IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

SeGShare: Secure Group File Sharing in the Cloud using Enclaves

Kunal Mahajan, Prasad Kharad,Nikita Darwade, Shibu Kumar, Prof. Rupali Salunke
NBN Sinhgad School of Engineering, Pune, India

Abstract:*File sharing applications using cloud storage are increasingly popular for personal and business use. Due to data protection concerns, end-to-end encryption is often a desired feature of these applications. Many attempts at designing cryptographic solutions fail to be adopted due to missing relevant features. We present SeGShare, a new architecture for end-to-end encrypted, group-based file sharing using trusted execution environments (TEE), e.g., Intel SGX. SeGShare is the first solution to protect the confidentiality and integrity of all data and management files; enforce immediate permission and membership revocations; support deduplication; and mitigate rollback attacks. Next to authentication, authorization and file system management, our implementation features an optimized TLS layer that enables high throughput and low latency. The encryption overhead of our implementation is extremely small in computation and storage resources. Our enclave code comprises less than 8500 lines of code enabling efficient mitigation of common pitfalls in deploying code.*

I. INTRODUCTION

In many applications, users want to share files with a group of other users. For instance, employees of a company want to share files with colleagues. One option is to distribute the files to each group member individually. A better option is a local or remote central repository to store the files and manage access control. A convenient remote repository is a cloud-based file sharing service as it can reduce cost, increase availability and enable seamless multi-device access to files. Many commercial vendorsprovide such a service, e.g., Google Drive [1], Dropbox [2], or WeTransfer [3]. However, data at cloud services could be accessed by unauthorized parties or exposed by internal attackers Frequently, company policies prohibit to upload files to an untrusted cloud provider.

II. LITERATURE SURVEY

The paper titled "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage" introduces the concept of Cloud-Edge- Collaborative Storage (CECS) as a framework for processing Internet of Things (IoT) data. The CECS framework enables real-time data processing on edge servers while storing the data on a cloud server, thereby facilitating rapid response to IoT device requests, offering large-scale cloud storage for IoT data, and convenient data sharing with users. However, the vulnerability of edge and cloud servers poses a risk of data leakage in CECS. Existing secure CECS schemes depend on the trustworthiness of all edge servers, making the entire system susceptible to data breaches if any edge server is compromised. Furthermore, requesting data from the cloud incurs significant costs that scale linearly with the number of edge servers.

To address these challenges, the authors propose a new secure data search and sharing scheme for CECS. The scheme improves existing secure CECS schemes in two key ways. First, it allows users to generate their own public-private key pairs and manage their private keys, eliminating the need for edge servers to handle user keys. Second, it employs searchable public-key encryption for more secure, efficient, and flexible data searching. The proposed scheme ensures data confidentiality, secure data sharing and searching, and avoids a single point of failure. Performance evaluations demonstrate that the scheme significantly reduces users' computing costs by offloading most cryptographic operations to edge servers, including a reduced computing and communication overhead for generating search trapdoors compared to existing secure CECS schemes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

III. PROPOSED METHODOLOGY AND ALGORITHM

3.1Proposed Methodology

The proposed methodology in the paper aims to address the challenges of secure data sharing and search in the Cloud-Edge-Collaborative Storage (CECS) framework. The authors introduce a new scheme that improves upon existing secure CECS schemes in two main aspects.

Firstly, the scheme enables users to generate their own public-private key pairs and manage their private keys independently. This approach eliminates the reliance on edge servers for key management, enhancing the overall security of the system. By allowing users to have control
over their private keys, the scheme reduces the risk of unauthorized access and potential data leakage if an edge server is compromised.

Secondly, the proposed scheme utilizes searchable public-key encryption to achieve more secure, efficient, and flexible data searching. This technique enables users to search for specific data stored in the cloud without compromising its confidentiality. By leveraging searchable public-key encryption, the scheme enhances the privacy and security of data retrieval operations.

The authors emphasize that the proposed methodology ensures the confidentiality of cloud data and provides secure data sharing and searching capabilities while avoiding a single point of breakthrough. By decentralizing key management and employing searchable public- key encryption, the scheme mitigates the vulnerabilities associated with traditional secure CECS schemes.

Algorithm:

The paper does not explicitly mention a specific algorithm for the proposed scheme. However, based on the description of the methodology, it can be inferred that the scheme likely involves a combination of cryptographic techniques, such as public-key encryption, searchable encryption, and key management protocols. The algorithmic details and implementation specifics are likely provided in the main body of the paper beyond the abstract.

It is important to note that without access to the full paper, it is not possible to provide a detailed algorithmic description. The proposed methodology and algorithm would be further elaborated and explained in the paper's subsequent sections, including the methodology, security analysis, and performance evaluation

IV. EXPERIMENTAL RESULTS

In our experimental setup, as shown in table 1, the total numbers of 720 of trained images for 35 categories such as A-Z and 0-9 and 72 new images were tested. These images go through CNN framework by following feature extraction using our image processing module. Then our trained model of classification of signs get classifies the image into specifies category. We get the accuracy 98.23% at 100 epochs as shown in figure4 and figure5.

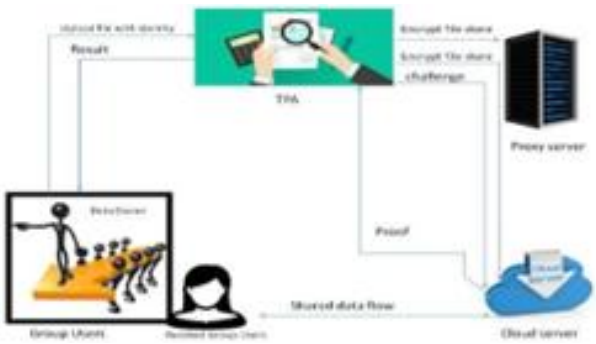

Figure: Accuracy Graph Fig4. Loss Graph

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 16, May 2023

V. CONCLUSION

We introduce SeGShare an end-to-end encrypted, group file sharing solution supporting large and dynamic groups using trusted execution environments (TEE), e.g., Intel SGX. SeGShare protects the confidentiality and integrity of content files, the file system structure, permissions, existing groups, group memberships. Among other features, it enforces immediate permission and membership revocations; supports deduplication; mitigates rollback attacks; and provides separation of authentication and authorization.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2012.
[2] L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k- NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017.
[3] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.
[4] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2012.
[5] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.