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.*

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.