IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906198 |

Securing Cloud Data under Key Exposure

Karrolla Shashi Preetham, Payam Kavya, Pedasanaganti Shirisha, Dr. K. Ramakrishna

UG Students, Dept. of C.S.E., J.B.I.E.T Hyderabad, Telangana, India

Assistant Professor, Dept. of C.S.E., J.B.I.E.T Hyderabad, Telangana, India

ABSTRACT: Recent news reveal a powerful attacker which breaks data confidential ity 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 attackers 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.

KEYWORDS: Key Exposure, Data Confidentiality, Dispersed Storage.

I. INTRODUCTION

THE world recently witnessed a massive surveillance program aimed at breaking users privacy. Perpetrators were not hindered by the various security measures deployed within the targeted services. For instance, although these services relied on encryption mechanisms to guarantee data confidentiality, the necessary keying material was acquired by means of backdoors, bribe, or coercion. If the encryption key is exposed, the only viable means to guarantee confidentiality is to limit the adversary access to the ciphertext, 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 ciphertext blocks stored therein.

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 (e.g., at the user-side or in the cloud). As far as we are aware, this adversary invalidates the security of most 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). 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 ciphertext 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 ciphertext blocks. Existing AON encryp tion 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. We evaluate the performance of Bastion in comparison with a number of existing encryption schemes.

II. 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906198 |

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).

Disadvantages:

- Existing AON encryption schemes, however, require at least two rounds of block cipher encryption on the data: one preprocessing round to create t he 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

III. PROPOSED METHODOLOGY

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.

Advantages:

We evaluate the performance of Bastion in comparison with a number of existing encryption schemes. Ourresults show that Bastion only incurs a negligible performance deterioration when compared to symmetric encryption schemes, and considerably improves the performance of existing AON encryption schemes.
We propose Bastion, an efficient scheme which ensures the data confidentiality against an adversary that knows the encryption key and has access to a large fraction of the cipher text blocks.
We introduced a novel security definition that capture data confidentiality against the new adversary.

IV. ARCHITECTURAL DIAGRAM

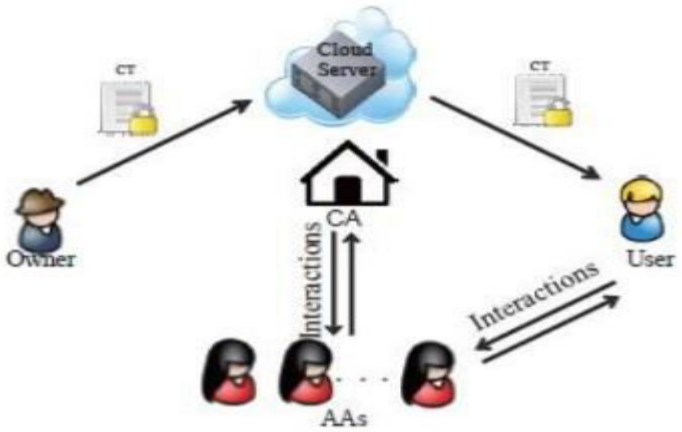


Fig 4 ARCHITECTURAL DIAGRAM

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906198 |

V. ALGORITHMS USED

Clustering Algorithm

Clustering or cluster analysis is the way of clubbing a set of objects in such a way that the set of objects in similar set are more similar than the set of objects in other set. This is known as Clustering Algorithm.

Cipher text- Policy Attribute-Based Encryption

This algorithm encrypts the data uploaded by the owner and sets a passcode to it. Only the user with the passcodes can gain access to the file

VI. MODULE DESCRIPTION

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

Test cases

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906198 |

VII. RESULTS

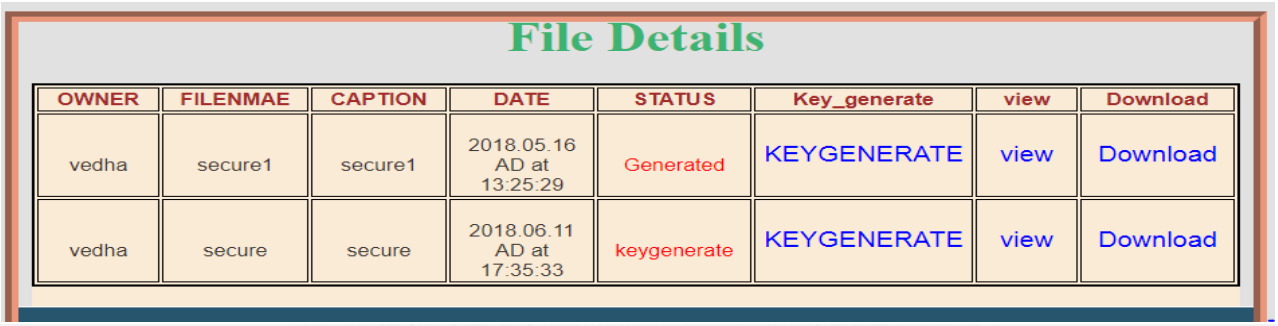
S.NO	TEST CASE	Scenario	EXPECTED OUTPUT	ACTUA L OUTPUT	RESULT
1	Depressed Tweet	Feeling Down	True	True	True Positive
2	Depressed Tweet	Extreme Sadness,lackof energy, hopelessness	True	True	True Positive
3	Depressed Tweet	My depression will not let me work	True	True	True Positive
4	Non Depressed Tweet	Lovely how me and my lovely partner is talking about what we want	False	False	False Negative
5	Non Depressed Tweet	It is the little things that make me smile	False	False	False Negative
6	Non Depressed Tweet	Super happy that tomorrow is Friday	False	False	False Negative

HOME PAGE

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906198 |



FILE DOWNLOAD

VIII. CONCLUSION

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 evaluate edits 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 system.

REFERENCES

1. M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, Fault-Scalable Byzantine Fault-Tolerant Services, in ACM Symposium on Operating Systems Principles (SOSP), 2005, pp. 5974.
2. M. K. Aguilera, R. Janakiraman, and L. Xu, Using Erasure Codes Efficiently for Storage in aDistributed System, in International Conference on Dependable Systems and Networks (DSN), 2005, pp. 336345.
3. W. Aiello, M. Bellare, G. D. Crescenzo, and R. Venkatesan, Security amplifica tion by composition: The case of doubly iterated, ideal ciphers, in Advances in Cryptology (CRYPTO), 1998, pp. 390407.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906198 |

4. C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic, Robust Data Sharing with Key-value Stores, in ACM SIGACT- SIGOPS Symposium on Principles of Distributed Computing (PODC), 2011, pp. 221222.
5. Beimel, Secret-sharing schemes: A survey, in International Workshop on Coding and Cryptology (IWCC), 2011, pp. 1146.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details