International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Securing Cloud Data using Identity-Based Encryption Scheme under Key Exposure

Y Supriya, M.Tech
PG Scholar, SVCET (A), Chittoor, India
G.B.Hima Bindu, M.Tech., (Ph.D)
Associate Professor, Department of IT, SVCET(A), Chittoor, India
K. Dasaradharami Reddy, M.Tech.,
Assistant Professor, Department of CSE, SVCET(A), Chittoor, India

ABSTRACT

Cloud 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 negligible administration exertion, regularly finished in the Internet. Distributed computing depends on sharing of assets to accomplish intelligibility and economies of scale, like an open utility. In existing framework, a novel and productive plan that ensures information classification regardless of whether the encryption key is spilled and the foe approaches all figure content squares. We dissect the security of Bastion, and we assess its execution by methods for a model usage. We likewise talk about functional experiences as for the reconciliation of Bastion in business scattered capacity frameworks. In this paper, we are going to discuss how to handle the basic issue of personality denial, we bring outsourcing calculation into IBE out of the blue and propose a revocable IBE conspire in the server-helped setting. Our plan offloads the vast majority of the key age related tasks amid key-issuing and key-refresh procedures to a Key Update Cloud Service Provider, leaving just a steady number of basic activities for PKG and clients to perform locally. This objective is accomplished by using a novel arrangement safe method: we utilize a half breed private key for every client, in which an AND entryway is included to associate and bound the character segment and the time segment.

Keywords: Cloud Computing, IBE Scheme, Encryption

I. INTRODUCTION

Distributed computing is a technique for conveying data innovation (IT) benefits in which assets are recovered from the Internet through online instruments and applications, rather than an immediate association with a server. Instead of keeping records on a restrictive hard drive or neighborhood stockpiling gadget, cloud-based capacity makes it conceivable to spare them to a remote database. For whatever length of time that an electronic gadget approaches the web, it approaches the information and the product projects to run it. It's called distributed computing in light of the fact that the data being found in the cloud and does not require a client to be in a particular place to access it. This kind of framework enables representatives to work remotely. Organizations giving cloud administrations empower clients to store documents and applications on remote servers, and afterwards every one can retrieve the information by means of the web.

Character Based Encryption (IBE) is an intriguing contrasting option to open key encryption, which is proposed to rearrange enter administration in an authentication based Public Key Infrastructure (PKI) by utilizing human comprehensible personalities (e.g., one of a kind name, email address, IP address, and so forth) as open keys. Along these lines, sender utilizing IBE does not have to look into open key and declaration [1-5], however specifically scrambles message with recipient's character. Likewise, beneficiary getting the private key related with the comparing personality from Private Key Generator (PKG) can unscramble such figure content. Despite the fact that IBE permits a subjective string as people in general key which is considered as engaging focal points over PKI, it requests a proficient disavowal system. In particular, if the private keys of a few clients get traded off, we should give an intend to disavow such clients from framework. In PKI setting, repudiation instrument is acknowledged by affixing legitimacy periods to authentications or utilizing included blends of methods. By the by, the awkward administration of declarations is accurately the weight that IBE endeavors to mitigate [10].

In this paper, we bring outsourcing calculation into IBE denial, and formalize the security meaning of outsourced revocable IBE out of the blue to the best of our insight. We propose a plan to offload all the key age related tasks amid key-issuing and key-refresh, leaving just a consistent number of straightforward activities for PKG and qualified clients to perform locally [6,7]. In our plan, as with the recommendation in, we understand repudiation through refreshing the private keys of the unrevoked clients. Be that as it may, not at all like that work which inconsequentially links era with personality for key age/refresh and requires to re-issue the entire private key for unrevoked clients, we propose a novel plot safe key issuing method: we utilize a half and half private key for every client [4], in which an AND door is included to associate and bound two sub-parts, in particular the character segment and the time segment. At to begin with, client can get the character part and a default time segment (i.e., for current day and age) from PKG as his/her private key in key-issuing. A while later, with a specific end goal to look after decrypt ability, unrevoked clients needs to intermittently ask for on key-refresh for time segment to a recently presented element named Key Update Cloud Service Provider (KU-CSP) [15-16]. Besides, we consider to acknowledge revocable IBE with a semi honest KU-CSP. To accomplish this objective, we exhibit a security improved development under the as of late formalized Refereed Delegation of Computation (RDoC) display [9]. At last, we give broad trial results to exhibit the effectiveness of our proposed development.

II. RELATED WORK

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

Privacy preserving personal health record using multi-authority attribute-based encryption with revocation

Personal health record (PHR) service is an emerging model for health information exchange. In PHR systems, patient's health records and information are maintained by the patient himself through the Web. In reality, PHRs are often outsourced to be stored at the third parties like cloud service providers. However, there have been serious privacy concerns about cloud service as it may expose user's sensitive data like PHRs to those cloud service providers or

unauthorized users. Using attribute-based encryption (ABE) to encrypt patient's PHRs in cloud environment, secure and flexible access control can be achieved. Yet, problems like scalability in key management, fine-grained access control, and efficient user revocation remain to be addressed. In this paper, we propose a privacy-preserving PHR, which supports fine-grained access control and efficient revocation. To be specific, our scheme achieves the goals (1) scalable and fine-grained access control for PHRs by using multi-authority ABE scheme, and (2) efficient on-demand user/attribute revocation and dynamic policy update. In our scheme, we consider the situation that multiple data owners exist, and patient's PHRs are encrypted and stored in semi-trust servers. The access structure in our scheme is expressive access tree structure, and the security of our scheme can be reduced to the standard decisional bilinear Diffie–Hellman assumption.

Searchable cipher text-policy attribute based encryption with revocation in cloud storage

To protect the sensitive data outsourced to cloud server, outsourcing data in an encrypted way has become popular nowadays. However, it is not easy to find the corresponding cipher text efficiently, especially the large cipher text stored on cloud server. Besides, some data owners do not want those users who attempt to decrypt to know the sensitive access structure of the cipher text because of some business or private reasons. In addition, the user attributes revocation and key updating are important issues, which affect application of cipher text-policy attribute-based encryption (CP-ABE) in cloud storage systems. To overcome the previous problems in cloud storage, we present a searchable CP-ABE with attribute revocation, where access structures are partially hidden so that receivers cannot extract sensitive information from the cipher text. The security of our scheme can be reduced to the decisional bilinear Diffie–Hellman (DBDH) assumption and decisional linear (DL) assumption.

Identity-based encryption with outsourced revocation in cloud computing

Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption [5]. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Revocable hierarchical identity-based encryption: history-free update, security against insiders, and short Cipher texts

In the context of Identity-Based Encryption (IBE), both revocation and delegation of key generation are important functionalities. Although a number of IBE schemes with *either* efficient revocation *or* efficient delegation of key generation functionality has been proposed, an important open problem is efficiently delegating both the key generation and revocation functionalities in IBE systems. Seo and Emura (CT-

RSA 2013) proposed the first realization of Revocable Hierarchical IBE (RHIBE), a sole IBE scheme that achieves both functionalities simultaneously. However, their approach implements history-preserving updates, wherein a low-level user must know the history of key updates performed by ancestors in the current time period, and it renders the scheme very complex.

In this paper, we present a new method to construct RHIBE that implements history-free updates. Our history-free approach renders the scheme simple and efficient. As a second contribution, we redefine the security model for RHIBE to ensure security against *insiders*, where adversaries are allowed to obtain all internal system information, e,g., state information. In addition, we also consider the decryption key exposure attack, which was considered by Seo and Emura (PKC 2013).

Further, we propose two RHIBE schemes with shorter secret keys and constant size cipher texts that implement the aforementioned history-free updates approach and security model. For revocation, our constructions use the Complete Sub tree (CS) method and the Subset Difference (SD) method. Both schemes are selectively secure in the standard model under the qq-weak Bilinear Diffie-Hellman Inversion (qq-wBDHI) assumption.

New constructions of revocable identity-based encryption from multi linear maps

A revocable identity-based encryption (RIBE) provides an efficient revocation method in IBE that a trusted authority periodically broadcasts an update key for non revoked users and a user can decrypt a cipher text if he is not revoked in the update key. Boldyreva, Goyal, and Kumar (CCS 2008) defined RIBE and proposed an RIBE scheme that uses a tree-based revocation encryption scheme to revoke users' private keys. In this paper, we devise a new technique for RIBE and propose RIBE schemes with a constant number of private key elements. We achieve the following results. We first devise a new technique for RIBE that combines a hierarchical IBE (HIBE) scheme and a public-key broadcast encryption (PKBE) scheme using multi linear maps. In contrast to the previous technique for RIBE, our technique uses a PKBE scheme in bilinear maps for revocation to achieve short private keys and update keys. Following our new technique for RIBE, we propose an RIBE scheme in three-leveled multi linear maps that combines the HIBE scheme of Boneh and Boyen (EUROCRYPT 2004) and the PKBE scheme of Boneh, Gentry, and Waters (CRYPTO 2005). The private key and update key of our scheme possess a constant number of group elements. Next, we propose another RIBE scheme with reduced public parameters and short keys by combining the HIBE scheme of Boneh and Boyen and the PKBE scheme of Boneh, Waters, and Zhandry (CRYPTO 2014), which uses multi linear maps. Compared with our first RIBE scheme, our second RIBE scheme requires high-leveled multi linear maps.

Algorithm:

REVOCABLE IBE SCHEME WITH CRA

Here, we propose an effective revocable IBE plot with CRA. The plan is built by utilizing bilinear pairings (Segment 2).

• System setup: A trusted PKG takes as information two parameters, in particular, a protected parameter λ and the aggregate number z of periods. The PKG haphazardly picks two cyclic gatherings G and GT of a prime request $q > 2^{\lambda}$.

Additionally, it haphazardly picks a generator P of G, an allowable bilinear guide $e\hat{} : G \times G \rightarrow GT$ and two mystery values $\alpha, \beta \in Z * q$. The esteem α is the ace mystery key used to figure the framework open key $Ppub = \alpha \cdot P$. The PKG at that point transmits the ace time key β to the CRA by means of a safe channel. The esteem β is utilized to process the cloud open key $Cpub = \beta \cdot P$. The PKG chooses three hash capacities $H0, H1 : \{0, 1\} * \rightarrow G$, $H2 : GT \rightarrow \{0, 1\} l$, and $H3 : \{0, 1\} * \rightarrow \{0, 1\} l$, where l is settled, and distributes people in general parameters P =< q, G,

GT , e, P, P ˆ bar, Cpub, H0, H1, H2, H3 >. Character key concentrate: Upon getting the personality ID ∈ {0, 1} of a client, the PKG utilizes the ace mystery key α to register the relating character key DID = α · SID, where SID = H0(ID). At that point, the PKG sends the personality key DID to the client by means of a safe channel.

• Time key refresh: To create the time refresh key PID,i at period I for a client with character ID ∈ {0, 1}, the CRA utilizes the ace time key β to figure the time refresh key PID,i = β·TID,i, where TID,i = H1(ID, I). At long last, the CRA sends the time refresh key PID,i to the client by means of an open channel.

• Encryption: To scramble a message M ∈ {0, 1} l with a recipient's personality ID and a period I, a sender chooses an irregular esteem r ∈ Z

∗ q furthermore, registers U = r ·P. The sender likewise registers V = M ⊕H2((g1 · g2) r), where g1 = ˆe(SID, Ppub) and g2 = ˆe(TID,i, Cpub). At that point, the sender registers W = H3(U, V, M, ID, I). At long last, the sender sets the cipher text as C = (U, V, W) and sends it to the recipient. Unscrambling: To decode a cipher text C = (U, V, W) with a recipient's character ID and a period I, the collector utilizes his/her personality key DID and time refresh key PID,i to register the plaintext

M = V ⊕ H2(ˆe(DID + PID,i, U)). On the off chance that W = H3(U, V, M, ID, I), return M as the plain text output, else return ⊥The correctness of the decryption algorithm follows since

$V \oplus H_2(\hat{e}(D_{ID} + P_{ID,i}, U))$

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

$= M \oplus H_2((g_1 \cdot g_2)^r) \oplus H_2(g_1^r \cdot g_2^r)$

$= M,$

$H_2(\hat{e}(D_{ID} + P_{ID,i}, U))$

$= H_2(\hat{e}(D_{ID}, U) \cdot \hat{e}(P_{ID,i}, U))$

$= H_2(\hat{e}(\alpha \cdot S_{ID}, r \cdot P) \cdot \hat{e}(\beta \cdot T_{ID,i}, r \cdot P))$

$= H_2(\hat{e}(S_{ID,\alpha} \cdot P)^r \cdot \hat{e}(T_{ID,i,\beta} \cdot P)^r)$

$= H_2(\hat{e}(S_{ID}, P_{pub})^r \cdot \hat{e}(T_{ID,i}, C_{pub})^r)$

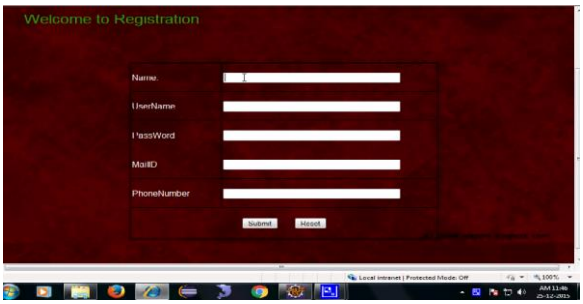
$= H_2(g_1^r \cdot g_2^r).$

Note that the proposed scheme above will be proved to be an IND-ID-CCA-secure IBE scheme in the next section. Indeed, a simple IND-ID-CPA-secure IBE scheme is obtained by removing W from C = (U, V, W) in the proposed scheme, namely, the cipher text only consists of C = (U, V).

III. RESULTS

Home page

User can register with the credentials like user name, password, mail id, phone no etc as shown in below.



Admin can login with credentials like user name, password is as shown in below.

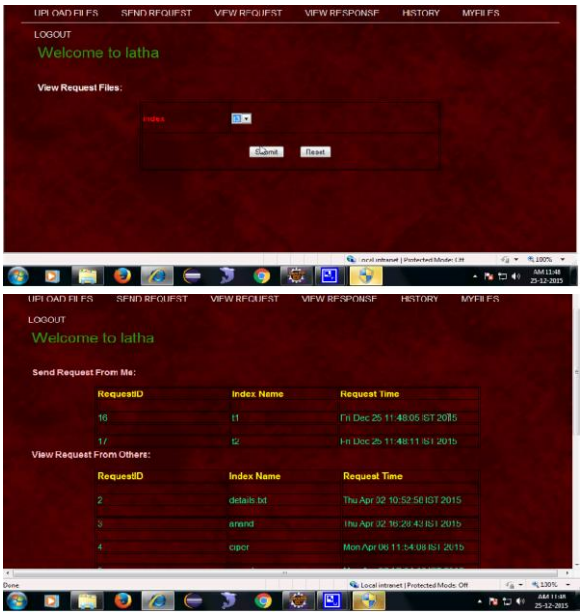
Admin can view user details as shown below.

Admin can give response to user

User can upload files is as shown in below

User can send request files to admin is as shown in below

User can send request files to admin those files are seen shown below



Admin can give the response to user, user can view that response is as shown below

IV. CONCLUSION

In this paper, concentrating on the basic issue of character disavowal, we bring outsourcing calculation into IBE and propose a revocable plan in which the repudiation activities are appointed to CSP. With the guide of KU-CSP, the proposed conspire is full-highlighted: 1) It accomplishes steady productivity for both calculation at PKG and private key size at client; 2) User needs not to contact with PKG amid key-refresh, as it were, PKG is permitted to be disconnected subsequent to sending the denial rundown to KU-CSP; 3) No protected channel or client verification is required amid key-refresh amongst client and KU-CSP. Moreover, we consider acknowledging revocable IBE under a more grounded enemy show. We show a propelled development also, indicate it is secure under RDoC display, in which no less than one of the KU-CSPs is thought to be straightforward. Hence, regardless of whether a denied client and both of the KU-CSPs conspire, it can't enable such client re-to get his/her decryptability.

V. REFERENCES

1. W Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology - CRYPTO-98. Springer, 1998.
2. V Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247-259.

3. F Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375-388.
4. D Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology - CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213-229.
5. A Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS -08. New York, NY, USA: ACM, 2008, pp. 417-426.
6. A Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557-557.
7. R Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," Cryptology ePrint Archive, Report 2011/518, 2011.
8. U Feige and J. Kilian, "Making games short (extended abstract)," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC -97. New York, NY, USA: ACM, 1997, pp. 506-516.
9. S Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proceedings of the Second international conference on Theory of Cryptography, ser. TCC-05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264-282.
10. R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 2012, vol. 7412, pp. 37-61.
11. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in 17th European Symposium on Research in Computer Security (ESORICS), 2012.
12. M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS -10. New York, NY, USA: ACM, 2010, pp. 48-59.
13. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology - CRYPTO, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin / Heidelberg, 1985, vol. 196, pp. 47-53.
14. C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, ser. Lecture Notes in Computer Science, B. Honary, Ed. Springer Berlin / Heidelberg, 2001, vol. 2260, pp. 360-363.
15. R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology EUROCRYPT 2003, ser. Lecture Notes in Computer Science, E. Biham, Ed. Springer Berlin / Heidelberg, 2003, vol. 2656, pp. 646-646.
16. D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2004, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds. Springer Berlin / Heidelberg, 2004, vol. 3027, pp. 223-238.
17. "Secure identity based encryption without random oracles," in Advances in Cryptology - CRYPTO 2004, ser. Lecture Notes in Computer

Science, M. Franklin, Ed. Springer Berlin / Heidelberg, 2004, vol. 3152, pp. 197-206.

18. B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 114-127.
19. C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2006, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed. Springer Berlin / Heidelberg, 2006, vol. 4004, pp. 445-464.
20. C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proceedings of the 40th annual ACM symposium on Theory of computing, ser. STOC -08. New York, NY, USA: ACM, 2008, pp. 197-206.