Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing

Submitted by grigby1 on Fri, 06/26/2020 - 12:44pm

Title	Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing
Publication Type	Conference Paper
Year of Publication	2019
Authors	Bouchaala, Mariem, Ghazel, Cherif, Saidane, Leila Azouz
Conference Name	2019 15th International Wireless Communications Mobile Computing Conference (IWCMC)
Date Published	June 2019
Publisher	IEEE
ISBN Number	978-1-5386-7747-6
Keywords	advanced encryption standard, Asymmetric Encryption, attribute-based encryption, authorisation, CipherText Policy Attribute Based Encryption, Cloud access control, cloud computing, cloud migration, composability, compositionality, computational cost, Computational modeling, cost-efficient service, CP-ABE, critical task, cryptography, Cyber-physical systems, data access security, data integrity, data owner overhead, data privacy, data size, efficient cryptographic technique, efficient encryption, Encryption, encryption scheme, entrusted cloud servers, fine-grained access control model, flexible access control model, Human Behavior, individual industries, Metrics, outsourcing, policy-based governance, pubcrawl, resilience, Resiliency, revocable sliced ciphertext policy attribute, revocation, revocation limitations, Scalability, scalable access control model, sensitive data outsourcing, Servers, single slice, sliced revocable solution, splitting algorithm, symmetric encryption

Abstract

Cloud Computing is the most promising paradigm in recent times. It offers a cost-efficient service to individual and industries. However, outsourcing sensitive data to entrusted Cloud servers presents a brake to Cloud migration. Consequently, improving the security of data access is the most critical task. As an efficient cryptographic technique, Ciphertext Policy Attribute Based Encryption(CP-ABE) develops and implements fine-grained, flexible and scalable access control model. However, existing CP-ABE based approaches suffer from some limitations namely revocation, data owner overhead and computational cost. In this paper, we propose a sliced revocable solution resolving the aforementioned issues abbreviated RS-CPABE. We applied splitting algorithm. We execute symmetric encryption with Advanced Encryption Standard (AES)in large data size and asymmetric encryption with CP-ABE in constant key length. We re-encrypt in case of revocation one single slice. To prove the proposed model, we expose security and performance evaluation.

URL	https://ieeexplore.ieee.org/document/8766597
DOI	10.1109/IWCMC.2019.8766597
Citation Key	bouchaala_revocable_2019

advanced encryption standard Asymmetric Encryption attribute-based encryption authorisation CipherText Policy Attribute Based Encryption Cloud access control Cloud Computing cloud migration composability Compositionality computational cost Computational modeling cost-efficient service CP-ABE critical task Cryptography cyber-physical systems data access security data integrity data owner overhead data privacy data size efficient cryptographic technique efficient encryption encryption encryption scheme entrusted cloud servers fine-grained access control model flexible access control model Human behavior individual industries Metrics outsourcing policy-based governance pubcrawl resilience Resiliency revocable sliced ciphertext policy attribute revocation revocation limitations Scalability scalable access control model sensitive data outsourcing Servers single slice sliced revocable solution splitting algorithm symmetric encryption