ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

A Revocation Scheme for Gateway Applications in Cloud using ID

[1] A.BhagyaLakshmi [2] Dr.P.Ezhumalai
[1] Student [5] Professor and HOD
[1][2]Department of Computer Science and Engineering,
R.M.D. Engineering College, Chennai-601206
[1]bhagyarumugam@gmail.com, [2]hodcse@rmd.ac.in,

Abstract: **Cloud provides most of the services to its customers on demand via internet which are expected to be always on and have a critical nature. But before the customer or user gains permission to access the cloud service, the user must me authenticated and authorized by the cloud server. There are many ways where a user is been provided with authorization to access the cloud services. Once the user is provided with the authorization for a particular period of time (day or week or month or year) accessibility of the services are provided to the users. The revocation procedure is triggered at the end of the time period. This paper brings out a survey of various ways of revocation scheme which are used for accessing the cloud services. Compared with various revocable procedures such as attribute encryption and certificate encryption which are based on the public key cryptosystems, our mechanism can significantly improve the efficiency of user revocation using the identity. ID-based revocation possibly removes the use of public key infrastructure (PKI) and certification authorization which involves an online assistance to get authorized for accessing the services of cloud.**

Keywords: **Cloud service, Identity, Revocation, Time period, PKI.**

I. INTRODUCTION

Cloud services are made available to users on demand via the Internet from a cloud computing provider's servers. It provides easy and scalable access to applications which is managed by cloud services provider. Revocation of the services like data backup, e-mail services, documentation services, technical services are provided to the customers, it should be done in a proper way when it is provided to the users which include security, scalability, and trust worthy.

In cloud, the revocation is done by the operation of some cryptosystems, usually under the environment of public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked. The entities presenting those (revoked) certificates should no longer be trusted. A CRL is generated and published periodically, often at a defined interval. The revocation list is always issued by the certificate authority which issues the corresponding certificates. The lifetime of each CRL is maintained during which they are valid. This lifetime is often 24 hours or less. The PKI-enabled applications are considered to verify a certificate based on the use during a CRL's validity period. There are two different ways where the revocation can be done easily. These two revocation methods are Revoked and Hold. The below figure shows the PKI infrastructure for the revocation scheme.

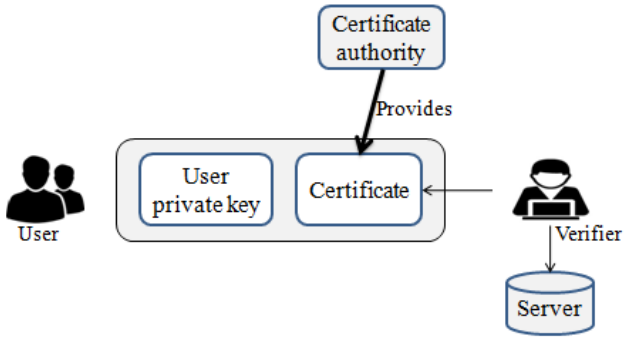

Fig.1: PKI Infrastructure

In revoked state it is discovered that the certificate authority (CA) has to issue the certificate but can be done improperly if misused by hackers or if the private key is compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements, such as publication of false documents, mis-representation of software behaviour, or violation of any other policy specified by the CA operator or its customer. The most

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

common reason for revocation is the user no longer being in sole possession of the private key (e.g., the token containing the private key has been lost or stolen). In case if the user's private key has been lost and the user is unsure about it then temporarily the certificates are invalid. At this point of time the status of the user is kept hold without providing the authorization to access the services from the cloud server. In case if the private key is found, then the certificate is valid again to access the services from the cloud server. Whenever the authorization is dependent on the certificate, it is important to check the status of the certificate however and whenever it is maintained. In case of failing this checking processes there may incorrectly occur the acceptance of the certificate as valid without revocation. This clearly says that the public key infrastructure should be effective for one for accessing the cloud services efficiently. The process of self-authenticating eliminates the use of this environment over cryptography.

II.ORGANISATION

The remainder of this survey is organised as follows. The section III demonstrates the literature survey of various revocation procedures in cloud with the methodologies used and its disadvantages, and the procedures to overcome the limitations. Section IV demonstrates the future enhancement of the paper. Lastly we draw a conclusion in section V.

III.LITERATURE SURVEY

1. Boneh and franklin ,Identity-based encryption from the Weil pairing,2001.

Boneh and franklin [1] in 2001, has proposed an Identity-based Encryption (IBE) [1] from weil pairing as a first practical scheme. In order for the non-revoked users to receive a new private key periodically the Boneh and franklin has proposed a simple revocation scheme. Using the ID of the receiver (name, e-mail address) the sender encrypts the messages. While the receiver decrypts the messages using the private key they currently have. Hence a new private key has to be updated by the user periodically. In order to revoke the user from the cloud services the private key is simply stopped providing. Hence it results in heavy load for private key generated (PKG) to generate a private key for each user. Also there is no secure channel that can be maintained between the user and the PKG. Boneh and Franklin has used the Bilinear Diffie-Hellman [1] problem in the random model for security.

2. D. Boneh, X. Ding, G. Tsudik, and C.-M. Wong, "A Method for fast revocation of public key certificates and security capabilities",2001.

To overcome the load of the Private key the Boneh [1] in Boneh and franklin scheme has proposed another revocation scheme [2]. It is known as immediate revocation. To manage the load of the previous [1] system proposal, Boneh [2] immediate revocation method is designed to be trusted online authority. As the authorisation involves both the user and the online mediator, they can be cheated by one another. Even when the user is been revoked the online mediator must help the user to decrypt the private key which becomes a bottleneck because of large number of users.

3. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," 2008.

In order to improve the efficiency of the key generation Boldyreva [3] in 2008 has proposed a new revocable scheme based on the concept of fuzzy [11] in order to decrease the large number [2] of key updates Boldyreva adopts a binary tree structure of the users. He suggests that this method of sub tree can improve the efficiency for the user to success the services.

4. B. Libert and D. Vergnaud, "Adaptive-ID secure revocable identity-based encryption, ,2009.

Libert and vergnaud [5] in 2009 furthermore presented a method named adaptive-Id in order to improve the security of the Boldyevera [3] sub-tree method. However this scheme resulted in many problems. It resulted in enormous workload for the encryption and decryption computation. Also resulted in the problem of workload to maintain enormous number of user's binary tree. This becomes a disadvantage for handling large number of binary tree and to provide it security.

5. J.-H. Seo and K. Emura, "Revocable identity-based encryption revisited: security model and construction," 2013.

A more refined method of security model is introduced by the Seo and Emura [6]. Decryption key attacks can be a threat to the Boldyvera [3] model. In order to resist the decryption key attack a new revocable scheme is proposed based on the idea of [5]. However this decryption key attack is based only on the size of the private key used by each user.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

6. 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, 2015.

Decryption key attacks have the possibility of happening based on the size of the private key. Park [7] proposed a new revocable scheme in order to reduce the size of the private key to avoid the decryption key attacks [6]. But Park revocation has a problem where, the size of the key is dependent only on parameters of the users. In order to avoid Park disadvantage Wang in 2000 used both the encryption method and sub tree method to propose a new revocation method.

7. J.-H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption,", 2013.

Seo and Emura [10] presented a first revocable HIBE scheme in order to extend their old methodology. In this new scheme a secret key is generated by each user for each period by the multiplication of various partial keys. To generate these secret key a history of pervious hierarchy tree is used. It is critical to have a history of keys of the time period which results this scheme as very complex.

8. Y.-M. Tseng. and T.-T. Tsai, "Efficient revocable ID-based encryption with a public channel," , 2012.

In 2012, Tseng and Tsai [11] proposed a new revocable IBE scheme to remove the usage of secure channel between each user and the authority and use a public channel instead to transmit users' periodic private keys. However, the key-update efficiency is linear in the number of users so that the computation burden of PKG is still enormous.

9. S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," , 2013.

Using the attributes of the user the encryption and decryption of the messages are done. But this technique [12] S.Hohenberger and B.Waters will incur significant amount of cost for functioning. However there may cause a problem based on the size of the messages used. A limit is fixed for the number of attributes which are used for the cipher text or private key. A more generalized decryption algorithm is used which breaks the attributes into rows of access matrix. However the performance of this technique is still an open problem.

10. K. Kurosawa and S. Heng, "From digital signature to ID-based identification/signature," 2004.

In 2004, Kurosawa and S.Heng [16] formalized the digital signature and ID-based identification scheme. Comparing the both scheme Kurosawa [16] developed ID-based digital signature scheme. This paper also discusses the difference between normal identification scheme and ID-based identification scheme

11. A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. Eurocrypt'05, LNCS, vol. 3493, pp. 457-473, 2005.

A.Sahai and B.Waters [17] proposed a new type of identity based encryption based on the concept of fuzzy. This paper introduces two identities to be used. One for encryption and other for decryption. Based on the metrics used, only if both the identities are close then the access is provided. This incurs significant communication problem. The below table shows the comparison of various revocation schemes and their limitations.

Table 1. Comparison of various revocable schemes.

	[5],[6], [7],[10]	[11]	Our scheme
Workload	Medium	High	Low
Scalability	Not support	Un scalability	Yes
Efficiency	No	No	Yes
Computation authority	No	No	Yes

According to the survey made above the certificate revocation list (CRL) method if a party receives a public key and its associated certificate, they 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. And in immediate revocation method employs a designated semi-trusted and online authority (i.e. mediator) to mitigate the management load of the PKG and assist users to decrypt cipher text. In such a case, the online mediator must hold shares of all the user's private keys. Since the decryption operation must involve both parties, neither the user nor the online mediator can cheat one another. When a user was revoked, the online mediator is instructed to stop assisting the user. However, the online mediator must help users to decrypt each cipher text so that it becomes a bottleneck for such schemes as the number of users grows enormously. As

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 12, December 2016

there is large number of users the load of maintaining the each user's private key is difficult.

IV.FUTURE ENHANCEMENT

Here, we enhance our survey of revocable scheme for accessing the services in the cloud using the identity as follows. We divide our proposal into three roles namely, an Administrator, a Revocation authority (RA) and users. When the user wants to access the cloud services the user is permitted for the registration first using his/her credentials such as name, e-mail address, etc. Using the credentials the administrator generates a master ID for each and individual user. Each and every time the user logins to access the cloud services the user is provided with the time update ID. The user no longer needs to decrypt any private key to get the authorization to access the services. Also a gateway application is created where the user need not remember the ID and password of each and every account. Also the enhancement is positively free from history and load. The efficiency and scalability to accessing the cloud services from the cloud server can be improved over public network.

V.CONCLUSION

As compared with various scheme, the performances of computation and communication are very high. The enhancement of new revocable scheme in cloud for the user to access the services and applications in cloud server can significantly improve to performance and computation. This new revocable scheme can also alleviate the heavy load of managing the entire private key. It is also free from history and the scalability and efficiency of accessing the applications for the users can be improved. It can also be improved in a way where the user is free from various kinds of user ID by using the gateway application access.

REFERENCES

[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proc. Crypto'01, LNCS, vol. 2139, pp. 213-229, 2001.

[2] 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.

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

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

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

[6] 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.

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

[8] C. 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.

[9] A. 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.

[10] 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.

[11] Y.-M. Tseng. and T.-T. Tsai, "Efficient revocable ID-based encryption with a public channel," Computer Journal, vol.55, no.4, pp. 475-486, 2012.

[12] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," Proc. PKC'13, 2013.

[13] P.-W. Chi and C.-L. Lei, "Audit-free cloud Storage via deniable attribute-based encryption," IEEE Transactions on Cloud Computing, article in press), 2015.

[14] J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute based encryption with revocation in cloud storage," International Journal of Communication Systems, article in press , 2015.

[15] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," International Journal of Information Security, vol. 14, 2015.

[16] K. Kurosawa and S. Heng, "From digital signature to ID-based identification/signature," Proc. PKC'04, LNCS, vol. 2947, pp 248-261, 2004.

[17] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. Eurocrypt'05, LNCS, vol. 3493, 2005.

[18] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2) ," IETF, RFC 7296,2014.

[19] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," IETF, RFC 6101, 2011.