2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

COLLABORATING DATA OWNER-SIDE AND CLOUD-SIDE ACCESS CONTROL FOR CRYPTCLOUD STORAGE

[1]KOLUGURI SHIRISHA [2]MR.K.RAGHUPATI

[1] M. tech Student, Department of Computer Science and Engineering, Chaitanya Institute of Technology and science Kishanpura,Hanamkonda,Warangal -506001, (.TS).india

[2]Assistant Professor, Department of Computer Science and Engineering ,Chaitanya Institute of Technology and Science kishanpura,Hanamkonda,Warangal -506001, (TS).india

[1]Sharon.siri38@gmail.com, [2]raghu.kanala@gmail.com

Abstract:

People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, Ciphertext-Policy Attribute-based Encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch Economic Denial of Sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of CP-ABE. We present two protocols for different settings, followed by performance and security analysis.

I.INTRODUCTION

Cloud storage has many benefits, such as always-online, pay-as-you-go, and cheap [1]. During these years, more data are outsourced to public cloud for persistent storage, including personal and business documents. It brings a security concern to data owners [2]–[4]: the public cloud is not trusted, and the outsourced data should not be leaked to the cloud provider without the permission from data owners. Many storage systems use server-dominated access control, like password-based [5] and certificate-based authentication [6]. They overly trust the cloud provider to protect their sensitive data. The cloud providers and their employees can read any document regardless of data owners' access policy. Besides, the cloud provider can exaggerate the resource consumption of the file storage and charge the payers more without

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

providing verifiable records [2], [7], [8], since we lack a system for verifiable computation of the resource usage.

Relying on the existing server-dominated access control is not secure. Data owners who store files on cloud servers still want to control the access on their own hands and keep the data confidential against the cloud provider and malicious users. Encryption is not sufficient. To add the confidentiality guarantee, data owners can encrypt the files and set an access policy so that only qualified users can decrypt the document. With Ciphertext-Policy Attribute-based Encryption (CP-ABE) [9], [10], we can have both fine-grained access control and strong confidentiality [11]–[16]. However, this access control is only available for data owners, which turns out to be insufficient. If the cloud provider cannot authenticate users before downloading, like in many existing CP-ABE cloud storage systems [14], [15], the cloud has to allow everyone to download to ensure availability. This makes the storage system vulnerable to the resource-exhaustion attacks. If we resolve this problem by having data owners authenticate the downloaders before allowing them to download, we lose the flexibility of access control from CP-ABE. Here lists the two problems should be addressed in our work.

Problem I: resource-exhaustion attack. If the cloud cannot do cloud-side access control, it has to allow anyone, including malicious attackers, to freely download, although only some users can decrypt. The server is vulnerable to resource-exhaustion attacks. When malicious users launch the DoS/DDoS attacks to the cloud storage, the resource consumption will increase. Payers (in pay-as-you-go model) have to pay for the increased consumption contributed by those attacks, which is a considerable and unreasonable financial burden. The attack has been introduced as Economic Denial of Sustainability (EDoS) [17]–[20], which means payers are financially attacked eventually. In addition, even files are encrypted, unauthorized downloads can reduce security by bringing convenience to to offline analysis and leaking information like file length or update frequency.

II.EXISTING SYSTEM:

- In the existing system, R. K. Koet.al., the authors discussed key issues and challenges about how to achieve accountability in cloud computing. In the literature, D. O´ .Coilea´et.al., the authors surveyed existing accounting and accountability in content distribution architectures.
- V. Sekaret. al. and C. Chen et. al., the authors respectively proposed a systematic approach for verifiable resource accounting in cloud computing.

DISADVANTAGES OF EXISTING SYSTEM:

- The accounting approach involves changes to the system model, and requires the anonymous verification of users, which is not supported in previous systems.
- The access control is only available for data owners, which turns out to be insufficient.

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

- This makes the storage system vulnerable to the resource-exhaustion attacks.
- It loses the flexibility of access control from CP-ABE.

III .PROPOSED SYSTEM:

- In this paper, we combine the cloud-side access control and the existing data owner-side CP-ABE based access control, to resolve the aforementioned security problems in privacy preserving cloud storage. Our method can prevent the EDoS attacks by providing the cloud server with the ability to check whether the user is authorized in CP-ABE based scheme, without leaking other information.
- For our cloud-side access control, we use CP-ABE encryption/ decryption game as challenge-response. While upload an encrypted file, the data owner firstly generates some random challenge plaintexts and the corresponding ciphertexts. The ciphertexts are related to the same access policy with the specific file. For an incoming data user, the cloud server asks him/her to decrypt randomly selected challenge ciphertext.
- If the user shows a correct result, which means he/she is authorized in CP-ABE, the cloud-side access control allows the file download. To make our solution secure and efficient in real world applications, we provide two protocols of cloud-side and data owner-side combined access control.

Advantages of Proposed System:

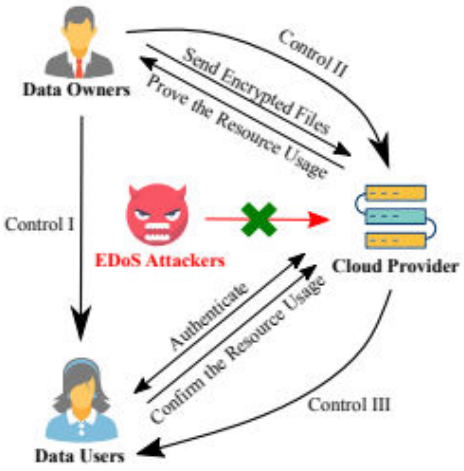
- We propose a general solution to secure encrypted cloud storage to prevent the EDoS attacks, as well as have fine-grained access control and resource consumption accountability. To the best of our knowledge, this is the first work to claim that insufficient cloud-side access control in encrypted cloud storage will lead to EDoS attacks and provides a practical solution. The solution can be compatible with many CP-ABE schemes.
- For different data owner online patterns and performance concern, we provide two protocols for authentication and resource consumption accounting. We also introduce the bloom filter and the probabilistic check to improve the efficiency but still guarantee the security.
- Compared with many state-of-arts constructions of encrypted cloud storage that assume the existence of a semi-honest cloud provider, we use a more practical threat model where we assume the cloud provider to be a covert adversary, which provides higher security guarantee.

Compared with relevant schemes, our approach works on the protocol level to provide the resource verifiability that relies on authorized users who satisfy the CP-ABE

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

policy, and achieves the covert security which is more practical and secure.

Architecture:



Control I: Data owners only allow authorized data users to decrypt the files.
Control II: Data owners verify the resource consumption records of the cloud provider.
Control III: The cloud provider verifies the data users before the download.

Algorithm:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

Symmetric key symmetric block cipher
128-bit data, 128/192/256-bit keys
Stronger and faster than Triple-DES
Provide full specification and design details
Software implementable in C and Java

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

IV.IMPLEMENATATION:

Data owners:

In this module, Data owners are the owner and publisher of files and pay for the resource consumption on file sharing. As the payers for cloud services, the data owners want the transparency of resource consumption to ensure fair billing. The data owners require the cloud provider to justify the resource usage. In our system, the data owner is not always online.

Data users:

In this module users want to obtain some files from the cloud provider stored on the cloud storage. They need to be authenticated by the cloud provider before the download (to thwart EDoS attacks). The

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

authorized users then confirm (and sign for) the resource consumption for this download to the cloud provider.

Cloud provider:

Cloud provider hosts the encrypted storage and is always online. It records the resource consumption and charges data owners based on that record. The cloud is not public-accessible in our system as it has an authentication based access control. Only data users satisfying the access policy can download the corresponding files. The cloud provider also collects the proof of the resource consumption to justify the billing

V.CONCLUSION:

In this paper, we propose a combined the cloud-side and dataowner-side access control in encrypted cloud storage, whichis resistant to DDoS/EDoS attacks and provides resource consumptionaccounting. Our system supports arbitrary CP-ABEconstructions. The construction is secure against maliciousdata users and a covert cloud provider. We relax the securityrequirement of the cloud provider to covert adversaries,which is a more practical and relaxed notion than that withsemi-honest adversaries. To make use of the covert security,we use bloom filter and probabilistic check in the resourceconsumption accounting to reduce the overhead. Performanceanalysis shows that the overhead of our construction is smallover existing systems.

VI.REFERENCES:

[1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-artand research challenges," Journal of Internet Services and Applications,vol. 1, no. 1, pp. 7–18, 2010.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the publiccloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[3] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query overencrypted data in cloud with limited key-disclosure and offline dataowner," Computers & Security, vol. 69, pp. 84–96, 2017.

[4] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT:Privacy-preserving outsourcing computation of feature extractions overencrypted image data," IEEE Transactions on Image Processing, vol. 25,no. 7, pp. 3411–3425, 2016.

[5] H.-M. Sun, Y.-H.Chen, and Y.-H. Lin, "oPass: A user authenticationprotocol resistant to password stealing and password reuse attacks,"IEEE Transactions on Information Forensics and Security, vol. 7, no. 2,pp. 651–663, 2012.

[6] L. Harn and J. Ren, "Generalized digital certificate for user authenticationand key establishment for secure communications," IEEE Transactionson Wireless Communications, vol. 10, no. 7, pp. 2372–2379,2011.

[7] V. Sekar and P. Maniatis, "Verifiable resource accounting for cloudcomputing services," in Proceedings of the 3rd ACM

workshop on Cloudcomputing security workshop. ACM, 2011, pp. 21–26.

[8] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, "Towardsverifiable resource accounting for outsourced computation," in ACMSIGPLAN Notices, vol. 48, no. 7. ACM, 2013, pp. 167–178.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebasedencryption," in 2007 IEEE Symposium on Security and Privacy(SP'07). IEEE, 2007, pp. 321–334.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive,efficient, and provably secure realization," in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 53–70.

[11] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharingof personal health records in cloud computing using attribute-basedencryption," IEEE Transactions on Parallel and Distributed Systems,vol. 24, no. 1, pp. 131–143, 2013.

[12] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution withhidden policy," in Proceedings of 4th Workshop on Secure NetworkProtocols (NPSec2008). IEEE, 2008, pp. 39–44.