International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 3218 – 3220

Analysis of Cryptographic Techniques for Attribute based Data Sharing

Ms.Kavita Patil
Department of Information Technology
Vidyalankar Institute of Technology
Mumbai, India
patil.kavita121@gmail.com

Prof. Vidya Chitra
Department of Information Technology
Vidyalankar Institute of Technology
Mumbai, India
vidya.chitra @vit.edu.in

Abstract— Now a day's most of the people move their data to cloud services due to which it saves enormous cost. But they are taken aback due to one main reason "Security". The vulnerabilities of cloud storage are extremely high, even the leading service providers have been compromised at some point .This paper is focusing on various modern techniques like key policy attribute based encryption, Ciphertext policy attribute based encryption, Hierarchical attribute based Encryption are discussed. So that it will be helpful for us to provide more security against vulnerabilities in cloud storage that are identified to be exploited.
Keywords- *Ciphertext, Security, vulnerability, Encryption, cryptographic, attribute based encryption*

*****

I. INTRODUCTION

Over the Internet, Cloud computing is the delivery of computing services. Cloud services allow businesses and individuals to use software and hardware that are managed by third parties at remote locations [1]. The Examples of cloud services includes online file storage, social networking sites, webmail, and online business applications [1]. So, the massive number of peoples is moving their data to a cloud. But Storing there data on untrusted storage like icloud makes faced challenging issue instead of providing ease of secure data and sharing of data. Cloud service provider must be provides the security and belief, as there is more valuable and sensitive data in huge number of amount stored on the clouds. There are fears about flexibility, scalability, fine grained access control in the cloud computing. To resolve these issues various cryptographic methods are addressed.

II. LITERATURE SURVEY

In cloud computing, various different existing schemes are there which provides data protection, data secrecy and access control.

1) IBE:

In the year of 1998,Adi Shamir introduces concept of Identity based encryption. It is an old approach. These scheme replaces public key infrastructure. The data owner does not lookup [7] for the public key certificate of receiver. The Key management is simplifies by IBE. For closed groups of users this scheme is best. This scheme is based on public key cryptosystem. In IBE, for generation of public key, user chooses his own name and network address instead of generating random pair of public key /secret key and declare one of them as private key for encryption previously.

Advantages:

1. In this, recipient's public key is derived from his identity that's why it does not require certificates.
2. If Keys are expired, then they don't require to be revoked.
3. For future decryption it enables postdating of messages

Disadvantages:

1. The private key generator has a demanding task in a large network.
2. It requires a centralized server.
3. For transmission of private key it require IBE server as well as in between sender and receiver It needed secure channel.

2) ABE:

ABE is the First cryptographic approach proposed by Vipul Goyal, Pandey Amit and Sahaiz Brent Waters with fine grained data access. It provides method to describe access policy based on different attribute. In this system user key's and cipher text associated with set of descriptive attributes and particular key can decrypt a particular cipher text if there is match between the attributes.

Disadvantages:

1. it can be selectively shared only coarse grained level that means private key shared with another party.

3)THRESHOLD ABE :

The Sahai and Waters proposed the Threshold ABE system for error tolerant identity based encryption scheme in which ciphertext is associated with set of attributes S and user private key associate with both threshold parameter and another set of attribute. In order to decrypt a ciphertext at least k attribute overlapped with cipher text and private keys.

Disadvantages:

1.Threshold semantic are not expressive.

4)KEY-POLICY ATTRIBUTE–BASED ENCRYPTION:

This new encryption technique is proposed by Vipul Goyal in 2006 called as Key Policy Attribute Based Encryption (KP-ABE). In this system cipher text is associated with set of attributes and private key is associated with access structure with the aim of specify. The key policy Attribute based encryption allow user who wants to decrypt ,for decryption of the ciphertext only when at least k attributes should be overlapped between ciphertext and key structure. In the Key policy Attribute based encryption system also define scheme known as secret sharing scheme of data where the access structure involved threshold gate Shamir and Balkley first time proposed the secret sharing scheme and in which if two or more parties come together they can create secret. The secret sharing scheme specify tree access structure where interior node consist of AND & OR gate and leaves consist different

parties. Any set of parties that satisfy the tree come together and reconstruct secret. In this system the user key is associated with access Structure tree and leaves are associated with attributes. The user could decrypt ciphertext if attributes associated with ciphertext satisfies key access structure.

5) CIPHERTEXT-POLICY ATTRIBUTE BASED ENCRYPTION

Ciphertext-policy ABE (CP-ABE) proceeds in the dual way, by assigning attribute sets to private keys and letting senders specify an access policy that receivers' attribute sets should comply with[2].

CPABE has design new access scheme for ubiquitous learning system based on cloud computing. CP-ABE enables encryptor to define attribute set over a universe of attributes that decryptor requires to possess in order to decrypt the ciphertext. Thus the different set attributes is permitted to decrypt data based on security policy. CPABE has attracted much attention to design new access [8] scheme for ubiquitous learning system based on cloud computing.

Advantages:

1.CP-ABE enables public key based one -to - many encryption ,where differential yet flexible access rights can be assign to individual user. So, CP-ABE provides a new way for solving access control in the cloud based ubiquitous learning system.

Disadvantages:

1. The Length of cipher text is depends on the number of attributes.

6) HIBE:

HIBE is nothing but hierarchical IBE. In 2-HIBE scheme, three types of entities are there. first one is the root PKG, who acquire a master key. At upper level, there are domain PKGs, who can request their domain key from the root PKG. At the end, from their domain PKG, users are there, they knows how to request a private keys from its PKGs domain. By permitting subdomains,[9] subsubdomains, and hence Forth, We are able to generalize to HIBE schemes by obtaining more levels. There are various Applications of HIBE systems first is for portable computing [12] devices it is generating short-lived keys and second most important benefit is, total collusion resistance at the upper level and partial collusion resistance at the lower level .

Advantages of an HIBE system over standard PKI:

1. Senders can derive the recipient's public key from their address without an online lookup.
2. It reduces the amount of required storage and the complexity of the access right management.

Disadvantages of HIBE:

1. It increases demand in key management and transfer.
2. HIBE scheme can be expensive in terms of performance. This could become a problem when a client employs a computationally weak device for accessing information

7)FIBE:

Amit Sahai , Brent Waters introduces Fuzzy Identity Based Encryption. Fuzzy IBE scheme can be applied to enable encryption. For this, it uses biometric inputs like identities. A user's Identity consist of a set of biometric attributes. For [10] each attribute, a user receives a private key in its identity. Fuzzy IBE scheme provides one important property know as error tolerance. Error tolerance property is used to differentiate private key and [11] public key identities used for encryption. This property precisely allows for the use of biometric identities and it has some noise. So for this each time it is sampled.

Advantages:

1. To fit it fuzzy IBE model, it does not require additional public key infrastructure.
2. Server does not need to store the clients identity after generating the cipher text.
3. It limits the vulnerability window to be compromised.
4. By using its own private key, client communication become more secure.
5. FIBE does not rely on shared key with server's security.

Disadvantages:

1. It is interactive.
2. It requires two rounds of additional communication overhead to perform decryption.

III. CONCLUSION

This Paper presents various encryption techniques which are needed to improve the security in the data sharing system. This paper consist of basic encryption schemes as well as advance encryption scheme. Also their advantages and disadvantages are also mentioned here. The future scope of our paper will be detailed implementation of proposed methodology to overcome the drawbacks of existing system .

REFERENCES

[1]]Fact sheet: https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf
[2] Goyal,V.Pandey, O., Sahai,A., Waters,B.(2006) "Attribute based encryption for fine grained access control of encrypted data", ACM Conference on Computer and Communication Security, pp. 89-98.
[3] D.F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in *15th National Computer Security Conference*, 1992
[4] Zhibin Zhou and Dijiang Huang," On Efficient Ciphertext- Policy Attribute Based Encryption and BroadcastEncryption", Arizona State University, pp.1-19
[5] Nuttapong Attrapadung1, Javier Herranz, Fabien Laguillaume3, Beno^_t Libert4,Elie de Pana_eu5, and Carla R_afols2 " Attribute-Based Encryption Schemes with Constant-SizeCiphertexts", pp. 1-15, 2011.
[6] Nuttapong Attrapadung1, Beno^_t Libert2?, and Elie dePana_eu3," Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts", pp.1-18
[7] Adi Shamir," identity based cryptosystems and signature schemes ", the Weizmann institute of secience isarael, 1998. Pp.47-53.
[8] Ling Yu, Bo Chen, Ning Wang," context-aware access control for resources in the ubiquitous learning system using ciphertext-policy attribute-based encryption".

[9] Jeremy Horwitz and Ben Lynn," Toward Hierarchical Identity-Based Encryption", Stanford University, Stanford, CA 94305, USA
[10] Jonathan kirsch, "Towards key-privacy in a Fuzzy Identity based Encryption Scheme", Spring 2005, Johns Hopkins University
[11] Amit Sahai, Brent Waters," Fuzzy Identity-Based Encryption", pp.1-15
[12] Urs Hengartner† and Peter Steenkiste," Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information", First
[13] International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)0-7695-2369-2/05 $20.00 © 2005 IEEE