INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

RACSIT - 17

IMPLEMENTING CLOUD REVOCATION AUTHORITY WITH IDENTITY BASED ENCRYPTION AND ITS APPLICATIONS

Andal S. [*1], Tahera Tasneem [2], MeghanaMary M. [3], Ranjitha G. C. [4], Deepak N.A. [5]
[*1, 2, 3, 4] CSE, Ghousia College of Engineering, India
[5] HOD, CSE, Ghousia College of Engineering, India

DOI: https://doi.org/10.5281/zenodo.572292

Abstract

Identity-based encryption (IBE) is a public key cryptosystem(encoding and decoding) and eliminates the demands of public key infrastructure(PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, a revocable IBE scheme with a key-update cloud service provider (KU-CSP) was proposed. However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user. In the article, we propose a new revocable IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Finally, we extend the proposed revocable IBE scheme to present a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

Keywords: Cloud Revocation Authority; Private Key Generator; Master Time Key; Time Update Key; Identity Key; Identity Based Encryption; Public Key Infrastructure.

Cite This Article: Andal S., Tahera Tasneem, MeghanaMary M, Ranjitha G. C., and Deepak N.A.. (2017). "IMPLEMENTING CLOUD REVOCATION AUTHORITY WITH IDENTITY BASED ENCRYPTION AND ITS APPLICATIONS." *International Journal of Research - Granthaalayah*, 5(4) RACSIT, 38-40. https://doi.org/10.5281/zenodo.572292.

1. Introduction

1.1.Existing System

The PKG sends user the corresponding identity key via a secure channel. Meanwhile, the PKG must generate a random secret value (timekey) for each user and send it to the KU-CSP. Then the KU-CSP generates the current time update key of a user by using the associated time key and sends it to the user via a public channel outsourcing computation technique into IBE to propose a revocable IBE scheme with a key-update cloud service provider (KU-CSP). They shifts the key-update procedures to a KU-CSP to alleviate the load of PKG. Existing scheme also used the similar technique adopted in Tseng and Tsai's scheme, which partitions a user's private key into an identity key and a time update key.

1.2.Disadvantages of Existing System

ID-based encryption (IBE) allows a sender to encrypt message directly by using a receiver's ID without checking the validation of public key certificate. In existing system misbehaving/compromised users in an ID-PKS setting is naturally raised. Immediate revocation method employs a designated semi-trusted and online authority (i.e. mediator) to mitigate the Management load of the PKG and assist users to decrypt cipher-text. The computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is un-scalability in the sense that the KU- CSP must keep a time key for each user so that it will incur the management load.

2. Proposed System

In order to solve both the un-scalability and the inefficiency in existing scheme, we propose a new revocable IBE scheme with cloud revocation authority (CRA). In particular, each user's private key still consists of an identity key and a time update key. We introduce a cloud revocation authority (CRA) to replace the role of the KU-CSP in existing scheme. The CRA only needs to hold a random secret value (master time key) for all the users without affecting the security of revocable IBE scheme. The CRA uses the master time key to generate the current time update key periodically for each non-revoked user and sends it to the user via a public channel. It is evident that our scheme solves the un-scalability problem of the KU-CSP. We construct a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

3. Advantages of Proposed System

The proposed scheme possesses the advantages of both Tseng and Tsai's revocable IBE scheme and existing scheme. The proposed present framework of our revocable IBE scheme with CRA and define its security notions to model possible threats and attacks. CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

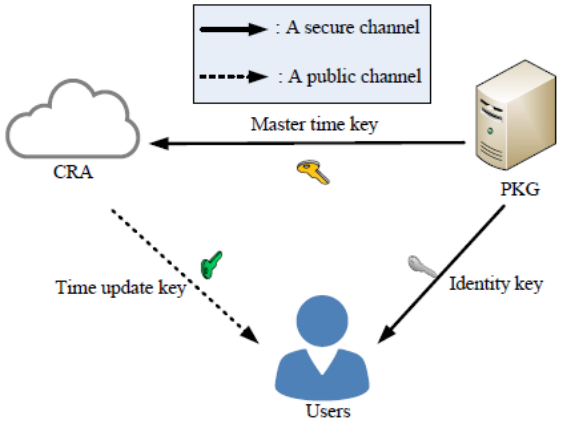

Figure 1: System Architecture

References

[1] Yuh-Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang, "Identity-Based Encryption with Cloud Revocation Authority and Its Applications , IEEE TRANS. CLOUD COMPUTING 2016.

*Corresponding author.
E-mail address: andal9585@gmail.com