Certificate-less Encryption in Cloud

[1]Siddharth Singh, [2]Aaishwarya Sahu, [3]Manoj Bhoye, [4]Prof. D. R. Pawar

Department Of Computer Engineering, Sinhgad College Of Engineering, Pune, India

Abstract: *Secure data sharing is one of the key functionalities of any cloud-based system to supply security to the clients and prevent it from attacks. RSA is one such cryptographic algorithm that provides security of the data shared on the cloud .RSA is cryptosystem for public-key encryption .RSA uses 2 totally different but mathematically linked keys, one is public key and the other is private key. The cloud is employed as a secure storage as well as a key generation center. In our system, data owner encrypts the sensitive data using the cloud-generated users public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The users subsequently fully decrypt the partially decrypted data using their private keys. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information.*

Keywords : Certificate Authority, Certificateless Public Key Cryptography, Chosen Plaintext Attack, KGC, RSA, PRE, SEM.

1. INTRODUCTION

Cloud Computing is the delivery of computing services over the Internet. Their are four types of Cloud Computing that is Private Cloud,Public Cloud,Hybrid Cloud and Community Cloud. Organizations have been adopting public cloud services such as Microsoft Skydrive, Dropbox, and Google Drive to manage their data with the help of Cloud Computing. Encryption The data owner obtains the key of users from the cloud. Then data owner encrypts the data using the public key of user. Types of Encryption are Symmetric Key Encryption and Public key Encryption. Decryption is when a user wants to read some data, it sends a request to the Sender to obtain the partially decrypted data. With the help of private key he decrypts the data and accesses it.

This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder therefore protecting unauthorized users from having access to the information even if they are able to break into the system.

Cryptography is playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender. It has become more critical to our day-to-day life because thousands of people interact electronically every day; through e-mail, e-commerce, ATM machines, cellular phones, etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users. Despite the fact that secured communication has existed for centuries, the key management problem has prevented it from commonplace application. The development of public-key cryptography has enabled large-scale network of users that can communicate securely with one another even if they had never communicated before.

2. RELATED WORK

Seung-Hyun Sco [1] proposed a system for certificate-less encryption for data sharing in public clouds, using mediated certificate-less pairing key encryption that solved the key escrow problem.

Shaheena Khatoon et al [5], proposed a certificate less key management for MANET using threshold cryptography. They have presented a distributed key mechanism, where certificate less public key cryptography and threshold cryptography are combined and employed. They have proved that their method is a secured scheme for MANET as well as it eliminates the need for certificate-based public key distribution and the key escrow problem. Certificate-less Efficient Group Key Management Scheme in Mobile Adhoc Networks [6], was proposed by Sanjeev Kumar et al. They have implemented identity based cryptography for secure multicast group communication. The method reduces storage space by avoiding the usage of PKI.They have hided the public key which is visible only to the trusted nodes and thereby increasing security from crackers as well as making the encryption and decryption faster.

Preeti et al [7], in their article proposed a key management with pairing and certificate less cryptography in MANETs. They have incorporated the idea of Shamir's secret sharing scheme in their method. The master secret keys are shared some are all the nodes in the MANET. They have proposed an improved secure tripartite authenticated key agreement protocol. They have enhanced d the key strength with some simulation mechanism. They have also presented an idea of adopting certificate-less public key encryption (CL-PKE) schemes over mobile ad hoc network (MA-NET). Fagen Li

et al [7], has proposed a scheme titled key management using certificate-less public key cryptography in ad hoc networks. They have present ted a distributed key management approach by using the recently developed concepts of certificate-less public key cryptography and threshold secret sharing schemes .They have assured that their method does not have the built - in key escrow feature of ID - PKC. In their method the KGC computes a partial private key from the user's identity and a master key. The user then combines the partial private key with some secret information to generate the actual private key.

Sattam S. Al - Lan Zhou [4], has presented a certificate-less public key cryptography which is a model for the use of public key cryptography that is intermediate between traditional PKI and ID - PKC. They have proved that their encryption scheme is secure in a new and appropriate model, given the hardness of an underlying computational problem. They have showed how their concept can be realized by specifying a certificate-less public key encryption (CL - PKE) scheme that is based on bilinear maps.

Sanjeev Kumar et al [5] have proposed a scheme called A Two Layer Encryption Approach to Secure Data Sharing in Cloud Computing in which they have given double encryption for securely outsourcing the data in cloud. They have made use of RSA algorithm of asymmetric key approach to resolve the key escrow problem and data revealing problem. Their method has certificate for the user and two layer encryption where one is done by the cloud and the other by the user thereby increasing the security. Securing Mobile Ad Hoc Networks with Certificate-less Public Keys has been presented by the authors Yanchao Zhang et al [8]. They have discussed about key management in their article as well as presented an ID - based key management scheme which is a combination of ID and threshold cryptography. In addition they have also provided guidelines about how to choose the secret sharing parameters that are used wit h the cryptography so as to improve security and robustness.

3. PROBLEM STATEMENT

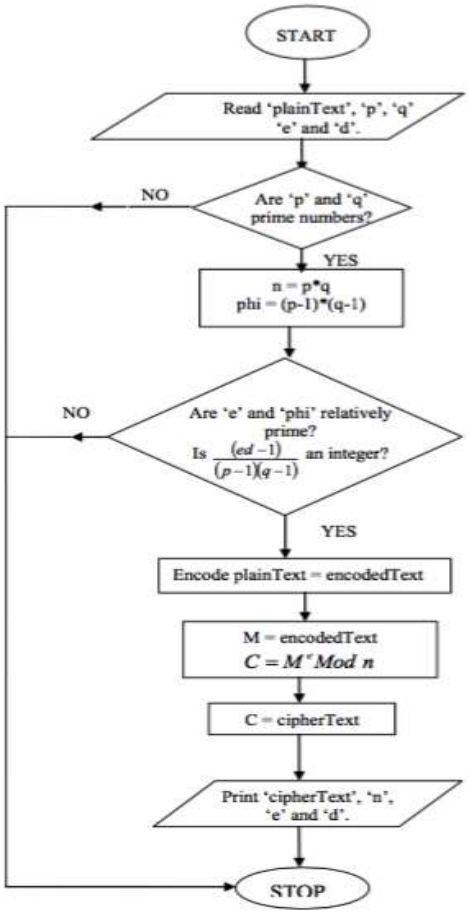
The data on the cloud must be strongly secured from unauthorized accesses. In order to assure confidentiality of sensitive data stored in public clouds, a commonly adopted approach is to encrypt the data before uploading it to the cloud. So a system is to be built which provides certificate-less encryption in cloud by key generation.

4. METHODOLOGY

4.1 The RSA Algorithm for Creating RSA Public and Private Key Pair

The RSA algorithm can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward. To create an RSA public and private key pair, the following steps can be used:

1. Choose two prime numbers, p and q. From these numbers you can calculate the modulus, $n = pq$
2. Select a third number, e, that is relatively prime to (i.e. it does not divide evenly into) the product $(p-1)(q-1)$, the number e is the public exponent.
3. Calculate an integer d from the quotient $(ed-1) / (p-1)(q-1)$. The number d is the private exponent.
4. The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.
5. To encrypt a message, M, with the public key, creates the cipher-text, C, using the equation: $C = M^e \ Mod\ n$
6. The receiver then decrypts the cipher-text with the private key using the equation: $M = C^d \ Mod\ n$



4.2 System Architecture

Architectural model represents the overall framework of the system. It contains both structural and behavioral elements of the system. Architectural model can be defined as the blue print of the entire system.

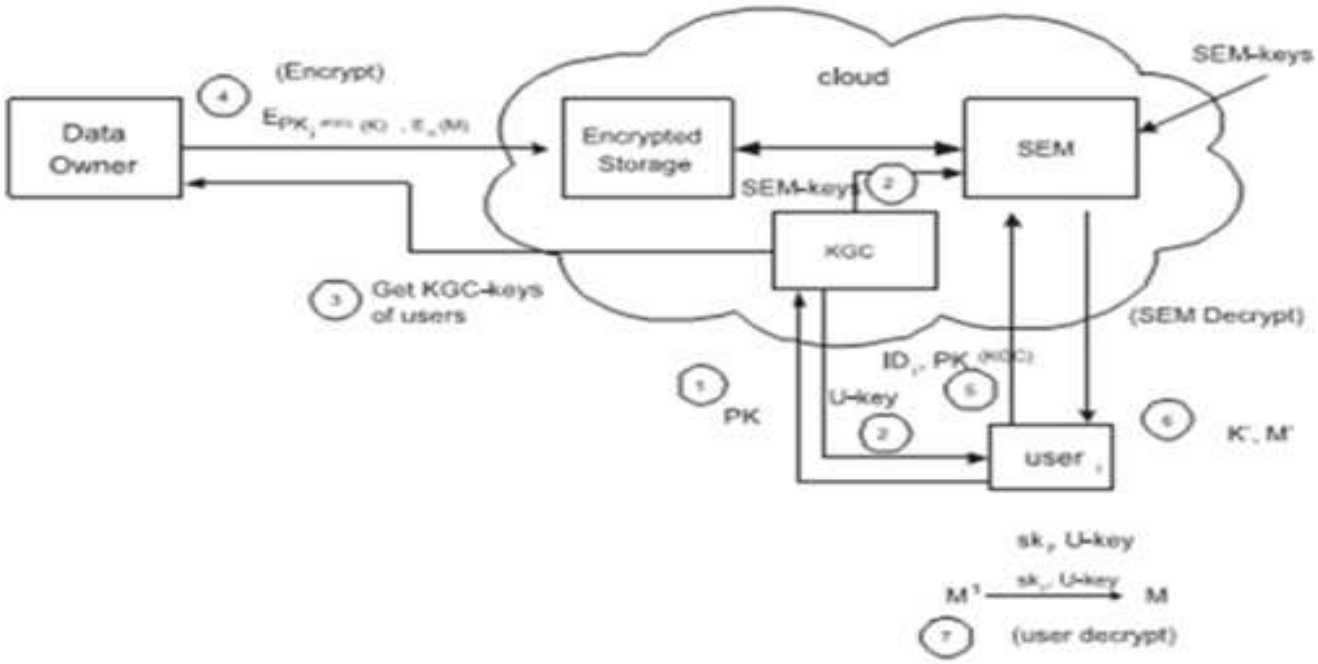


Fig 1: System Architecture

5. CONCLUSION

This is the basic function of the project is to provide an efficient certificate-less encryption in cloud. Our scheme reduces the computational overhead by using pairing-free approach. Compared to symmetric key based mechanisms, our approach can efficiently manage keys and user revocations? This is not only reduces the encryption cost but also provides better security of the data on cloud

REFERENCES

[1] Seung-Hyun Seo, Mohamed Nabeel,Member, and Elisa Bertino,Fellow, IEEE- "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 9, SEPTEMBER 2014.

[2] "An Efficient Certificateless Cryptography Scheme without Pairing"- Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding, Elisa Bertino Purdue University. Feb 2013.

[3] X. W. Lei Xu and X. Zhang, "CL-PKE: A certicateless proxy reencryption scheme for secure data sharing with public cloud," in ACM Symp. Inform. Comput. Commun. Security,2012.

[4] Z. Lan Zhou, Vijay Varadharajan, and Michael Hitchens," Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", Information Forensics and Security, IEEE Transactions on, vol. 8, no. 12, pp. 1947 – 1960, 2013.

[5] 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.

[6] Shaheena Khatoon 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.

[7] Fagen Li, Masaaki Shirase1, and Tsuyoshi Takagi1, 2008, Key Management Using Certificateless Public Key Cryptography, International Federation for Information Processing, pp.116-126.

[8] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang and Younggoo Kwon, 2005, ACPKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks, IEEE, pp. 3515-3519.