A Novel Identity-Based Encryption using Outsourced Revocation in Cloud Computing

Meenakshi.S[#1], Radhika.B.R[#2], Sripriya.B.S[#3], Tejashwini[#4], Nandini.G[#5]
[1,2,3,4] UG SCHALOR, [5] Assistant Professor, Department Of Computer Science And Engineering,
RAJARAJESWARI COLLEGE OF ENGINEERING, BENGALURU-560074, KARNATAKA, INDIA
meenakshi.yadava94@gmail.com, radhikabr1994@gmail.com, sripriyabs5@gmail.com, tejashwinitejunaik@gmail.com,
nanduamma@gmail.com

Abstract-Public key and certificate management is simplified using Identity-Based Encryption (IBE). Other way to public key encryption is provided by Certificate management at Public Key Infrastructure (PKI). During user revocation the overhead computation occurs at Private Key Generator (PKG) which is the major drawback of IBE. In this project, aiming at tackling the major problem of identity revocation is done for first time by introducing outsourcing computation and propose a revocable IBE scheme in the server-aided setting. During key-issuing and key-updation processes to a Key Update Cloud Service Provider, provides a constant number of simple operations for PKG and users to perform locally. Therefore, this scheme unloads most of the related operations for key generation during issuing and updation of keys. This is achieved by utilizing a novel collusion-resistant technique. Finally, extensive experimental results to demonstrate the efficiency of proposed construction are provided.

Key Terms-Identity based encryption (IBE), revocation, outsourcing, cloud computing.

1 INTRODUCTION

Identity Based Encryption (IBE) is an alternative to public key encryption. Public keys used here are unique name, email address, IP address, etc., Messages are encrypted with client‘s identity when server uses IBE. Similarly, client receive private key which is equivalent to the identity from Private Key Generator(PKG) to decrypt such cipher text. Any random string can be used as public key in IBE which is a superior advantage over PKI. If some users private key become objectionable then a means to revoke such users from system should be provided. [1]Boneh and Franklin‘s mechanism would result in an overhead load at PKG (Private Key Generator). Hindering management of certificates is precisely the burden that IBE strives to ease. Boneh and Franklin said that users should update their private keys constantly and senders should use clients‘ identities combined with present time period. Decriptability can be maintained only if active users update their key in regular manner. Liabilities of named Key Update Cloud Service Provider (KU-CSP) can be overcome in our scheme there is no need of re-issuing the entire private keys instead keys need to be updated constantly.

2 RELATED WORKS

[2]Adel Binbusayyis* and Ning Zhang had proposed Decentralized Attribute Based Encryption Schemes. Existing works toward decentralized ABE can be classified into two categories depending on how the attribute authorities are structured: multi-authority ABE and hierarchical ABE. In the setting of multi-authority ABE, several attribute authorities cooperate to manage the attributes in a system. Each attribute authority is given a unique set of attributes. A user may need to ask more than one authority in order to obtain his/her attributes.

One of the security challenges is how to resist the collusion attack of malicious users. The Chase work achieves collusion resistance by introducing a Global Identifier (GID) given to each user secret key. All the users‘ secret key components from different authorities will be tied to his GID. However, to make the cipher text be independent of the users GID, a central authority must be used to issue a special secret key for the user using his secret key and the other authorities‘ secret keys.

[8]Chase and Chow proposed an enhanced multi-authority ABE scheme. They managed to remove the central authority,

but they require that each authority has to assign at least one attribute to each user. This would result a heavy communication cost and a lack of scalability in large scale systems.

[3]Lekwo and Waters proposed a multiauthority ABE scheme that does not require either central authority or cooperation between the multiple authorities. They use a hash function on the user global ID to manage collusion resistance and tie users secret key components together. However, this scheme is not suitable enough to be applied on our scenario because each authority has to know all users GID in advance. In addition, they do not consider how to reduce the workload on an attribute authority when it needs to handle large number of users in large scale system.

[6]Wan et. al. proposed a hierarchical attribute-set-based encryption (HASBE) scheme. Similar to our CP-DABE scheme, their scheme requires a user only to communicate with his/her administering attribute authority, rather than with more than one attribute authority as the case in. However, the HASBE scheme has two drawbacks compared with our CP-DABE scheme. The first one is that our CP-DABE algorithms are faster than the HASBE algorithms in terms of the computational cost. In the decryption algorithm, as an example, in the HASBE scheme, the decryption requires two pairing operations for every leaf node used to satisfy the tree, one pairing for each translating node on the path from the leaf node used to the root, and one exponentiation for each node on the path from the leaf node to the root. However, in our CP-DABE scheme, the decryption algorithm requires only one pairing map for each attribute used to satisfy the access structure. The second drawback is that the HASBE scheme is only proven secure in the generic security model, while our CP-DABE scheme is formally proved against chosen-plaintext attacks under the decisional Bilinear Diffie-Hellman Exponent assumption.

[12]Qingwei Zhang, Mohammed Almulla proposed Revocation Schemes. User revocation is the act of removing privileges from a user so that the user can no longer access the data files. To revoke a user, the data owner needs to update all the attributes keys (i.e. attribute-public keys and attribute-master keys) that have been used to derive the revoked users keys (i.e. user-attribute secret keys). As a consequence of updating the attributes keys, the data owner also needs to update all other affected users keys (i.e. user-attribute secret keys) and re-encrypt each data that have been associated from with any of these revoked attributes.

[13]Pervez, Z. et. al. suggested creating a new access policy with each data file, which contains all the authorized users IDs. To revoke a user, the data owner will only need to remove the revoked users ID from the access policy. This is a straightforward solution, but not practical for large systems since the data owner will need to know the all the users‘ IDs a priori. To tackle this problem, an expiration time based revocation technique is proposed, which associates an attribute called expiration-time to each user secret key.

3 METHODOLOGY

Implement a portal accessible for two types of users:

- Client
- Server

Clients will be able to look up for the available servers and send a request for adding them to their servers list.

Server will be able to identify the client and either approve/reject the clients ADD request.

Client will use server‘s public key (IBE) for encryption and sends a message to the server.

Server will be decrypting all clients‘ message using its private key.

Server will be maintaining a flag called time-to-live for each public key it is going to expose. Once the time-to-live approaches, the KG will auto-revoke all the clients.

Encryption, key generation and user revocation will be handled in a decentralized manner.

4 DESIGN

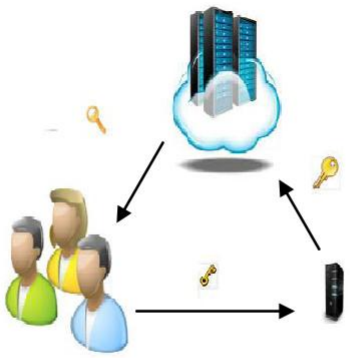


Fig1: Design model for Identity Based Encryption with single KU-CSP

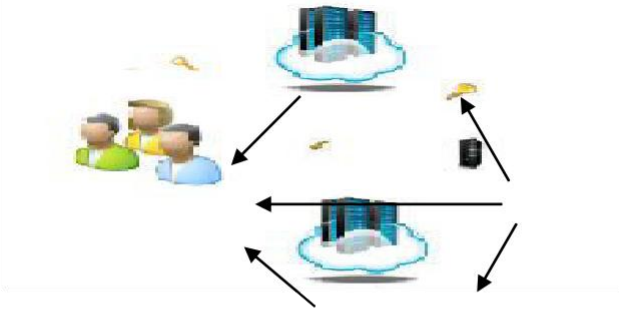


Fig2: Design model for IBE with two KU-CSPs

5 IMPLEMENTATION

Fig1: Front View

Fig2: Login and Register Page

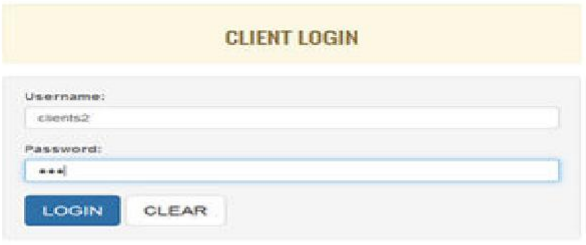
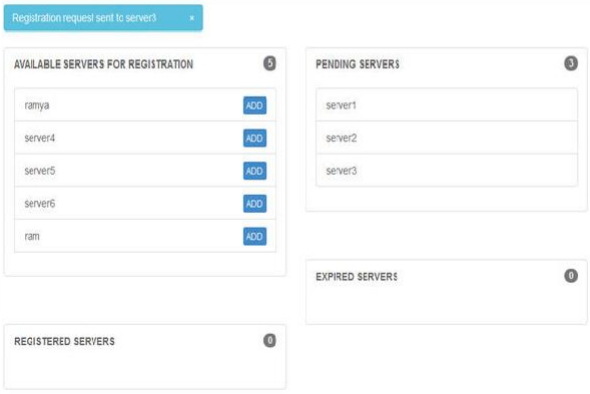


Fig 3: Client Login

Fig 4: Adding Servers



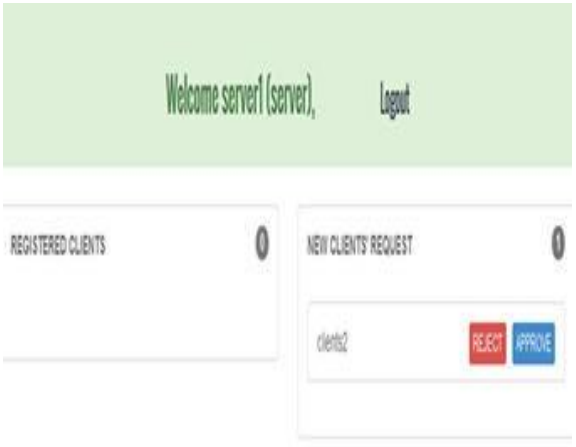


Fig 8: Encrypted and decrypted message

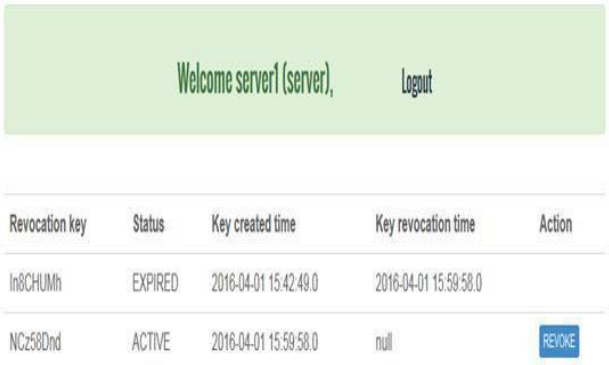


Fig 9: Revocation of Clients

Fig1 demonstrates the front screen of project. Fig2 shows option for client and server to register and Login.Fig3 illustrates client logging into page.Fig4 shows clients2 adding available servers for registration.Fig5 represents number of Registration servers, Pending servers, Expired servers, registered servers names.Fig6 displays the option for server whether to approve or reject client request.Fig7 indicates client sending message to server.Fig8 illustrates the server viewing the message which is both encrypted and decrypted along with sender name and received time.Fig9 demonstrates the server revoking the clients, which can no longer send messages to server.

6 CONCLUSIONS

The approach here is mainly concerned on the issuing of identity based revocation. The mathematical calculation for outsourcing into IBE is introduced and here we are proposing a method of revocable where the operations on revocation are treated as substitute to CSP. By the help of KU-CSP, this method has the following features: a) For both the size of private key at client and calculating the PKG constant efficiency has to be achieved. b) While updating the key the clients are not supposed to contact with the PKG i.e., the PKG is supposed to go offline after the list of revocation to KU-CSP is sent. c) Thorough examination is not needed while updating the key between the client and the KU-CSP. d) Revocable IBE below the stronger adversary model is considerable. Presenting an developed construction and showing that it is protected under RDoC model, where one of the KU-CSPs is expected to be loyal. It is not possible to provide aid to client to obtain his/her de-cryptability again, even if the revoked client and any of the KU-CSPs collude. Lastly, we provide the extensive experimental outcome to demonstrate the efficiency of our proposed construction.

7 REFERENCES

[1] Boneh and Franklin mechanism, R. Schlegel, D. S. Wong, and C. Tang, ―A con- ditional proxy broadcast re-encryption scheme supporting timed- release,‖ in Proc. 9th Int. Conf. Inf. Security Practice Experience, 2013, pp. 132–146.

[2] Adel Binbusayyis*, Ning Zhang, and C. Tang, ―A CCA-secure identity-based conditional proxy re-encryption without random oracles,‖ in Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–146.

[3] A. B. Lewko and B. Waters, ―Decentralizing attribute-based encryption,‖ in EUROCRYPT‘11. Springer, 2011, pp. 568–588.

[4] J. Kenney, ―Dedicated Short-Range communications (DSRC) standards in the united states,‖ Proceedings of the IEEE, vol. 99, no. 7, pp. 1162– 1182, Jul. 2011.

[5] L. Harn and J. Ren, ―Generalized digital certificate for user authen- tication and key establishment for secure communications,‖ Wireless Communications, IEEE Transactions on, vol. 10, no. 7, pp. 2372–2379, Jul. 2011.

[6] Wan et. al, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Public Key Cryptogra- phyPKC 2011. Springer, 2011, pp. 5370.

[7] M.J. Atallah and K.B. Frikken, __Securely Outsourcing Linear AlgebraComputations,‘‘inProc.5thACMSymp.Inf.,Comput.Commun. Secur., 2010, pp. 48-59.

[8] C.-K. Chu, J. Weng, Chase, S. S. M. Chow, J. Zhou, and R. H. Deng, ―Conditional proxy broadcast re-encryption,‖ in Proc. 14th Aus- tralasian Conf. Inf. Security Privacy, 2009, pp. 327–342.

[9] Q. Tang, ―Type-based proxy re-encryption and its construction,‖ in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol., 2008, pp. 130–144.

[10] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, ―A type-and-iden- tity-based proxy re-encryption scheme and its application in healthcare,‖ in Proc. 5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.

[11] L. Cheung and C. Newport, Provably secure ciphertext policy abe, in Proceedings of the 14th ACM conference on

Computer and communi- cations security. ACM, 2007, pp. 456465.

[12] Qingwei Zhang, Mohammed Almulla, Ciphertext-policy attribute- based encryption,‖ in Security and Privacy, 2007. IEEE Symposium

[13] Pervez, Z. et. al Attribute-based encryp- tion for fine-grained access control of encrypted data,‖ in New York, NY, USA: ACM, 2006.

[14] M.J. Atallah and J. Li, __Secure Outsourcing of Sequence Comparisons,‘‘ Int‘l J. Inf. Secur., vol. 4, no. 4, pp. 277-287, Oct. 2005.

[15] A. Sahai and B. Waters. Fuzzy identity based encryption. In EURO- CRYPT, pages 457473, 2005