International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Secure Semantic Scheme for Multiple Cloud Storage Services by Using IBE Scheme

Gajula Chandrababu[1], K Somasekhar[2]

[1]Department of MCA, RCR Institutes of Management &Technology,Tirupati,Andhra Pradesh,India

[2]Assistant Professor, Department of MCA, RCR Institutes of Management &Technology,Tirupati,Andhra Pradesh , India

ABSTRACT

An online comprehensive client care resolution to manage client interaction and complaints Identity-based encryption (IBE) could be a public key cryptosystem and eliminates the strain of public key infrastructure (PKI) and certificate administration in standard public key settings. attributable to the absence of PKI, the revocation drawback could be a crucial issue in IBE settings. many rescindable IBE schemes are planned concerning this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li et al. planned a rescindable IBE theme with a key-update cloud service supplier (KU-CSP). However, their theme has 2 shortcomings. One is that the computation and communication prices ar on top of previous revocable IBE schemes. the opposite disadvantage is lack of measurability within the sense that the KU-CSP should keep a secret price for every user. within the article, we tend to propose a replacement rescindable IBE theme with a cloud revocation authority (CRA) to resolve the 2 shortcomings, namely, the performance is considerably improved and also the CRA holds solely a system secret for all the users. For security analysis, we demonstrate that the planned theme is semantically secure beneath the decisional additive Diffie-Hellman (DBDH) assumption. Finally, we extend the planned rescindable IBE theme to gift a CRA-aided authentication theme with period-limited privileges for managing an oversized range of assorted cloud services.

Keywords: Encryption, Authentication, Cloud Computing, Outsourcing Computation, Revocation Authority.

I. INTRODUCTION

Identity (ID)- based open key framework (ID-PKS) is an alluring option for open key cryptography. ID-PKS setting dispenses with the requests of open key foundation (PKI) and endorsement organization in ordinary open key settings. An ID-PKS setting comprises of clients and a trusted outsider (i.e. private key generator, PKG). The PKG is mindful to create every client's private key by utilizing the related ID data (e.g. email address, name or government managed savings number). In this way, no endorsement what's more, PKI are required in the related cryptographic components under ID-PKS settings. In such a case, ID-based encryption (IBE) enables a sender to encode message straightforwardly by utilizing a beneficiary's ID without checking the approval of open key testament. Appropriately, the recipient utilizes the private key related with her/his ID to decode such ciphertext. Since an open key setting needs to give a client disavowal instrument, the exploration issue on the best way to renounce getting out of hand/traded off clients in an ID-PKS setting is normally raised. In customary open key settings, testament denial list (CRL) is an outstanding renouncement approach. In the CRL approach, if a gathering gets an open key and its related authentication, she/he initially approves

them and after that turns upward the CRL to guarantee that general society key has not been renounced. In such a case, the technique requires the on the web help under PKI with the goal that it will bring about correspondence bottleneck. To enhance the execution, a few effective disavowal instruments for ordinary open key settings have been very much concentrated for PKI. To be sure, analysts additionally focus on the renouncement issue of ID-PKS settings. A few revocable IBE plans have been proposed with respect to the denial components in ID-PKS settings.

Distributed computing is a data innovation (IT) worldview that empowers pervasive access to shared pools of configurable framework assets and more elevated amount benefits that can be quickly provisioned with insignificant administration exertion, regularly finished the Internet. Distributed computing depends on sharing of assets to accomplish cognizance and economies of scale, like an open utility.

Outsider mists empower associations to center around their center organizations as opposed to using assets on PC framework and maintenance. Advocates take note of that distributed computing enables organizations to stay away from or limit in advance IT foundation costs. Advocates additionally assert that distributed computing enables endeavors to get their applications up and running speedier, with enhanced reasonability and less support, and that it empowers IT groups to all the more quickly modify assets to meet fluctuating and capricious demand. Cloud suppliers normally utilize a pay-as-you-go demonstrate, which can prompt startling working costs if directors are not acquainted with cloud-valuing models.In this article, we first present the framework of our revocable IBE scheme with CRA and define its security notions to model possible threats and attacks. Accordingly, a new revocable IBE scheme with CRA is proposed. As the adversary model presented in it consists of two adversaries, namely, an inside adversary (or a revoked user) and an outside adversary. For security analysis, we formally demonstrate that our scheme is semantically secure against adaptive-ID and chosen-ciphertext attacks (CCA) in the random oracle model under the bilinear decision Diffie-Hellman problem . Finally, based on the proposed revocable IBE scheme with CRA, we construct a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

Multi-Cloud is the usage of different processing benefits in a solitary heterogeneous engineering. Multi-Cloud Capacity implies the usage of different distributed storage administrations utilizing a solitary web interface instead of the defaults gave by the distributed storage merchants in a solitary heterogeneous design. Multi-Cloud information frameworks have the ability to improve information sharing and this viewpoint will be fundamentally of incredible help to information clients. It empowers information proprietors to share their information in the cloud. In any distributed computing model, security is viewed as the most pivotal angle because of the affectability and delicacy of the client's data or information put away in a cloud. Directly, every Organization is driving its IT office to scale up their information sharing frameworks. Most cloud administrations are not free and have diverse sizes. For example, Single Cloud Capacity falls among the administrations with capacity constraint which makes it disadvantageous in contrast with multi-cloud capacity. The fundamental preferred standpoint of utilizing multi distributed storage is execution and higher security for information sharing. In the single distributed storage information stays on the unified stockpiling which can be effectively gotten to by the malevolent insiders. Organizations should begin thinking about working with in excess of one cloud supplier at once - for cost investment funds, execution, catastrophe recuperation and different reasons. Most business associations share the majority of their information

with either their customers or providers and consider information sharing as a need. Through information sharing, higher efficiency levels are come to.

II. ALGORITHM

Here, we propose an efficient revocable IBE scheme with CRA. The scheme is constructed by using bilinear pairings and consists of five algorithms.

• 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 $e^{\wedge} : G \times G \rightarrow GT$ 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 = α · 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 = β ·P. The PKG selects three hash functions H0, H1 : {0, 1} ∗ → G, H2 : GT → {0, 1} l , and H3 : {0, 1} ∗ → {0, 1} l , where l is fixed, and publishes the public parameters P P =< q, G, GT , e, P, P ^ pub, Cpub, H0, H1, H2, H3 >. • Identity key extract: Upon receiving the identity ID ∈ {0, 1} ∗ of a user, the PKG uses the master secret key α to compute the corresponding identity key DID = α · 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 ∈ {0, 1} ∗ , the CRA uses the master time key β to compute the time update key PID,i = β·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 ∈ {0, 1} l with a receiver's identity ID and a period i, a sender selects a random value r ∈ Z ∗ q and computes U = r ·P. The sender also computes V = M ⊕H2((g1 · g2) r), where g1 = ^e(SID, Ppub) and g2 = ^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 ⊕ H2(^e(DID + PID,i, U)). If W = H3(U, V, M, ID, i), return M as the plaintextoutput, else return ⊥. The correctness of the decryption algorithm follows since

$$\begin{aligned} & V \oplus H_2(\hat{e}(D_{ID} + P_{ID,i}, U)) \\ & = M \oplus H_2((g_1 \cdot g_2)^r) \oplus H_2(\hat{e}(D_{ID} + P_{ID,i}, U)) \\ & = M \oplus H_2((g_1 \cdot g_2)^r) \oplus H_2(g_1^r \cdot g_2^r) \\ & = M, \end{aligned}$$

Where the penultimate equality is due to the fact

$$\begin{aligned} & H_2(\hat{e}(D_{ID} + P_{ID,i}, U)) \\ & = H_2(\hat{e}(D_{ID}, U) \cdot \hat{e}(P_{ID,i}, U)) \\ & = H_2(\hat{e}(\alpha \cdot S_{ID}, r \cdot P) \cdot \hat{e}(\beta \cdot T_{ID,i}, r \cdot P)) \\ & = H_2(\hat{e}(S_{ID}, \alpha \cdot P)^r \cdot \hat{e}(T_{ID,i}, \beta \cdot P)^r) \\ & = H_2(\hat{e}(S_{ID}, P_{pub})^r \cdot \hat{e}(T_{ID,i}, C_{pub})^r) \\ & = H_2(g_1^r \cdot g_2^r). \end{aligned}$$

III. CONCLUSION

In this article, we proposed another revocable IBE plot with a cloud denial specialist (CRA), in which the repudiation technique is performed by the CRA to ease the heap of the PKG. This outsourcing calculation procedure with different experts has been utilized. revocable IBE conspire with KU-CSP. Be that as it may, their plan requires higher computational and communicational expenses than already proposed IBE plans. For the time key refresh method, the KU-CSP in Li et al's. conspire must keep a mystery esteem for every client with the goal that it is absence of adaptability. In our revocable IBE conspire with CRA, the CRA holds just an ace time key to play out the time key refresh techniques for every one of the clients without influencing security. As contrasted and Li et al's. plot, the exhibitions of calculation what's more, correspondence are altogether made strides. By trial results and execution investigation, our plan is appropriate for cell phones. For security investigation,

we have shown that our plan is semantically secure against versatile ID assaults under the decisional bilinear Diffie-Hellman supposition. At last, in view of the proposed revocable IBE plot with CRA, we built a CRAaided verification plot with period-restricted benefits for dealing with a substantial number of different cloud administrations.

IV. 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.

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

[10]. Gene Tsudik Dan Boneh, Xuhua Ding and Chi Ming Wong. A method for fast revocation of public key certificates and security capabilities. In The 10th USENIX Security Symposium, pages 297–308, 2001. [Gen03Craig Gentry. Certificate-based encryption and the certificate revocation problem. In Eli Biham, editor, EUROCRYPT, volume 2656 of Lecture Notes in Computer Science, pages 272–293. Springer, 2003.

[11]. Irene Gassko, Peter Gemmell, and Philip D. MacKenzie. Efficient and fresh cerification. In Public Key Cryptography, pages 342–353, 2000. [12Vipul Goyal. Certificate revocation lists or online mechanisms. In Eduardo Fern´andez-Medina, Julio C´esar Hern´andez Castro, and L. Javier Garc´ıa-Villalba, editors, WOSIS, pages 261–268. INSTICC Press, 2004.

[12]. M. Jakobsson. Fractal hash sequence representation and traversal, 2002. ISIT '02; available at http://eprint.iacr.org/2002/001 and www.markus-jakobsson.com.

[13]. Silvio Micali. Novomodo: Scalable certificate validation and simplified pki management. In 1st Annual PKI Research Workshop - Proceeding, 2002.

[14]. Patrick Drew McDaniel and Sugih Jamin. Windowed certificate revocation. In INFOCOM, pages 1406–1414, 2000.

[15]. Moni Naor and Kobbi Nissim. Certificate revocation and certificate update. In Proceedings 7th USENIX Security Symposium (San Antonio, Texas), Jan 1998.

[16]. William Aiello, Sachin Lodha, and Rafail Ostrovsky. Fast digital identity revocation (extended abstract). In CRYPTO, pages 137–152, 1998.

[17]. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, CRYPTO, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer, 2001.

[18]. Ahto Buldas, Peeter Laud, and Helger Lipmaa. Accountable certificate management using undeniable attestations. In ACM Conference on Computer and Communications Security, pages 9–17, 2000.

[19]. Don Coppersmith and Markus Jakobsson. Almost optimal hash sequence traversal. In Financial Cryptography, pages 102–119, 2002.