ISSN:0975-9646

A Survey on Various Attribute based Public Key Cryptography

Pooja Dubey
Scholar
Computer Science Engineering
Truba Inst. of Engg. & I.T.
Bhopal, India

Amit Saxena
Professor
Dept. Computer Science & Engg.
Truba Inst. of Engg. &I.T.
Bhopal, India

Dr. Manish Manoria
Director
Truba Institute of Engineering
& Information Technology
Bhopal, India

Abstract— A Public Key Encryption is a technique of encrypting the message using public keys so that the message is secure against various attacks. A Keyword based Public Key Encryption is a new way of providing security against various attacks. Although there are various keyword searches based public key encryption techniques are implemented. Here in this paper a survey of all the techniques based on Keyword search based public key encryption is analyzed and describes here, so that on the basis of their various advantages and limitations a new and efficient technique is implemented in future.

Keywords—CP-ABE, OTPK, TRNG, Data Sharing, Key Escrow, Proxy Encryption.

I. INTRODUCTION

Before a long time we were providing authentication with the physical appearance of person and by their signature manually, but now a day's different techniques were implemented. One of them is contracts signing. Contract signing is very important protocol by which we can exchange our data by online. So with the help of this technique we can prevent different attack so the solution is implemented a new scheme or new protocol which is more efficient and can be used for variety of applications especially in E-commerce. This technique allows an efficient signing between two parties such that the chances of attacks reduce. The technique is based on one time where after signing contract between parties the key destroys.

Proper security is achieved if exchange protocol having no los-preventing property. Loss preventing property means any party incurred no loss at all with other party. We can say that this protocol provide true fairness whenever parties exchange their data or information to each other or not [7].

Shared Key Cryptography

Symmetric key ciphers (i.e., shared key ciphers) have the advantage of relatively short keys and the ability of high rates of throughput. In such systems, secret crypto keys must be shared among those entities that are to communicate confidentially, so regarding two-party communication, the key must remain secret in both ends. In large networks, there would be many keys to be managed, and each user would have to securely manage a list containing the key pairs for each of his or her contacts. This could be impractical and troublesome, and lack ∞edibility concerning new and leaving users

Sharing long-term secret keys among a number of users is an impractical and troublesome assumption due to increased vulnerability from the aging of keys, and lack of flexible user constellations due to the shared keys. This could be mitigated by an online trusted third party (TTP) so that all communication goes through the TTP that shares a secret key pair with all relevant users. Nevertheless, this would in many cases be undesirable. It would correspondingly be a problem to distribute and establish new shared keys to new contacts over an insecure network if the key distribution protocol (that is, the key establishment protocol) is based on symmetric key ciphers, since this would require that a symmetric key is already shared between the distributor and the receiver.

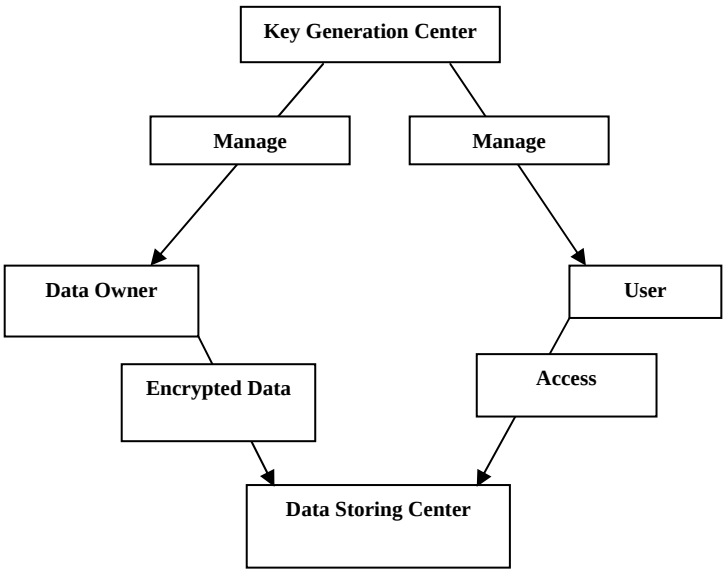

Figure 1. Basic architecture of Data Sharing System

In practice, symmetric key ciphers are mostly applied session-wise due to their capabilities of high throughput and efficiency. The shared session keys would be established by means of some secure key establishment protocol. Such protocols could be based on symmetric key ciphers or public key ciphers. However, a key establishment protocol based on symmetric key ciphers would still require that the two parties going to establish a shared secret session key still share a long-term secret key. Key establishment protocols based on public key ciphers eliminate the disadvantages of sharing long-term secret keys.

Many times, the objective for data security also includes user security. For example in the case of secure communication where two users would like to communicate securely over an insecure network, each of them would first have to make sure that the other party is who he or she claims to be. Since the parties cannot see each other physically, user authentication has to be performed over the insecure network. Secondly, the parties would have to agree on some secret shared cryptographic session key for subsequent secure communication. Most practical user authentication schemes and key agreement schemes with user authentication are based on public key cryptosystems in contrast to symmetric key cryptosystems.

II. RELATED WORK

Peng Xu and Hai Jin proposed a new and efficient technique for the public key encryption using fuzzy keyword based concept [1]. Here in this paper an efficient framework is implemented for the security prevention against password guessing attack. The technique is known as PEKS (public key encryption with keyword search which is less efficient as compared to PEFKS (public key encryption with fuzzy keyword search). Here in this technique the encryption and decryption is performed on the basis of fuzzy keywords, where the user encrypts the message using the generated fuzzy keyword and forms a tupple and sends to the proxy server which is then access on the basis of keyword and decrypts using the public key.

Hur, Junbeom proposed Improving security and efficiency in attribute-based data sharing.

Attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the ciphertext encrypted under the CPABE algorithm. Additionally, as the user revocation can be done on each attribute level rather than on system level extra fine-grained user access control can be achievable.

This scheme features a key issuing mechanism that removes key escrow during the key generation. The user secret keys are produced through a secure two-party computation such that any curious key generation center or data-storing center cannot derive the private keys individually. Thus, this scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials. This scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the ciphertext policy attribute-based encryption. Therefore, this scheme achieves more secure and fine-grained data access control in the data sharing system. According to result obtained this scheme is efficient and scalable to securely manage user data in the data sharing system [2].

Yu, Shucheng et al [3] suggested Attribute based data sharing with attribute revocation. They explore a feasible solution based on novel cryptographic methods. Fig.2 shows semi-trustable proxy servers that are always available for providing various types of content services. The scenario provided here in this technique is based on the semi-trusted servers where the data are shared among various users and the authentication is provided using the attribute policies provided to each user in the network [3].

A. Sahai and B. Waters proposed Fuzzy Identity-Based Encryption. They present two constructions of Fuzzy IBE schemes. This construction can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. This IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. They prove the security of this scheme under the Selective-ID security model. They first introduced attribute based encryption (ABE) for encrypted access control. In an ABE system, both the user secret key and the ciphertext are associated with a set of attributes. Only if at least a threshold number of attributes overlap between the ciphertext and his secret key, can the user decrypt the ciphertext [4].

V. Goyal et al. [5] first introduced the concept of CP-ABE based on ABE. The main idea is to develop a much richer and secure type of attribute-based encryption cryptosystem. In this system each ciphertext is labeled by the encryptor with a set of expressive attributes. Each private key is connected with an access construction that specifies which type of ciphertexts the key can decrypt. They call such a idea a Key-Policy Attribute-Based Encryption (KP-ABE), since the access structure is specified in the private key, while the ciphertexts are simply labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if the attributes associated with a ciphertext satisfy the key's access structure. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [5].

Bethencourt et al [6] suggested Ciphertext-Policy Attribute Based Encryption. They provide the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) to address this problem, and give the first construction of such a scheme. In this system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in this system, they specify an associated access structure over attributes. A user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertexts access structure. At a mathematical level, access structures in our system are described by a monotonic "access tree", where nodes of the access structure are composed of threshold gates and the leaves describe attributes. They created a system for Ciphertext-Policy Attribute Based Encryption.

R. Ostrovsky et al [7] proposed Attribute-Based Encryption with Non-Monotonic Access Structures. They present a new Attribute-Based Encryption scheme where private keys can represent any access formula over attributes, including non-monotone ones. In particular, our construction can handle any access structure that can be represented by a Boolean formula involving AND, OR, NOT, and threshold operations.

They achieved this through a novel application of revocation methods into existing ABE schemes. In addition, the performance of our scheme compares very

favorably to that of existing, less-expressive ABE systems. An important goal in ABE systems is to create even more expressive systems [7].

Alfin Abraham et al [8] proposed survey of Identity-based encryption with efficient revocation. They propose a new way to mitigate the limitation of IBE with regard to revocation, and improve efficiency of the previous solution. They want to remove interaction form the process of key update, as keeping the PKG online can be a bottleneck, especially if the number of users is very large [8].

S. No.	Paper	Author / Year	Technique Used	Advantages	Issues
1	Improving Security and Efficiency in Attribute-Based Data Sharing [2].	Junbeom Hur	Here CP-ABE attribute based data sharing technique is used which solves key escrow problem and proxy encryption.	It provides an efficient technique of attribute based encryption which prevents from various attacks.	Cost ineffective and chances of security is less.
6	Attribute Based Data Sharing with Attribute Revocation [3].	Shucheng Yu, Cong Wang, KuiRen	Here CP-ABE based attribute policy is described along with the fine grained control of encryption.	The property of Proposed scheme is that it places minimal load on authority upon attribute revocation events.	Another direction for future work is to allow proxy servers to update user secret key without disclosing user attribute information.
4	Fuzzy Identity-Based Encryption [4].	Amit Sahai, Brent Waters	A Fuzzy IBE scheme can be applied to enabl encryption using biometric inputs as identities	It allows for error-tolerance between the identity of a private key and the public key used to encrypt a ciphertext.	An open problem is to build other Fuzzy-IBE schemes that use different distance metrics between identities.
5	Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data [5].	Vipul goyal, omkant pandey, amit sahai, brent waters.	Anew cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE).	Supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).	Less secure and prevention from various attacks.
7	Over encryption: Management of Access Control Evolution on Outsourced Data [9].	Sabrina De Capitani di Vimercati	Our proposal is based on the application of selective encryption as a means to enforce authorizations.	It protect the resource confidentiality from both unauthorized users as well as “honest but-curious” servers.	A huge number of resources of considerable size and that have to be distributed in a selective way to a variety of users.
2	A Survey on Attribute Based Encryption Scheme in cloud computing [10].	Minu George, Dr. C.Suresh Gnanadhas, Saranya.K	Here in this paper presented a survey on various attribute based encryption techniques.	The paper contains various attribute based encryption techniques to be used in cloud computing such as ABE, CP-ABE, and KP-ABE.	Computational cost and time as well as user revocation
3	Attribute-Based Encryption for Circuits from Multilinear Maps [11].	Sanjam Garg Craig Gentry Shai Halevi Amit Sahai Brent Waters	Here in this paper proposed a new technique for the attribute based encryption using the concept of Multilinear Maps.	Here the circuits are used for the generation of attributes through which the encryption is done. The construction is done for using multilinear maps.	The algorithm achieves both the features of Key-Policy and Ciphertext- Policy and hence the performance is better.

III. CONCLUSION

The paper describes various techniques implemented for the attribute based public key cryptography. Here in this paper a survey of various technique implemented for the search based public key cryptography so that on the basis of their various advantages and limitations a new and efficient technique is implemented in future.

REFERENCES

[1] Peng Xu and Hai Jin, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack", IEEE 2013.

[2] Hur, Junbeom. "Improving security and efficiency in attribute-based data sharing", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October 2013.

[3] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Attribute based data sharing with attribute revocation." In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270. ACM, 2010.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt '05), pp. 457-473, 2005.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proceedings of ACM Conference on Computer and Communication Security, pp. 89-98, 2006.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute Based Encryption," Proceedings IEEE Symposium Security andPrivacy, pp. 321-334, 2007.

[7] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryptionwith Non-Monotonic Access Structures," Proceedings ACM Conference Computer and Comm. Security, pp. 195-203, 2007.

[8] Alfin Abraham, Vinodh Ewards, Harlay Maria Mathew "A Survey on Optimistic Fair Digital Signature Exchange Protocols", International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, Vol. 3, No. 2, pp. 821 – 825, Feb 2011.

[9] Di Vimercati, Sabrina De Capitani, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. "Over-encryption: management of access control evolution on outsourced data." In Proceedings of the 33rd international conference on Very large data bases, pp. 123-134. VLDB endowment, 2007.

[10] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing", IJARCCE November 2013.

[11] Sanjam Garg Craig Gentry Shai Halevi Amit Sahai Brent Waters," Attribute-Based Encryption for Circuits from Multilinear Maps", 2012.[12] Kretzschmar, Michael, and Sebastian Hanigk. "Security management interoperability challenges for collaborative clouds." *In IEEE 2010 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management (SVM)*, pp. 43-49, 2010.

[12] Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee et al. "A view of cloud computing." *Communications of the ACM,* vol. 53, no. 4, pp. 50-58, 2010.

[13] Chaudhuri, Surajit, and Luis Gravano. "Evaluating top-k selection queries." *In VLDB, vol.* 99, pp. 397-410. 1999.

[14] Fagin, Ronald, Amnon Lotem, and Moni Naor. "Optimal aggregation algorithms for middleware", *Journal of Computer and System Sciences*, vol. 66, no. 4, pp. 614-656, 2003.

[15] Balke, Wolf-Tilo, and Werner Kießling. "Optimizing multi-feature queries for image databases." *In Proceedings of the International Conference on Very Large Databases*, 2000.

[16] Balke, W-T., Wolfgang Nejdl, Wolf Siberski, and Uwe Thaden. "Progressive distributed top-k retrieval in peer-to-peer networks." *In Proceedings of IEEE 21st International Conference on Data Engineering (ICDE 2005)*, pp. 174-185, 2005.

[17] Wang, Cong, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou. "Secure ranked keyword search over encrypted cloud data." *In Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, pp. 253-262. IEEE, 2010.

[18] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage" *Ieee Transactions On Computers*, VOL. 62, NO. 2, FEBRUARY 2013.

[19] Cao, Ning, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." *Parallel and Distributed Systems, IEEE Transactions on 25*, no. 1 (2014): 222-233, 2014.

[20] Wong, Wai Kit, David Wai-lok Cheung, Ben Kao, and Nikos Mamoulis. "Secure kNN computation on encrypted databases." *In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, pp. 139-152, 2009.

[21] Hussain Abo Surrah, "Multi Keyword Retrieval On Secured Cloud" *Asian Journal of Technology & Management Research*, ISSN: 2249 –0892, Vol. 04, Issue – 01, Jan - Jun 2014.

[22] Stephen S. Yau, Fellow And Yin Yin "A Privacy Preserving Repository For Data Integration Across Data Sharing Services", *IEEE Transactions On Services Computing*, Vol. 1, No. 3, July-September 2008.

[23] T. Wood et al., "Black-Box and Gray-Box Strategies for Virtual Machine Migration," *Proceedings of Fourth USENIX Conf. Networked Systems Design and Implementation (NSDI '07)*, pp. 17-17, 2007.

[24] Clark, Christopher, Keir Fraser, Steven Hand, Jacob Gorm Hansen, Eric Jul, Christian Limpach, Ian Pratt, and Andrew Warfield "Live migration of virtual machines", *In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation*,Vol. 2, pp. 273-286, 2005.

[25] Liu, Haikun, Hai Jin, Cheng-Zhong Xu, and Xiaofei Liao "Performance and energy modeling for live migration of virtual machines", *Cluster computing*, vol. 16, no. 2, pp. 249-264, 2013.

[26] Greveler, Ulrich, Benjamin Justus, and Dennis Loehr. "A Privacy Preserving System for Cloud Computing." *In IEEE 11th International Conference on Computer and Information Technology (CIT- 2011)*, pp. 648-653, 2011.

[27] Mishra, Ranjita, Sanjit Kumar Dash, Debi Prasad Mishra, and Animesh Tripathy. "A privacy preserving repository for securing data across the cloud." *In IEEE 3rd International Conference on Electronics Computer Technology (ICECT-2011)*, vol. 5, pp. 6-10, 2011.

[28] Mishra, Ranjita, Sanjit Kumar Dash, Debi Prasad Mishra, and Animesh Tripathy. "A privacy preserving repository for securing data across the cloud." *In IEEE 3rd International Conference on Electronics Computer Technology (ICECT-2011)*, vol. 5, pp. 6-10, 2011.