ABSTRACT: Access Control in Searchable Encryption with the use of Attribute-Based Encryption and SGX

Antonis Michalas
antonis.michalas@tuni.fi
Tampere University
Tampere, Finland

Alexandros Bakas
alexandros.bakas@tuni.fi
Tampere University
Tampere, Finland

Hai-Van Dang
H.Dang@westminster.ac.uk
University of Westminster
London, UK

Alexandr Zalitko
alexandr.zalitko@tuni.fi
Tampere University
Tampere, Finland

ABSTRACT

We designed a hybrid encryption scheme that deals with the problem of storing data on untrusted clouds. Our work is an extension of [2, 7] and combines Symmetric Searchable Encryption (SSE) [3] and Attribute-Based Encryption (ABE) [4], along with the functionality offered by Intel SGX [6]. Our scheme compromises four SGX enclaves: Master Authority (MS) that generates public parameters and issues secret ABE keys to the users according to their attributes, a CSP enclave that verifies, stores and processes search requests by users, a KeyTray (KT) that acts as a storage server for SSE keys and a Revocation Enclave (REV) that controls access rights.

How it Works: A data owner u_i generates an SSE key $\mathsf{K_i}$, encrypts her data locally and then sends them to the CSP. Additionally, u_i encrypts $\mathsf{K_i}$ using ABE – this results to a ciphertext $c_p^{\mathsf{K_i}}$ of $\mathsf{K_i}$ – and sends it to KT. Finally, u_i sends a list of access rights to REV for the users that she wishes to share her data with. Access rights are represented as a one dimensional array s of length four, where each bit corresponds to one of the following scopes: view, add, delete and revoke. For example if $s_j = [1, 0, 0, 0]$, u_j can only read files.

If another user u_j wishes to access u_i's encrypted data, she first needs to contact KT and request $c_p^{\mathsf{K_i}}$. Since $c_p^{\mathsf{K_i}}$ is encrypted with ABE, u_j will only be able to decrypt it if her attributes satisfy the underlying policy. Assuming that u_j successfully recovers $\mathsf{K_i}$ she then needs to prove that she is allowed to access u_i's data. To this end, she requests a proof from REV indicating her access rights. With this proof, along with $\mathsf{K_i}$, u_j can create the SSE tokens needed to access the database. Finally, we have designed a revocation mechanism that is based on SGX and is agnostic to the underlying encryption schemes. If u_j wishes to revoke a scope from another user she needs to have certain access right enabled (i.e. $s_j[3] = 1$). Revocation is then as simple as sending a request to REV containing the id of the user to be revoked, u_ℓ, as well as an integer $n < 4$, indicating which bit of s_ℓ will be flipped from 1 to 0.

The security of our scheme is proved through a simulation-based security analysis as well as an analysis showing its resistance against a set of new attacks. The security proof is coupled with extensive experiments that show the efficiency and practicality of our approach. Our experiments mainly aimed at analyzing the processing time. For the implementation of the CP-ABE scheme, we used the library provided by Bethencourt et al. [5] while for the SSE scheme we used the Dynamic Forward Private SSE scheme described in [3]. Finally, for the implementation of the parts that run in secure enclaves we used the SGX-OpenSSL library [1]. Due to space constraints a detailed description of the scheme and its evaluation will be presented in the full version of the paper.

CCS CONCEPTS

• **Security and privacy → Cryptography**; **Key management**; **Public key encryption**; **Symmetric cryptography and hash functions**; **Access control**; **Security protocols**; **Privacy protections**; *Authorization*; Trusted computing;

KEYWORDS

attribute-based encryption, cloud computing, revocation, symmetric searchable encryption

REFERENCES

[1] 2017. SGX-OpenSSL. (2017). https://github.com/sparkly9399/SGX-OpenSSL
[2] Alexandros Bakas and Antonis Michalas. 2019. Modern Family: A Revocable Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX. Cryptology ePrint Archive, Report 2019/682. (2019). https://eprint.iacr.org/2019/682.
[3] Alexandros Bakas and Antonis Michalas. 2019. Multi-Client Symmetric Searchable Encryption with Forward Privacy. Cryptology ePrint Archive, Report 2019/813. (2019). https://eprint.iacr.org/2019/813.
[4] John Bethencourt, Amit Sahai, and Brent Waters. 2007. Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)*. IEEE, 321–334.
[5] John Bethencourt, Amit Sahai, and Brent Waters. 2007. Ciphertext-Policy Attribute-Based Encryption. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07)*. IEEE Computer Society, Washington, DC, USA, 321–334.
[6] Victor Costan and Srinivas Devadas. 2016. Intel SGX Explained. *IACR Cryptology ePrint Archive* 2016, 086 (2016), 1–118.
[7] Antonis Michalas. 2019. The Lord of the Shares: Combining Attribute-based Encryption and Searchable Encryption for Flexible Data Sharing. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (SAC '19)*. ACM, 10.

Funded by the ASCLEPIOS: Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare Project No. 826093 EU research project.

CCSW'19, November 11, 2019, London, United Kingdom
© 2019 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6826-1/19/11.
https://doi.org/10.1145/3338466.3358929