International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

An efficient revocable IBE scheme with CRA

Padmaja.V [1] ,Mrs P.Madhura[2]
[1]Department Of Computer Applications , Riims College, Tirupati, Andhra Pradesh, india
[2]Head, Department Of Computer Applications,Riims,Tirupati, Andhra Pradesh, india

ABSTRACT

Cloud computing is getting increasingly consideration from the data and correspondence advances industry as of late. In existing, an approach which utilizing logs model to building a measurable neighborly framework. Utilizing this model we can rapidly accumulate data from distributed computing for a few sorts of measurable reason. Furthermore, this will diminish the many sided quality of those sorts of legal sciences. we propose another revocable IBE conspire with a cloud renouncement specialist (CRA) to understand the two inadequacies, in particular, the execution is essentially enhanced and the CRA holds just a framework mystery for every one of the clients. For security examination, we exhibit that the proposed conspire is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) suspicion. At long last, we broaden the proposed revocable IBE plan to introduce a CRA-helped confirmation plot with period-restricted benefits for dealing with countless cloud administrations.

Keywords: Cloud computing, IBE scheme, cloud revocation authority (CRA)

I. INTRODUCTION

In conventional public key 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its associated certificate, she/he first validates them and then looks up the CRL to ensure that the public key has not been revoked.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 studied for PKI. Indeed, researchers also pay attention to the revocation issue of ID-PKS settings. Several revocable IBE schemes have been proposed regarding the revocation mechanisms in ID-PKS settings.

ID-PKS setting takes out the requests of open key foundation (PKI) and endorsement organization in customary open key settings. An ID-PKS setting comprises of clients and a trusted outsider. The PKG is mindful to produce every client's private key by utilizing the related ID data. Consequently, no testament and PKI are required in the related cryptographic instruments under ID-PKS settings. In such a case, ID-based encryption (IBE) enables a sender to encode message specifically by utilizing a recipient's ID without checking the approval of open key authentication. As needs be, the collector utilizes the private key related with her/his ID to decode such figure content. Since an open key setting needs to give an utilization disavowal component, the examination issue on the best way to repudiate making trouble/bargained clients in an ID-PKS setting is normally raised.

II. ALGORITHM

IBE SCHEME

Here, we propose an efficient revocable IBE scheme with CRA.

- System setup: A trusted PKG takes as input two parameters, namely, a secure parameter λ and the total number z of periods. The PKG randomly chooses two cyclic groups G and GT of a prime order $q > 2 \lambda$. Also, it randomly chooses a generator P of G, an admissible bilinear map $\hat{e} : G \times G \rightarrow GT$ and two secret values $\alpha, \beta \in Z * q$. The value α is the master secret key used to compute the system public key $Ppub = \alpha \cdot P$. The PKG then transmits the master time key β to the CRA via a secure channel. The value β is used to compute the cloud public key $Cpub = \beta \cdot P$. The PKG selects three hash functions $H0, H1 : \{0, 1\} * \rightarrow G$, $H2 : GT \rightarrow \{0, 1\} l$, and $H3 : \{0, 1\} * \rightarrow \{0, 1\} l$, where l is fixed, and publishes the public parameters $P P =< q, G, GT , e, P, P \hat{} pub, Cpub, H0, H1, H2, H3 >$.
- Identity key extract: Upon receiving the identity $ID \in \{0, 1\} *$ of a user, the PKG uses the master secret key α to compute the corresponding identity key $DID = \alpha \cdot SID$, where $SID = H0(ID)$. Then, the PKG sends the identity key DID to the user via a secure channel.
- Time key update: To generate the time update key PID,i at period i for a user with identity ID $\in \{0, 1\} *$, the CRA uses the master time key β to compute the time update key $PID,i = \beta \cdot TID,i$, where $TID,i = H1(ID, i)$. Finally, the CRA sends the time update key PID,i to the user via a public channel.
- Encryption: To encrypt a message $M \in \{0, 1\} l$ with a receiver's identity ID and a period i, a sender selects a random value $r \in Z * q$ and computes $U = r \cdot P$. The sender also computes $V = M \oplus H2((g1 \cdot g2) r)$, where $g1 = \hat{e}(SID, Ppub)$ and $g2 = \hat{e}(TID,i, Cpub)$. Then, the sender computes $W = H3(U, V, M, ID, i)$. Finally, the sender sets the ciphertext as $C = (U, V, W)$ and sends it to the receiver.
- Decryption: To decrypt a ciphertext $C = (U, V, W)$ with a receiver's identity ID and a period i, the receiver uses his/her identity key DID and time update key PID,i to compute the plaintext $M = V \oplus H2(\hat{e}(DID + PID,i, U))$. If $W = H3(U, V, M, ID, i)$, return M as the plaintextoutput, else return $\perp$.

The correctness of the decryption algorithm follows since

$V \oplus H2(\hat{e}(DID + PID,i, U))$
$= M \oplus H2((g1 \cdot g2) r) \oplus H2(\hat{e}(DID + PID,i, U))$
$= M \oplus H2((g1 \cdot g2) r) \oplus H2(g r 1 \cdot g r 2)$
$= M$,

where the penultimate equality is due to the fact that

$H2(\hat{e}(DID + PID,i, U))$
$= H2(\hat{e}(DID, U) \cdot \hat{e}(PID,i, U))$
$= H2(\hat{e}(\alpha \cdot SID, r \cdot P) \cdot \hat{e}(\beta \cdot TID,i, r \cdot P))$
$= H2(\hat{e}(SID, \alpha \cdot P) r \cdot \hat{e}(TID,i, \beta \cdot P) r)$
$= H2(\hat{e}(SID, Ppub) r \cdot \hat{e}(TID,i, Cpub) r)$
$= H2(g r 1 \cdot g r 2)$.

III. CONCLUSION

In this article, we proposed another revocable IBE conspire with a cloud disavowal expert (CRA), in which the repudiation technique is performed by the CRA to mitigate the heap of the PKG. This outsourcing calculation strategy with different experts has been utilized in Li et al's. revocable IBE conspire with KU-CSP. Be that as it may, their plan requires higher computational and communicational expenses than beforehand proposed IBE plans. At last, in light of the proposed revocable IBE plot with CRA, we developed a CRA aided verification conspire with period-restricted benefits for dealing with countless cloud administrations.

IV. REFERENCES

[1]. G. Hanaoka and J. Weng. Generic constructions of parallel key-insulated encryption. In SCN, volume 6280 of LNCS, pages 36–53. Springer, 2010.

[2]. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai. Identity-based hierarchical strongly key-insulated encryption and its application. In

ASIACRYPT 2005, volume 3788 of LNCS, pages 495–514. Springer, 2005.

[3]. J. Horwitz and B. Lynn. Towards hierarchical identity-based encryption. In EUROCRYPT 2002, volume 2332 of LNCS, pages 466–481. Springer-Verlag, 2002.

[4]. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In TCC 2010, volume 5978 of LNCS, pages 455–479. Springer, 2010.

[5]. A. B. Lewko and B. Waters. Unbounded HIBE and attribute-based encryption. In EUROCRYPT 2011, volume 6632 of LNCS, pages 547–567. Springer, 2011.

[6]. B. Libert, J.-J. Quisquater, and M. Yung. Parallel key-insulated public key encryption without random oracles. In PKC 2007, volume 4450 of LNCS, pages 298–314. Springer, 2007.

[7]. B. Libert and D. Vergnaud. Adaptive-ID secure revocable identity-based encryption. In CT-RSA 2009, volume 5473 of LNCS, pages 1–15. Springer, 2009.

[8]. J. H. Seo and K. Emura. Efficient delegation of key generation and revocation functionalities in identitybased encryption. In CT-RSA 2013, volume 7779 of LNCS, pages 343–358. Springer, 2013.

[9]. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, CRYPTO 2009, volume 5677 of LNCS, pages 619–636. Springer-Verlag, 2009.

[10]. J. Weng, S. Liu, K. Chen, D. Zheng, and W. Qiu. Identity-based threshold key-insulated encryption without random oracles. In CT-RSA 2008, volume 4964 of LNCS, pages 203–220. Springer, 2008.

[11]. M. Bellare and A. Palacio. Protecting against key exposure: strongly key-insulated encryption with optimal threshold. In IACR Cryptology ePrint Archive 2002:064, 2002. 12 A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In ACM CCS 2008, pages 417–426, 2008.

[12]. D. Boneh and X. Boyen. Efficient selective-id identity based encryption without random oracles. In EUROCRYPT 2004, volume 3027 of LNCS, pages 223–238. Springer-Verlag, 2004.

[13]. N. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "Analyzing the Energy Consumption of Security Protocols", ISLPED 2003.

[14]. C. K. Koc, "High-speed RSA implementation", Tech. Rep. TR 201, RSA Laboratories, November 1994.

[15]. D. Hankerson, A. Menezes, S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, Inc. 2004. ISBN 0-387-95273-X.

[16]. B. Kaliski, "TWIRL and RSA Key Size", RSA Laboratories Technical Note, May 2003.

[17]. D. Eastlake, P. Jones, "US Secure Hash Algorithm 1 (SHA1)", IETF Request for Comments 3174, 2001.

[18]. J. Polastre, J. Hill, D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks", SenSys, 2004.

[19]. M. Hamilton, M. Allen, D. Estrin, J. Rottenberry, P. Rundel, M. Srivastava, and S. Soatto. "Extensible Sensing System: An advanced Network Design for Microclimate Sensing", http://www.cens.ucla.edu