International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 11th Dec 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-11

Title **PRDADC: PROTECTED DATA DISTRIBUTION IN CLOUD**

Volume 08, Issue 12, Pages: 53–57.

Paper Authors

Y MOUNIKA, RAVI KUMAR CHANDU

Cmrec, Hyderabad, T.S, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

PRDADC: PROTECTED DATA DISTRIBUTION IN CLOUD

Y MOUNIKA[1], RAVI KUMAR CHANDU[2]

[1]M.Tech Student, Dept of CSE, Cmrec, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Cmrec, Hyderabad, T.S, India

ABSTRACT:

Cloud storage is a cloud application that frees organizations from creating internal data storage systems. However, cloud storage poses security problems. In the case of group shared data, the data faces internal threats to a private and unconventional cloud. Sharing data securely between groups of accountants is a serious investigation problem for legitimate users and criminals. In this document, we suggest the Secure Data Sharing in Clouds methodology that establishes: 1) data confidentiality and integrity; 2) access control. 3) Data exchange (forwarding) without the use of algorithmic redefinition; 4) threat security from the inside; and 5) access control back and forth. The methodology encrypts a file with a single encryption key. Two different main publications are created for each user, with only one shared user. Having only one part of the key allows the methodology to address internal threats. The other main publication is stored by a reliable party, which is called an encryption server. The methodology applies to both traditional and mobile cloud computing. We implement a practical prototype of the The methodology and evaluate its performance based on the time spent on different operations. We are officially validating the work of using the top-level Petri nets, the Satisfability Modulo theory Library and the Z3 Store. The results proved encouraging and show that has the ability to use it effectively to share secure data in the cloud.

Keywords: Encryption, authentication, cloud computing, outsourcing computation, revocation authority. Access control, cloud computing, high-level Petri nets (HLPNs), modeling, Satisfiability Modulo Theory (SMT), Scyther, verification.

1. INTRODUCTION:

ID-PKS [1], [2] is an attractive alternative to public key cryptography. The ID-PKS configuration eliminates the PKI requirements and certificate management in the traditional public key configuration. The ID-PKS configuration consists of users and a trusted third party (such as the private key creator, PKG). PKG is responsible for creating a private key for each user using the associated identification information (such as email address, name or Social Security number). Therefore, a certificate and PKI are not required in the associated cryptographic mechanisms within the ID-PKS configuration. In this case, the IBE allows the sender to directly encrypt the

message with the recipient's ID without validating the validation of the public key certificate. Consequently, the recipient uses the private key associated with their identity / decryption to decrypt this encrypted text. Since the configuration of the public key must provide a mechanism for user cancellation, the problem of finding how to avoid abusive / vulnerable users in the ID-PKS configuration arises naturally. In traditional public key configuration, CRL [3] is a known revocation method. In a CRL curriculum, if a party receives a public key and a certificate associated with it, it first validates it and then searches for the CRL to ensure that the public key is not revoked. In such a case, the procedure requires online assistance under PKI to cause communication bottlenecks. To improve performance, several effective cancellation mechanisms [4], [5], [6], [7], [8] have been well studied for traditional public key configurations for PKI. In fact, researchers also pay attention to the problem of canceling the ID-PKS configuration. Several revocable IBE schemes have been suggested regarding cancellation mechanisms in the ID-PKS configuration. In order to ease the burden of PKG in the Poon and Franklin scheme, he proposed another method of cancellation, called immediate cancellation. The immediate revocation method employs a certain semi-reliable and online authority (that is, the means) to ease the burden of administration on the PKG and help users decipher the encrypted text. In this case, the online broker must maintain the exchange of the private keys of all users. Since the decryption process must involve both parties, neither the user nor the online media can fool each other. When the user is revoked, the online agent must stop helping the user. However, the online broker should help users to decode each encrypted text so that it becomes a bottleneck for schemes such as considerably increasing the number of users. On the other hand, in the invalidation method of Boneh and Franklin [2], all users must periodically update the new private keys sent by PKG. As more users grow, downloading important updates becomes the bottleneck for PKG. The IBE scheme proposal is subject to cancellation to improve the efficiency of the main updates. The cancelable IBE system is based on the Fuzzy IBE concept and adopts the full subtree method to reduce the number of major updates from linear to logarithmic in number of users. In fact, with the users' binary tree data structure, the scheme efficiently facilitates the download of the main PKG update. In addition, the security of the IBL revocable IBL scheme has been improved. By providing a secure identity adaptation scheme. However, the scheme of Boldyreva et al. It results in several problems:

(1) The size of the private key for each user is 3log n points on an elliptical curve, where n is the number of paper nodes (users) in the binary tree.

(2) The scheme also results in a significant workload in computer encryption and decryption procedures.

(3) It is a massive PKG download to keep the binary tree with a large number of users

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

2. TERMINOLOGY AND PROBLEM STATEMENT

The IBE to Outsourcing calculation technology offered proposes a cancelable IBE plan with a cloud update service provider (KU-CSP). They convert the main update procedure to KU-CSP to reduce PKG download. Use the similar method adopted in the Tseng and Tsai scheme, which divides the user's private key into an identity key and the time update key. PKG sends an appropriate identity key through a secure channel. Meanwhile, PKG must create a random secret value (time key) for each user and send it to KU-CSP. Then, the current time update key of the user KUCSPgenering uses the linked time key and sends it to the user through a public channel. The IBE allows the sender to directly encrypt the message with the recipient's ID without validating the validation of the public key certificate. Misconduct / endanger users when configuring ID-PKS normally. The immediate revocation method uses a reliable and semi-reliable (ie, average) online reference to ease the burden of PKG management and help users decode encrypted text. Account and connection costs are higher than previous cancelable IBEschemes. Another drawback is the inability to expand the feeling that KU-CSP must maintain a time code for each user to bear the burden of administration.

3. IMPLEMENTING DYNAMIC FACETED SEARCH

We offer IBE scheme system operations that can be canceled with CRA. Our system has three roles: the private key generator (PKG), the cloud cancellation authority (CRA) and the users (senders and receivers). First, PKG sets the master secret key α, the main time key β and the total number of z periods, and sends the main time key β to the CRA. PKG uses the master secret key α to calculate the user's DID ID key with the ID, and sends the ID key the DID to the user through a secure channel. On the other hand, the CRA is responsible for producing time update keys for all users that are not revoked with the main time key β. To do this, at the beginning of each period i, the CRA uses the identity of the primary time key and the user ID that has not been revoked to create the current time update key PID, i, and sends it to the user through a public channel (for example, email). When the sender wishes to send an M message to a recipient with an ID in period i, the sender issues an encrypted text C = E (ID, i, M) and sends it to the recipient, where E indicates our IBE scalable encryption algorithm with CRA. Upon receiving the encrypted text, the receiver uses the DID identification key and the PID time update key, and to decrypt the encrypted text.

System configuration: Trusted PKG takes two parameter inputs, which are the safe parameter λ and the total number z of intervals. PKG randomly selects two periodic groups G and GT for a preliminary order q> 2 λ. In addition, randomly choose the generator P of G, a permissible binomial map e: G x G → GT and two secret values α, β ∈ Z ∗ q. The value α is the master secret key used to calculate the public key of the system Ppub = α • P. PKG then transfers the primary time key to the CRA through a secure channel. The value of is used to

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

calculate the public key of the cloud Cpub = P • P. PKG selects three hash functions H0 and H1: {0 and 1} ∗ → G and H2: GT → {0, 1} l and H3: { 0, 1} ∗ → {0, 1} l, where l is constant, and generates the general parameters PP = <q, G, GT, e, P, P ˆ pub, Cpub, H0, H1, H2, H3> .

Identity key extraction: Upon receiving the ID ∈ {0,1} ∗ for the user, PKG uses the master secret key α to calculate the corresponding identification key DID = α • SID, where SID = H0 (ID). Then, PKG sends the DID identity key to the user through a secure channel.

Time key update: to create the PID time update key, I am in the first period of a user with ID ∈ {0,1} ∗, CRA uses the main time key β to calculate the update key of PID time, i = β • TID, i, where TID, i = H1 (ID, i). Finally, the CRA sends the PID i i update key to the user through a public channel.

Encoding: to encode the message M ∈ {0, 1} l with the recipient's ID and period i, the transmitter chooses a random value r ∈ Z ∗ q and calculates U = r • P. The sender also calculates V = M ⊕ H2 ((g1 • g2) r), where g1 = ˆe (SID, Ppub) and g2 = (e (TID, i, Cpub). Next, the transmitter calculates W = H3 (U, V, M, ID, i) Finally, the sender sets the encoded text as C = (U, V, W) and sends it to the recipient.

Decoding: to decode C = (U, V, W) with the recipient's ID and period i, the recipient uses their DID and PID, calculate the plain text M = V ⊕ H2 ((e (DID + PID, i , U)). If W = H3 (U, V, M, ID, i), M returns as the unusual text, otherwise ⊥ is returned.

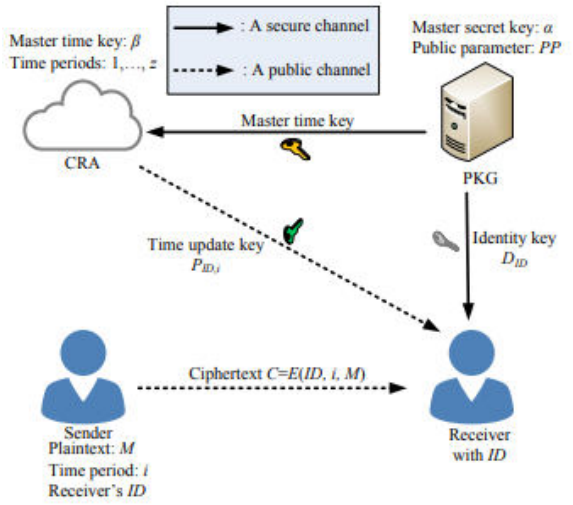

Figure 1: System Architecture

4. CONCLUSION:

In this article, there is a new cancelable IBE scheme with a revocation authority in the cloud in which a CRA performs a revocation action to mitigate the PKG burden. This technique has been used to calculate outsourcing with other authorities in a cancelable IBE scheme with KU-CSP. However, your plan requires higher mathematical and communication costs than the IBE diagrams proposed above. For the time key update procedure, KU-CSP must keep the scheme at a secret value for each user that is expandable. In our reversible IBE system with CRA, CRA has only the master time key to perform time key update actions for all users without affecting security. Compared to the scheme, the calculation and communication performance has been significantly improved. Through experimental results and performance analysis, our scheme is very suitable for mobile devices. For the security analysis, we have shown that our plot is completely

secure against adaptive identity attacks under the Diffie-Hellman linear assumption. Finally, based on the IBE's cancelable scheme with CRA, we have created a CRAaided Authentication System with limited time privileges to manage a large number of different cloud services.

REFERENCES:

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Crypto'84, LNCS, vol. 196, pp. 47-53, 1984.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proc. Crypto'01, LNCS, vol. 2139, pp. 213-229, 2001.

[3] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 3280, 2002.

[4] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," Proc. Crypto'98, LNCS, vol. 1462, pp. 137-152, 1998.

[5] M. Naor and K. Nissim, "Certificate revocation and certificate update," IEEE Journal on Selected Areas in Communications, vol. 18 , no. 4, pp. 561 - 570, 2000.

[6] S. Micali, "Novomodo: Scalable certificate validation and simplified PKI management," Proc. 1st Annual PKI Research Workshop, pp. 15-25, 2002.

[7] F. F. Elwailly, C. Gentry, and Z. Ramzan, "QuasiModo: Efficient certificate validation and revocation," Proc. PKC'04, LNCS, vol. 2947, pp. 375-388, 2004.

[8] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," Proc. Financial Cryptography, LNCS, vol. 4886, pp. 247-259, 2007.