International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 4 – MARCH 2017.

Survey of Certificateless Public Key Encryption for Cloud Security

Naveen Kumar C.G [#1] and Dr.SanjayPande M.B [*2]

[#]*Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, India.*

[*] *Professor& Principal, Sampoorna Institute of Technology & Research, Ramanagar, Karnataka, India*

***Abstract*— Cloud computing is the recent domain focused by several researchers. With the advents of cloud technologies, it has tremendous growth among the organizations and users.Security and Privacy are the two distinguished parameters used to secure the information from attackers. Third party is used as service providers to grasp the data sent by owner by offline mode in cloud environment. In some scenario, the cloud may reveal the data by accidentally for unauthorized users that degrades the performance of privacy and confidentiality. In this paper, we have surveyed about the novel concept "Certificateless Public Key Encryption (CL-PKE) schemes that emerged from the baseline of public key techniques and identity based cryptography systems. Key management is the primitive and mandate communication process between two authorized users. We have discussed about the fundamentals in Key based cryptography management systems that depicts the significance and variants of key management systems. And also discussed the prior works carried out in CL-PKE by other researchers and its pitfalls. From this survey, we have concluded that the study on key revocation issues has to be widely focused to decrypt the messages when public key is no longer valid.**

***Index Terms*— Cloud computing, security, privacy, Certificateless encryption, Key management systems and Identity based encryption.**

I. INTRODUCTION

A recent development made in Information and Communication Technologies (ICT) is the 'Cloud Computing'. Cloud system plays prominent role in IT sector for its high storage space and efficient data access. In recent years, the cloud computing has ruined the entire network of the IT sector [1]. It is configurable computing resources that can rapidly provision and released with minimal management efforts. The aim of the cloud computing system is to provide better quality of the service with minimal computing resources.It shares the resources over large-scale system. Hence, the data can be shared with minimal cost and location independent. The cloud users can use the cloud resources with the help of cloud service providers like, Amazon, google, IBM, sales force, Rackspace, and Microsoft.Using Cloud Service Providers (CSP) [2], the cloud entities shares the software's and other tools in which they required on demand basis. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises [3].

Rivest, Shamir and Adleman introduced the public key encryption scheme, named, RSA in 1978 [4].The objective of the RSA algorithm is to protect the message between two entities.It is executed using two keys, viz, public key and private key. Public key is used for encryption process whereas private key is used for decryption process. Though, public key encryption scheme exhibits some practical problems. Sender should ensure that the generated public key is validated one for the receiver [5].Therefore, the need of public key encryption with third party auditor to verify the association among receiver's ID, connection ID and intended public key.The study reveals that Public Key Management (PKM) is the most unmanageable task under any framework that utilizes the public key cryptography.Fig.1. presents the general flow of Certificateless encryption schemes.

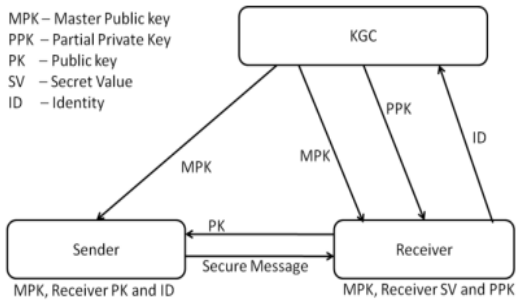

Fig.1 Generalflow of Certificateless encryption schemes [5]

Public key management is the controllable function under the concept of Identity based encryption scheme.It consists of digital identifier and public keythat has to be monitored and verified so as to build the public infrastructure [6]. With the received public key, knowledge is discovered for generating the private key.Using efficient key management systems, public key system operates efficiently. Since, some practical issues occur with identity based public key cryptosystem that handles the key revocation model.These drawbacks are surmounted from the public key encryption and identity based encryption which is known as Certificateless public key encryption (CL-PKE). The thought of CL-PKE is to merge the advent of public key model with the identity based scheme.

The rest of the paper is organized as follows: Section II describes the basic primitives of the cloud security and Section III summarizes the major key points of the cloud

security system.

II. RELATED WORK

This section depicts the overview about key based cryptography system and the prior techniques suggested by other researchers.

A. CRYPTOGRAPHY SYSTEM

Encryption and access control are the major security parameters that ensure the data confidentiality in the IT environment.Key Management System (KMS) is been deployed as security management functions.

a) Overview of key management:

The cryptographic keys is divided into two categories [7],

Secret key: Secret key is used in symmetric cryptographic algorithms and to support data integrity in Message Authentication Codes (MAC).Secret key is also known as 'symmetric key' where both encryption and decryption process uses the same key.

*Public/Private key pair:*This key is applied to authentication, digital signature and key establishment. Public key is published to both senders and receivers whereas private key is generated based on the received public key. Some cases it is also referred as 'secret key'.

Based on the above keys as the primitives, the cloud deployed additional keys like [8]:

*i) Public/Private authentication key pair:*This type of key pair is used for authenticating the other users. It has been applied to various concepts like Transport Layer Security (TLS), Virtual Private Network (VPN) and smart card login system. This key pair is used in long-term applications.

ii) Public/ Private signature key pair: This process signs the message or data in order to verify whether authorized users received the packets. Public key is used for validating the signature of the message. Sample instances like Secure/ Multipart Internet Mail Extensions (S/ MIME), signed electronic documents and code. It is also used for validating the signatures on stored data.

*iii) Public/Private key establishment pair:*The key is established between the users. Generally, it is applied to the stipulated period of time where the data confidentiality is assured.

iv) Symmetric Encryption/ Decryption key: The symmetric key is used for data integrity process. It is guaranteed in three ways: a) Employing symmetric algorithms and MAC operations b) Encryption mode of operation and c) Employing hash based MAC.

v) Symmetric key wrapping key: A symmetric key is used to encrypt a symmetric key or an asymmetric private key. A Key Wrapping Key is also called a Key Encrypting Key.

The states of the keys are presented as follows [9]:

i) Generation: The private key or public key or symmetric key is generated based on the requirements.

ii) Activation: The generated symmetric key will be activated once requirement is initiated.

iii) Deactivation: When the cryptographic time is finished off, and then no longer is used for other cryptographic protection data.

iv) Suspension: In certain period of time, the key may be suspended based on different reasons.

v) Expiration: When the stipulated time is over, the key gets expires with its associated metadata.

vi) Destruction: key is destroyed when it is no longer needed

vii) Revocation: It operates on the private key. The unauthorized users are removed from the network environment.

b) Certificateless public key encryption

The general flow of certificateless public key encryption consists of seven algorithms [10].

a) Setup (SU): Based on the given security parameter k, the Key Generation Center (KGC) assists to outputs the master secret key msk and master public key mpk. The master public key contains message M and ciphertext space C.

b) Partial Private key Extract (PPKE): Using mpk, msk, and identifier ID for the entity A, the KGC runs on Probabilistic Polynomial Time (PPT) which in turn generate private key for the entity A. And this private key is transferred to the entity A over a confidential channel.

c) SetSecretValue (SSV): Using the mpk and ID_A, then the secret value X_A is computed.

d) SetPrivateKey (SPK): With the mpk and secret value X_A, the private key SK_A is generated.

e) SetPublicKey(SPK): Using the mpk and secret value X_A, then the public key PKA for the entity A.

f) Encrypt (E): Using the given plaintext m € M, the entity A with its mpk, ID_A and public key PK_A, the sender A creates ciphertext C.

g) Decrypt (D): Using the mpk, private key SKA, and the ciphertext C, the original message M is derived for the authorized users.

B. PRIOR WORKS

Al- Riyami and Paterson introduced Certificateless encryption schemes in 2003. The author in [11] surveyed variants of CLE security models and their pitfalls. Usually, there are two types of adversariespersist in Certificateless encryption model. The type I adversary model is the group of attackers who acts like normal users and steals the sensitive data. Owing to the lack of certificate, the attackers can modify the public keys. The type II adversary owns a Key Generation Center (KGC) that holds the master key and updates the public key of the users. The type I scheme is strongly secured than the type II model [12].The author in [13] presented the first security model for Certificateless encryption schemes.Their model is not secured since the public key of the user depends on the identity. This drawback was overcome by the author in [14] in which hierarchical based CLE schemes are presented.None of the study has revealed that hierarchical

based CLE is secured model.

The author in [15] discussed about the CLE schemes without using the concept of pairing. Their model worked with security lack of protecting the normal users. This was further improved by author in [16]. They proposedidentity oriented trapdoor functions that strongly secured the normal users before being attacked. The author in [17] studied about the partial decryption of the users using a Security Mediator (SEM) which is named as Security Mediated Certificateless Encryption (SMCLE). They constructed random oracle model which exhibits strong and secured systems.The author in [18] suggested an enhanced Certificateless Intermediary Re- Encryption scheme (CL-PRE). They discussed about the data sharing process in cloud computing models. They solved the issue of key escrow from matched records. Computational cost was significantly minimized by the standard operations. They also discussed about the Chosen Ciphertext attack.The author in [19] proposed a generic certificateless KEM scheme based on public key encryption ID-based KEM and message authentication code, in the standard model. They proved the security of the scheme against malicious-but-passive KGC attacks without using a random oracle model.

Secondly, they proposed a certificateless tag-based KEM scheme based on the concept proposed in [20]. They also showed the construction of a hybrid certificateless encryption scheme by applying Abe et al.'s transformation to a certificateless tag-based KEM and one time DEM. The schemes were less efficient but comparable to the certificateless KEM scheme of [21] in which only random oracle models were used to prove the security. The author in [22] proposed certificateless encryption schemes in the standard model and proved the secure against strong adversaries without using random oracle models. The proposed scheme was based on a combination of certificateless encryption schemes, public key encryption schemes, and the extended version of [23] and [24] for non-interactive zero-knowledge proofs. In [25], they showed that the schemes of [26] and [21] were insecure and required random oracle models to prove their security. Then, they proposed an improved and secure scheme against a malicious KGC attack in the standard model.

The study on key generation technique was studied by author [27] where one public key was used for one private key generation using CL-PRE. They resolvedbilinear Diffie Hellman issue. The author [28] discussed the traditional ID based public key cryptosystem using the revocation concepts. In order to provide the forward and backward security, Revocable Storage Identity Based Encryption (RSIBE) was framed to update the ciphertext eventually. Two parties authenticated based certificateless public key encryption scheme was introduced. The author in [29] studied the similar approach under multi-authorityby identifying their user's attributes. The main intention of the Identity based cryptography is to decrypt the ciphertext by its intended users.The author in [30] Identity-based Cryptography (ID-PKC) which eliminates the need for certificate by deriving public keys for users directly from their human-memorizable information, such as e-mail address and IP address. The private keys are fully generated by a Private Key Generator (PKG) which inevitably introduces the key escrow problem.

III. CONCLUSION

This paper portrayed the survey of certificateless public key cryptography schemes which emerges from the advents of identity based and public key encryption techniques. The objective of this scheme is to resolve the key management issues. We have depicted the drawbacks of CL-PKE schemes proposed by Al-Riyami et al.And also we discussed about the security schemes for Type I and Type II attackers models.The problems associated with constructing a certificateless encryption scheme that is provably secure in the Strong Type I and Weak Type II models without using the random oracle methodology were also considered. Hence, we conclude that the Certificateless Public Key Encryption (CL-PKE)is not furnished completely for providing better cryptographic solutions. The infrastructures of the CL-PKE schemes have to be focused. The key revocation problems for certificateless encryption schemes which develop from the baseline of those identity-based encryption, does not seem to be adequate way of revoking a user's right to decrypt messages or of informing users when a public key is no longer valid. The distribution problem is more unusual. Any solution to the problem of public-key distribution has to prevent a user being overwhelmed with 'false' public keys, and the problem of selecting a real public key from a false one.

REFERENCES

[1] S. Al-Riyami. Cryptographic schemes based on elliptic curve pairings. PhD thesis, Royal Holloway, University of London, 2004. Available from http://www.isg.rhul.ac.uk/~kp/sattthesis.pdf.

[2] M. Bellare and P. Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In S. Vaudenay, editor, Advances in Cryptology – Eurocrypt 2006, volume 4004 of Lecture Notes in Computer Science, pp. 409–426.

[3] C. Yang, F. Wang, and X. Wang,"Efficient mediated certificates public key encryption scheme without pairings," in AINAW, Niagara Falls, ON, May. 2007, pp. 109–112.

[4] Y. Sun, F. Zhang, and J. Baek, "Strongly secure certificateless public key encryption without pairing," in Proc. 6th Int. Conf. CANS, Singapore, 2007, pp. 194–208.

[5] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in Proc. ASIACRYPT 2003, C.-S.Laih, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452–473.

[6] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Securitymediatedcertificateless cryptography," in Proc. 9th Int.Conf. Theory Practice PKC, New York, NY, USA, 2006,pp. 508–524.

[7] S. Coull, M. Green, and S. Hohenberger, "Controlling access toan oblivious database using stateful anonymous credentials," inIrvine: Proc. 12th Int. Conf. Practice and Theory in PKC, Chicago, IL,USA, 2009, pp. 501–520.

[8] van der Merwe, J., Dawoud, D., and McDonald, 2007,"A survey on peer-to-peer key management for mobile ad hoc networks,‖ ACM Comput. Surv. 39, 1.

[9] ShaheenaKhatoon and Balwant Singh Thakur, 2015, "Certificate less key management scheme in manet using threshold cryptography‖, International Journal of Network Security & Its Applications (IJNSA) Vol.7, pp.55-59.

[10] Sanjeev Kumar Rana and Manpreet Singh, 2011, "Certificateless Efficient Group Key Management Scheme in Mobile Adhoc Networks‖, International Journal of Computer Science Issues, Vol. 8, pp.343-351.

[11] PreetiSheoran and VirenderKumar ,"Key management with pairing and with certificateless cryptography in manets‖, International Journal of Advanced Computer Technology (IJACT), Vol. 3., pp.27-35.

[12] Fagen Li, Masaaki Shirase1, and Tsuyoshi Takagi1, 2008, "Key Management Using Certificateless Public Key Cryptography‖, International Federation for Information Processing, pp.116-126.
[13] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang and Younggoo Kwon, 2005, "AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks‖, IEEE, pp. 3515-3519.
[14] Mr. BhaveshRahulkar , Mr. Praveen Shende, 2013, " A Two Layer Encryption Approach to Secure Data Sharing in Cloud Computing‖, International Journal of Advanced Research in Computer Engineering & Technology, Vol 2, pp.3252-3254
[15] A. W. Dent, B. Libert and K. G. Paterson, "Certificateless encryption schemes strongly secure in the standard model‖, in Public Key Cryptography–PKC 2008, Springer, (2008), pp. 344–359.
[16] X. Boyen, Q. Mei and B. Waters, "Direct chosen ciphertext security from identity-based techniques‖, in Proceedings of the 12th ACM conference on Computer and communications security, (2005), pp. 320– 329.
[17] J. Kar, "Provably Secure Identity-Based Aggregate Signcryption Scheme in Random Oracles‖, International Journal of Network Security, Taiwan, vol. 17, no.5, (2015), pp. 580-587.
[18] J. Kar, "Deniable Authentication Protocol based on Discrete Logarithms and Integer Factorization Problems‖, ICIC Express Letters, Japan, 2012. vol. 7, no. 7, (2013) July, pp. 2061-2067.
[19] D. H. Yum and P. J. Lee, "Generic Construction of Certificateless Encryption‖, in Computational Science and Its Applications – ICCSA 2004, A. Laganá, M. L. Gavrilova, V. Kumar, Y. Mun, C. J. K. Tan, and O. Gervasi, Eds. Springer Berlin Heidelberg, (2004), pp. 802–811.
[20] J.Kar, "Non-interactive Deniable Authentication Protocol using generalized ECDSA Signature Scheme‖, International Journal of Smart Home. Korea, vol. 5, no. 4, (2011) Oct., pp. 39-49.
[21] J. Kar & D. M. Alghazzawi, "On Construction of Signcryption Scheme for Smart Card Security‖, IEEE International Conference on Intelligence and Security Informatics (IEEE ISI 2015), US, (2015), pp. 109-113.
[22] G. Kappes, A. Hatzieleftheriou and S. V. Anastasiadis, "Dike: Virtualization-Aware Access Control for Multitenant Filesystems", University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.
[23] Srinivasa Rao Chintada, ChandraSekharChinta, "Dynamic Massive Data Storage Security Challenges in Cloud Computing Environments", International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 3, pp. 3609-3616, March 2014.
[24] Kevin D Bowers, Ari. Juels and Alina Oprea, "HAIL: A High Availability and Integrity Layer for Cloud Storage", In the Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, pp. 187-198, 2009.
[25] Spillner J, Mller J and Schill A, "Creating Optimal Cloud Storage Systems", IEEE Transactions on Utility and Cloud Computing, vol. 29, issue. 4, pp. 1062-1072, June 2013.
[26] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach and Security Challenge", International Journal of Soft Computing and Engineering (IJSCE), vol. 2, no. 1, pp. 421-424, March 2012.
[27] Victor Chang, Muthu Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transaction on Service Computing, vol. 9, issue. 1, pp. 138-151, ISSN: 1939- 1374, January 2016.
[28] KalpanaBatra, Ch. Sunitha, Sushil Kumar, "An Effective Data Storage Security Scheme for Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, no. 4, pp. 808-815, June 2013.
[29] Hamdan M. Al-Sabri, Saleh M. Al-Saleem, "Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security", IJCSI International Journal of Computer Science Issues, vol. 10, no. 1, pp. 259-266, March 2013.
[30] Keiko Hashizume, David G Rosado, Eduardo FernndezMedina and Eduardo B Fernandez, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, pp. 1-13, 2013.