International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 7
March 2018

Identity-Based Cipher Text Conversion with Revocation Ability and Its Application in the Cloud Computing Environment

Narasimhulu K & Dr. Naimullah Khan
[1]Research scholar, Dept of CSE, Aligarh Muslim University
[2]Professor, Dept of CSE (R&D), Aligarh Muslim University

ABSTRACT: *Identity-based definitely encryption is a public key cryptosystem and eliminates the desires of public key infrastructure and certificate management in traditional public key settings. Due to the absence of PKI, the revocation trouble is a vital difficulty in IBE settings. Several revocable IBE schemes had been proposed concerning this issue. Quite lately, with the useful resource of embedding an outsourcing computation method into IBE, Li et al. Proposed a revocable IBE scheme with a key-update cloud company issuer. However, their scheme has shortcomings. One is that the computation and conversation costs are better than previous revocable IBE schemes. The extraordinary shortcoming is lack of scalability in the feel that the KU-CSP needs to hold a mystery fee for each person. In the thing, we recommend a cutting-edge revocable IBE scheme with a cloud revocation authority to remedy the two shortcomings, especially, the performance is significantly superior and the CRA holds simplest a device secret for all the customers. For safety evaluation, we display that the proposed scheme is semantically relaxed under the decisional bilinear Diffie-Hellman assumption. Finally, we make bigger the proposed revocable IBE scheme to provide a CRA-aided authentication scheme with period-restricted privileges for coping with a big type of various cloud offerings.*

Key Terms: Encryption, authentication, cloud computing, outsourcing computation, revocation authority.

INTRODUCTION

Identity-based totally public key machine is an attractive possibility for public key cryptography. ID-PKS putting receives rid of the demands of public key infrastructure (PKI) and certificate management in traditional public key settings. An ID-PKS putting consists of customers and a relied on zero.33 party. The PKG is responsible to generate each consumer's personal key with

the aid of the usage of the related ID information. Therefore, no certificate and PKI are required inside the associated cryptographic mechanisms under ID-PKS settings. In such a case, ID-based encryption lets in a sender to encrypt message without delay through the use of a receiver's ID without checking the validation of public key certificate. Accordingly, the receiver uses the private key related to her/his ID to decrypt such cipher textual content. Since a public key setting has to provide a client revocation mechanism, the studies trouble on how to revoke misbehaving or compromised users in an ID-PKS placing is naturally raised. In conventional public key settings, certificate revocation listing is a famous revocation approach. In the CRL technique, if a party gets a public key and its related certificate, she/he first validates them and then appears up the CRL to make certain that the general public key has now not been revoked. In this kind of case, the procedure calls for the internet assistance beneath PKI a terrific way to incur verbal exchange bottleneck. To enhance the overall performance, numerous efficient revocation mechanisms for classic public key settings were nicely studied for PKI. Indeed, researchers also are aware about the revocation trouble of ID-PKS settings. Several revocable IBE schemes have been proposed concerning the revocation mechanisms in ID-PKS settings.

I. LITERATURE WORK

In 2001, Boneh and Franklin proposed the first practical IBE scheme from the Weil pairing and cautioned an easy revocation method wherein each non-revoked consumer receives a contemporary private key generated via way of the PKG periodically. A length may be set as a day, per week, a month, and so forth. A sender uses a chosen receiver's ID and present day length to encrypt messages at the same time as the right receiver decrypts the cipher text the usage of the current personal key. Hence, it is important for the users to replace new personal keys periodically. To revoke a patron, the PKG honestly stops imparting the ultra-modern non-public key for the user. It is obvious that a comfortable channel need to be established between the PKG and each patron to transmit the new private key and this would bring about heavy load for the PKG. In order to relieve the load of the PKG in Boneh and Franklin's scheme, Boneh et al proposed each other revocation method, referred to as without delay

revocation. Immediate revocation technique employs a chosen semi-depended on and on-line authority (i.e. Mediator) to mitigate the control load of the PKG and assist clients to decrypt cipher text. In this kind of case, the internet mediator should keep stocks of all the customers' personal keys. Since the decryption operation should contain every activity, neither the person nor the net mediator can cheat each other. When a person changed into revoked, the online mediator is cautioned to stop supporting the client. However, the internet mediator has to help clients to decrypt each cipher text just so it will become a bottleneck for such schemes as the wide variety of users grows exceptionally. On the alternative hand, in Boneh and Franklin's revocation technique, all of the clients want to periodically replace new personal keys dispatched by means of the PKG. As the wide variety of users will boom, the weight of key updates becomes a bottleneck for the PKG. In 2008, Boldyreva et al proposed a revocable IBE scheme to enhance the vital element update efficiency. Their revocable IBE scheme is primarily based on the idea of the Fuzzy IBE and adopts the entire subtree approach to lower the huge kind of key updates from linear to logarithmic within the sort of customers. Indeed, by binary tree statistics shape of clients, the scheme efficiently alleviates the critical component-replace load of the PKG. Furthermore, Libert and Vergnaud superior the protection of Boldyreva et al.'s revocable IBE scheme thru providing an adaptive-ID comfy scheme. Nevertheless, Boldyreva et al.'s scheme nonetheless outcomes in numerous troubles: Each person's private key length is 3log n points in an elliptic curve, in which n is the variety of leaf nodes inside the binary tree. The scheme additionally consequences in massive computation workload for encryption and decryption strategies. It is large load for PKG to maintain the binary tree with a big quantity of customers.

II. TECHNIQUES IMPLEMENTED

Moreover, Seo and Emura refined the safety model of Boldyreva et al.'s revocable IBE scheme thru considering a cutting-edge risk, called decryption key exposure attacks. Based at the concept of Libert and Vergnaud's scheme further they proposed a revocable IBE scheme with decryption key exposure resistance. In order to reduce the sizes of every non-public keys and update keys, Park et al proposed a brand new

revocable IBE scheme with the resource of the use of multilinear maps, but the duration of the majority parameters depends to the kind of customers. For achieving constant the dimensions of most of the people parameters, Wang et al employed every the dual machine encryption approach and the whole sub tree technique to indicate a modern revocable IBE scheme. Furthermore, Seo and Emura extended the concept of revocable IBE scheme to recommend the first revocable HIBE scheme. In Seo and Emura's scheme, for every period, every client generates a secret key via multiplying some of the partial keys, which relies upon at the partial keys utilized by ancestors inside the hierarchy tree. In this form of case, the call of the sport key duration of each client will increase quadratically within the hierarchy tree in which a low-stage consumer need to recognize the statistics of key updates finished by way of using ancestors within the modern-day term, and it renders the scheme very complex. In 2015, Seo and Emura proposed a modern day method to assemble a completely unique revocable HIBE scheme with statistics-free updates. Nevertheless, the said revocable IBE and HIBE schemes above employed the complete subtree technique to decrease the amount of key updates from linear to logarithmic in the range of customers. However, the ones schemes also suffered from the same risks of Boldyreva et al.'s revocable IBE scheme and despite the fact that used a relaxed channel to transmit periodic private keys.

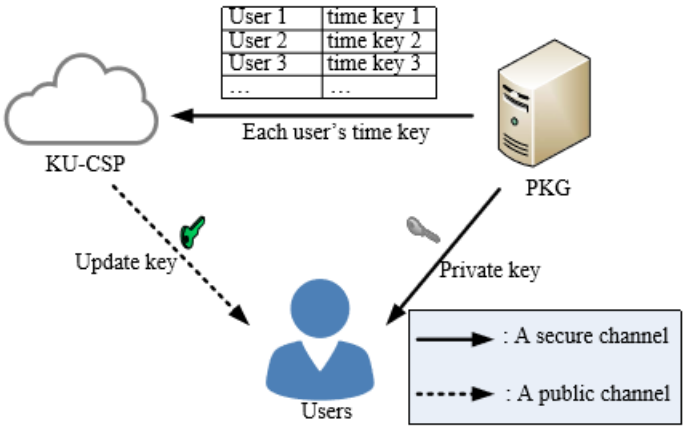

Fig: 1 System Model

III. PROPOSED TECHNOLOGY

System model for revocable IBE scheme with CRA: In this text, we first present the framework of our revocable IBE scheme with CRA and define its protection notions to version feasible threats and attacks. Accordingly, a new revocable IBE scheme with CRA is proposed. As the adversary model provided in [6] it includes adversaries,

particularly, an inner adversary and an outside adversary. For protection assessment, we formally display that our scheme is semantically comfy in the direction of adaptive-ID and selected-cipher textual content attacks (CCA) inside the random oracle version below the bilinear preference Diffie-Hellman hassle. Finally, based totally on the proposed revocable IBE scheme with CRA, we construct a CRA-aided authentication scheme with period-limited privileges for managing a massive extensive form of diverse cloud services.

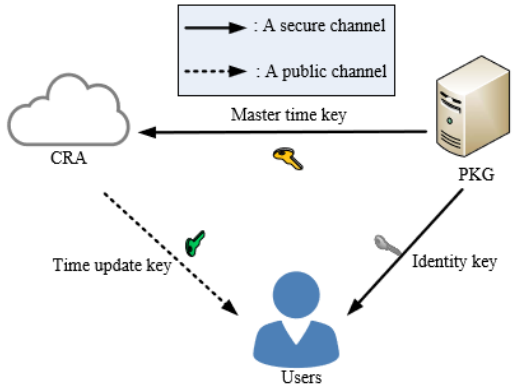

FIG: 2 System model for revocable IBE scheme with CRA

To display the deserves of our scheme,Table1lists the comparisons amongst sub tree-based totally IBE schemes HIBE schemes Tseng-Tsai scheme Li et al.'s scheme and ours in phrases of the use of key update channel, the size of every person's private key, key replace load, outsourced computation of authority, the workload of the PKG and scalability of authority. Those subtree-primarily based IBE schemes and HIBE schemes hired the whole subtree approach to lower the quantity of key updates from linear to logarithmic inside the variety of customers. However, each consumer's private key length is O (logn), where n is the amount of clients. These schemes still used a comfortable channel to transmit periodic private keys on the equal time as no one-of-a-kind authority stocks the obligation of customer revocation. In Tseng and Tsai's revocable IBE scheme each the identity key and time replace key are issued through the PKG. In order to relieve the load of the PKG, Li et al employed a key update cloud issuer to proportion the responsibility of client revocation. In our revocable IBE scheme, we hire a cloud revocation authority to perform consumer revocation. Indeed, the PKG in Li et al.'s scheme and ours can also moreover perform the revocation operations. Both the KUCSP and the CRA are specific to percent duty for acting individual

revocation. For scalability, the KU-CSP in Li et al.'s scheme have to preserve n diverse time keys for n users simply so it does no longer own scalability and incurs the manipulate load. On the evaluation, the CRA in our scheme holds simplest one master time key for all of the customers. When the range n of customers inside the machine can be very massive, the PKG can also additionally designate more than one CRA to percentage the obligation of character revocation even as every CRA holds most effective the equal grasp time key. However, in Li et al.'s scheme, every KUCSP need to additionally preserve n time keys. Indeed, cloud computing is a ubiquitous computing surroundings so that setting multiple CRAs on clouds might also additionally offer handy control of patron revocation whilst decreasing the burden of the unmarried PKG. The specific comparisons concerning computation and communiqué efficiency may be given in similarly sections.

Framework: In this section, we present the syntax of revocable IBE schemes with CRA. A revocable IBE scheme with CRA consists of five algorithms: system setup, identity key extract, time key update, encryption and decryption. • System setup is a probabilistic algorithm that is run by the PKG. The PKG takes as input two parameters, namely, a secure parameter λ and the total number z of periods, and outputs public parameters PP, a obtain a mater secret key α, a mater time key β and public parameters PP. It forwards PP to the adversary AI while α and β are kept secret by B. The adversary AI is allowed to issue the following queries in an adaptive manner. Identity key extract query (ID). When AI issues such a request along with a user's identity ID ∈ {0, 1} ∗, B runs the Identity key extract algorithm to generate the identity key DID and sends it to AI. – Time key update query (ID, I). When AI issues such a request along with a user's identity ID ∈ {0,1}∗ and a period I, B runs the Time key update algorithm to generate the time update key PID, I and responds with it. – Decryption query (C, ID, I). Upon receiving the query along with a cipher text C, a user's identity ID ∈{0,1}∗ and a period I, B obtains the private key pair by issuing the Identity key extract query with ID and the Time key update query with (ID, I). The challenger B runs the Decryption algorithm to decrypt the cipher text C and returns the corresponding plaintext M to AI.

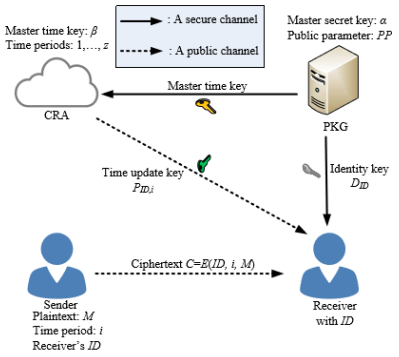

Fig: 3 System Operations of Revocable IBE Scheme with CRA

CRA-aided authentication scheme with period limited privileges: An authentication scheme is a cryptographic mechanism to authenticate customers over public networks. Before a client profits get entry to a server's offerings, the person ought to be authenticated and authorized through the server. Here, we growth our revocable IBE scheme to construct a cloud-revocation authority aided authentication scheme with period restrained privileges for handling a huge quantity of numerous cloud services. When a enterprise (or agency) constructs severa diverse cloud services, the way to efficiently manipulate the authorizations for the ones cloud services is an essential hassle because of the reality a user want to authenticate herself/himself to a cloud provider server before getting access to the cloud services. In the device with multiple cloud offerings, more than one CRAs replace the placement of the CRA in our proposed scheme. The draw near time key is modified with a couple of draw near privilege keys. A CRA with a master privilege key can manage the corresponding privilege to have get entry to a few company servers at numerous intervals. A CRA is capable of use its grasp privilege key to generate and deliver a duration-confined privilege key to a purchaser. A customer with every the associated identity key and a length-restricted privilege key's able to get right of entry to the corresponding server. Indeed, a CRA can also moreover manage single or more than one organization servers. Without loss of generality, we expect that there are k impartial CRAs which are responsible for handling k impartial carrier servers, respectively.

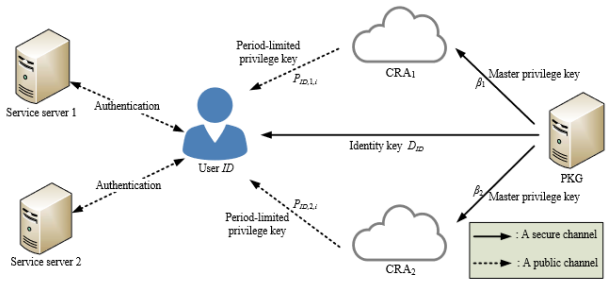

Fig: 4 Example of system model for managing multiple cloud services

IV. CONCLUSION

In this text, we proposed a modern-day revocable IBE scheme with a cloud revocation authority, wherein the revocation method is achieved with the useful resource of the CRA to relieve the load of the PKG. This outsourcing computation technique with distinctive government has been hired in Li et al.'s revocable IBE scheme with KU-CSP. However, their scheme calls for better computational and communicational fees than previously proposed IBE schemes. For the time key update method, the KU-CSP in Li et al.'s scheme want to preserve a mystery value for absolutely everyone just so its miles lack of scalability. In our revocable IBE scheme with CRA, the CRA holds quality a master time key to carry out the time key replace techniques for all of the customers without affecting protection. As compared with Li et al.'s scheme, the performances of computation and conversation are significantly advanced. By experimental outcomes and performance evaluation, our scheme is nicely right for cell devices. For protection evaluation, we have confirmed that our scheme is semantically relaxed in opposition to adaptive-ID assaults below the decisional bilinear Diffie-Hellman assumption. Finally, based at the proposed revocable IBE scheme with CRA, we constructed a CRA aided authentication scheme with period-limited privileges for dealing with a big wide variety of various cloud offerings.

V. REFERENCES

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

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

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

[4]. B. Libert and J. J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," Proc. PODC2003, pp. 163-171, 2003.

[5]. J.Baek and Y. Zheng, "Identity-based threshold decryption," Proc. PKC'04, LNCS, vol. 2947, pp. 262-276, 2004.

[6]. H.-S. Ju, D.-Y. Kim, D.-H. Lee, H. Park, and K. Chun, "Modified ID-based threshold decryption and its application to mediated ID based encryption," Proc.APWeb2006,LNCS, vol.3841, pp. 720-725, 2006.

[7]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," Proc. CCS'08, pp. 417-426, 2008.

[8]. A Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. Eurocrypt'05, LNCS, vol. 3494, pp. 557-557, 2005.

[9]. Libert and D. Vergnaud, "Adaptive-ID secure revocable identity-based encryption," Proc. CT-RSA'09, LNCS, vol. 5473, pp. 1-15, 2009.

[10]. J.-H. Seo and K. Emura, "Revocable identity-based encryption revisited: security model and construction," Proc. PKC'13, LNCS, vol. 7778, pp. 216-234, 2013.

[11]. S. Park, K. Lee, and D.H. Lee, "New constructions of revocable identity-based encryption from multilinear maps," IEEE Transactions on Information Forensics and Security, vol.10 , no. 8, pp. 1564 - 1577, 2015.

[12]. Wang, Y. Li, X. Xia, and K. Zheng, "An efficient and provable secure revocable identity-based encryption scheme," PLoS ONE, vol. 9, no. 9, article: e106925, 2014.

[13]. Lewko A and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," Proc. TCC'10, LNCS, vol. 5978, pp. 455-479, 2010.

[14]. J.-H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," Proc. CT-RSA'13, LNCS, vol. 7779, pp. 343-358, 2013.