Available online at http://www.journalijdr.com

IJDR

International Journal of DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 07, Issue, 06, pp.13107-13109, June, 2017

Full Length Research Article

CLOUD REVOCATION AUTHORITY USING IDENTITY BASED ENCRYPTION

[1,*]Ashwini, A., [2]Nethravathi, H.T., [3]Hemavathi, M. and [4]Asha, R.N.

[1,2,3]B.E. Student, Global Academy of Technology
[4]Asst. Prof., Dept. of CSE, Global Academy of Technology

ARTICLE INFO

Article History:
Received 24th March, 2017
Received in revised form
09th April, 2017
Accepted 27th May, 2017
Published online 16th June, 2017

Key Words:
Encryption,
Authentication,
Cloud Computing,
Outsourcing Computation,
Revocation Authority.

ABSTRACT

Identity-based encryption (IBE) is a public key cryptosystem and eliminates the demands of public key infras structure (PKI) and certificate admiration in conventional public key settings .Due to the absence of PKI, the revocation problem is a critical issue in IBEs settings .Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li et al. proposed a revocable IBE scheme with a key -update cloud service provider (KU-CSP). 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 lac k of scalability in the sense that the KU -CSP must keep a secret value for each user. In the article, we propose e a new revocable IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings, namely, the performance is significantly imp roved and the CRA holds only a system s secret for all the users. For security analysis is , 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. We proposed a new revocable IBE scheme with a cloud revocation authority (CRA), in which the revocation procedure is performed by the CRA to alleviate the load of the PKG. This outsourcing computation technique with other authorities has been employed in Li et al.'s revocable IBE scheme with KU -CSP. Their scheme requires higher computational and communicational costs than previously proposed IBE schemes. For the time key update procedure, the KU-CSP in Li et al.'s scheme must keep a secret value for each user so that it is lack of scalability. In our revocable IBE scheme with CRA, the CRA holds only a master time key to perform the time key update procedures for all the users without affecting security

INTRODUCTION

Identity (id)-based public key s system (ID-PKS) is an attractive alternative for public key cryptography. ID-PKS setting eliminates the demands of public key infra-structure (PKI) and certificate administration in conventional public key settings. An ID-PKS setting cons is it's of users and a trusted third party (i.e. Private Key generator, PKG). The PKG is res pons bile to generate each user's private key by u sing the as associated id information (e.g. E-mail address, name or social security number). Therefore, no certificate and PKI are required in the associated cryptographic mechanisms under ID-PKS settings. In s such a case e, Id-based encryption (IBE) allows a s ender to encrypt message directly by using a receiver's id without checking the validation of public key certificate. Accordingly, the receiver uses the private key associated with her/his id to decrypt such cipher text. Since a public key setting has to provide a user revocation mechanism, the research issue on how to revoke misbehaving/ compromised users in a n ID-PKS setting is naturally raised. In conventional public keys settings certificate revocation list (CRL) is a well-known revocation approach. In the CRL approach, if a party receives a public key and its associated certificate, she/he fir t validates t hem and then looks up the CRL to ensure that the public key has not been revoked. In such a case, the procedure requires the online. Assistance under PKI. So that it will incur communication bottleneck. To improve the performance, several efficient revocation mechanisms for conventional public key settings Have been well s studied for PKI. Indeed, researchers also pay attention to the revocation issue of ID-PKS settings.

Corresponding author: Ashwini, A.,
B.E. Student, Global Academy of Technology.

Several revocable IBE schemes have been proposed regarding the revocation mechanisms in ID-PKS settings. In 2001, boneh and franklin proposed the first practical IBE scheme from the Weil pairing and suggested a s imp le revocation method in which each non-revoked user receives a new private key generated by the PKG periodically. A period can be set as a day, a week, a month, etc. A sender uses a des ignited receiver's id and current period to encrypt messages while the designated receiver decrypts the cipher text using the current private key. Hence, it is necessary for the users to update new private keys periodically. To revoke a user, the PKG simply s tops providing the new private key for the user. It is obvious that a secure channel must be established between the PKG and each user to transmit the new private key and this would result in heavy load for the pkg.

LITERATURE S URVEY

R. Hous ley, W. P olk, W. For d, and D. Solo

Is proposed the x.509 v3 certificate and x.509 v2 certificate revocation list for us e in the internet. An overview of this approach and model is provided as an introduction a s et of required certificate extent ions is specified. The x.509 v 2 CRL format is described in detail a long with standard and internet -specific extensions. An algorithm for x.509 certification path validation is described. An as n.1 module and examples are provided in the appendices. [Standards -track]

M. Scott, N. Cos tigan, and W. AbdulW ahab:

Is proposed the imp le mentation of various pairings on a contemporary 32-b its mart-card, the philipshipers marttm, and an instantiation of the mips -32 based s mart mips tm architecture. Three types of pairing are considered first the standard Tate pairing on a non-super singular curve e (Fp), second the ate pairing, also on a non-super singular curve e(FP), and finally the pairing on a super singular curve e(f2m).

T.-Y. W u and Y.-M. Ts eng:

Is proposed the identity (id)-based public-key system with bilinear pairings defined on elliptic curves offers a flexible approach to achieve simplifying the certificate management as compared with the recently proposed pairing -based user authentication schemes , our protocol provides both mutual authentication and key exchange. Performance analysis is made to s how that our presented protocol is well suited for mobile client–server environment. Security analysis is given to demonstrated that our proposed protocol is provably secure against t previous attacks .

F. F. El wailly, C. Gentr y, and Z. Ramz an:

Is proposed two new schemes for efficient certificate revocation. At the core of our schemes is a novel cons truced termed a Quasimodo tree, which is like a merkle tree but contains a length-2 chain at the leaves and also directly utilizes interior Nodes . This concept is of independent interest, and we believe such trees will have numerous other applications. The idea, while s imp le, immediately provides a strict improvement in the relevant time and communication complexities over previously published scheme

EXIS TING S YSTEM

The concept of attribute-based encryption (ABE) which refines IBE scheme by associating cipher texts and a s et of attributes. In an ABE scheme, the PKG typically s ends the corresponding attribute keys for the user with several attribute. An ABE scheme allows a data owner to encrypt data under a s et of attributes associated with access structures , and users who own these corresponding attribute keys are able to decrypt the encrypted data. Afterward, there are numerous ABE schemes that have been propos ed. Indeed, we may combine the revocability concept of the proposed revocable IBE scheme with the existing ABE Schemes to construct revocable ABE schemes. Indeed, proposed an ABE scheme with us er/attribute revocation for various applications. Both schemes still adopt the sub -tree method in to address the revocation rekeying issue so that a secure channel is used to transmit the new updated user keys and attribute keys .

DISADVANTAGE

It consumes more time gives less accuracy.

Proposed Architecture Diagram

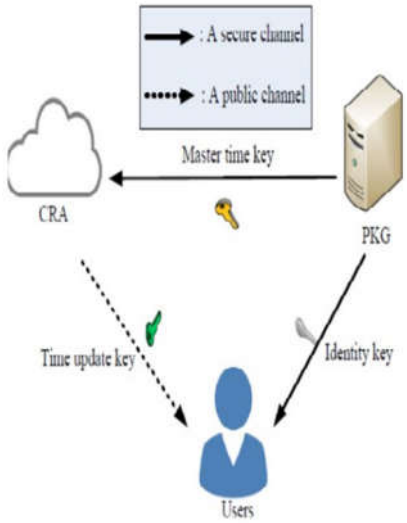

Figure 1. Proposed Architecture Diagram

MO DULES

- Cloud Based Revocation.
- Public Key Generator.
- Revocation Authority.
- Encryption Module.

Cloud Based Revocation:

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. Cloud revocation authority (CRA) to solve the two s shortcomings , namely, the performance is s significantly improved and the CRA holds only a system s secret for all the users. For security analysis is, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie -Hellman (DBDH) assumption. Revocable IBE scheme to present a CRA -aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

Public K`ey Generator

Revocation method in which each non -revoked user receives a new private key generated by the PKG periodically. A period can be set as a day, a week, a month, etc. A s ender uses a designated receiver's ID and current period to encrypt messages while the designated receiver decrypts the cipher text using the current private key, it is necessary for the users to update new private keys periodically. To revoke a user, the PKG simply s tops providing the new private key for the user. It is obvious that a secure channel must be established between the PKG and each user to transmit t he knew private key and this would result in heavy load for the PKG.

Re vocation Authority

Key updates from linear to logarithmic in the number of users. However, each user's private key size is O (log n), where n is the number of users. These schemes s till used a secure channel to transmit periodic private keys while no other authority s hares the responsibility of user revocation. The PKG in Li et al.'s scheme and ours may also perform the revocation Operations. Both the KU CSP and the CRA are designated t o s hare responsibility for performing user revocation.

Encr yption Module

To reduce the sizes of both private keys and update keys, Park et al. proposed a new revocable IBE scheme by using multiline maps , but the size of the public par meters is dependent to the number of users the secret key size of each user increases quadratic ally in the hierarchy tree wherein a low-level user must t know the history of key updates performed by ancestors in the current time period, and it renders the scheme very complex Seo and Emura proposed a new method to construct a novel revocable HIBE scheme with history -free updates .

Conclusion

We proposed a new revocable IBE scheme with a cloud revocation authority (CRA), in which the revocation procedure is performed by the CRA to alleviate the load of the PKG. This outsourcing computation technique with other authorities has been employed in Li et al.'s revocable IBE scheme with KU - CSP. In our revocable IBE scheme with CRA, the CRA holds only a master time key to perform the time key update procedures for all the users without affecting security. As compared with Li et a l's scheme, the performances of computation and communication are significantly imp roved. By experimental results and performance analysis, our scheme is well suited for mobile devices. Our scheme is semantically secure against adaptive-ID attacks under the decisional bilinear Diffie-Hellman assumption. Based on the proposed revocable IBE scheme with CRA, we constructed a CRA aided authentication scheme with period -limited privileges for managing a large number of various cloud services.

REFERENCES

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

Boneh, D., Ding, X., Tsudik, G. and Wong, C.M. 2001. "A Method for fast revocation of public key certificates and security capabilities," Proc. 10th USENIX Security Symp., pp.297-310.

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

Ding, X. and Tsudik, G. 2003. "Simple identity -based cryptography with mediated RSA," Proc. CT-RSA'03, LNCS, vol. 2612, pp. 193-210.

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

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

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

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

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

Shamir, A.1984. "Identity-based cryptosystems and signatureschemes," Proc. Crypto'84, LNCS, vol. 196, pp. 47-53, 1984.

****