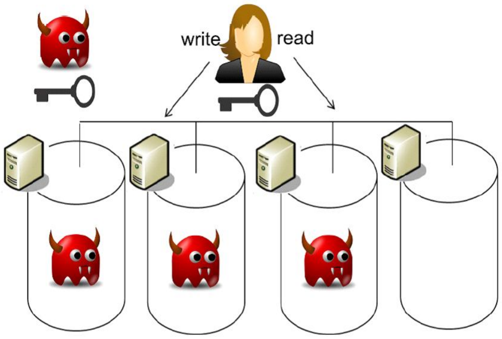

Figure: 1 System Architecture

7. FLOW DIAGRAM

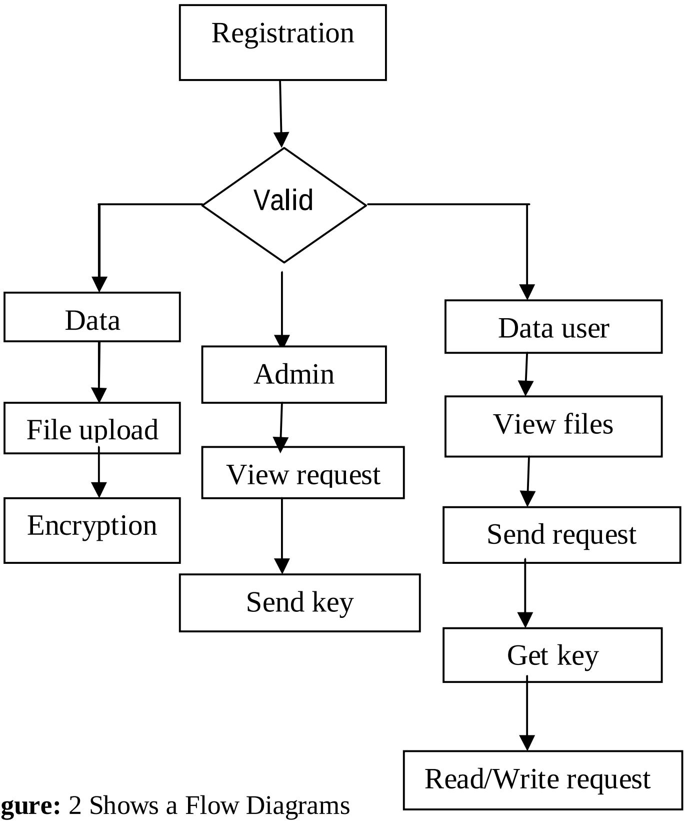

Figure: 2 Shows a Flow Diagrams

8.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 cipher-text blocks. Bastion is most suitable for settings where the cipher text 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.

REFERENCES

[1]Ghassan O. Karame, *Member, IEEE*, Claudio Soriente, *Member, IEEE*, Krzysztof Lichota, Srdjan Capkun, *Senior Member, IEEE*, “Securing Cloud Data under Key Exposure”, IEEE Transactions on Cloud Computing, 2017.

[2] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Re-iter, and J. J. Wylie, “Fault-Scalable Byzantine Fault-Tolerant Services,” in ACM Symposium on Operating Systems Principles (SOSP), 2005, pp. 59–74. https://doi.org/10.1145/1095810.1095817

[3]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. https://doi.org/10.1109/DSN.2005.96

[4] L JagajeevanRao "Key Exposure in Cloud Data Services "International Journal of Big Data Security Intelligence Vol. 4, No. 1 (2017)

About The Authors

Mr. GOODUBAIGARI AMRULLA is assistant professor at DRK College Engineering and Technology. He has 3.5 years of experience in teaching field. He has received B.Tech (Information Technology) degree from VVIT Chevella, JNTUH University in the year 2010 and M.Tech (Software Engineering) degree from NIET Deshmukhi, JNTUH University in the year 2013.

Mr. MURLIDHER MOURYA is assistant professor at Vardhaman College of Engineering. He has 7 years of experience in teaching field. He has received B.Tech (CSE) degree from GRIET Bachupally, JNTUH University in the year 2007 and M.Tech (CSE) degree from TKRCET Medbowli, Meerpet, JNTUH University in the year 2010.

Mr. RAJASEKHAR REDDY SANIKOMMU is assistant professor at DRK College Engineering and Technology. He has 2 years of experience in teaching field. He has received B.Tech (CSE) degree from JB Institute of Engineering and Technology ,Moinabad, JNTUH University in the year 2012 and M.Tech (CS) degree from, JNTUH SIT University in the year 2015.

Mr. ABDUL AHAD AFROZ is assistant professor at Sree Dattha Institute of Engineering and Science. He has 4 years of experience in teaching field. He has received B.Tech (Information Technology) degree from Green Fort Engineering College Bandla Guda, Chandrayanagutta, JNTUH University in the year 2008 and M.Tech (Software Engineering) degree from NIET Deshmukhi, JNTUH University in the year 2013.