International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Privacy and Shoulder Surfing Attack Preserving Anonymous Attribute Based Encryption Scheme

Shital S.Salokhe[1], N. N. Patil[2]

[1]PG Student, Ashokrao Mane group of institution, Vathar
[2]Associate Professor, Ashokrao Mane group of institution, Vathar

---

Abstract Cloud services provide great opportunity for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. Several schemes have been proposed for access control of outsourced data in cloud computing. Despite the tremendous benefits, security is the primary obstacle that prevents the wide adoption of this promising computing model. Identity-based encryption (IBE) is the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. In the KP-ABE, a ciphertext is associated with a set of attributes, and a private key is associated with a monotonic tree, which describes this user's identity. A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. However, the encrypter does not have entire control over the encryption policy. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation. All problems and overhead are solved in the CP-ABE. In this, ciphertexts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. Hence the encrypter holds the encryption policy. Also, issued private keys will not be modified till the whole system reboots.

Index Terms— Cloud computing, shoulder surfing, privacy preserving, anonymous attribute based encryption.

I. INTRODUCTION

Now a day's focus on the authentication to realize that a user's private data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the users privacy. The existing systems define shared authority based privacy-preserving authentication protocol which allows security and privacy in the cloud storage. Shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations. Attribute based access control is adopted to realize that the user can only access its own data fields; proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. All problems and overhead are solved in the CP-ABE. In this, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. Hence the encrypter holds the encryption policy. Also, issued private keys will not be modified till the whole system reboots.

II.RELETED WORK

Techo Jung, Xiang-Yang. [1], proposed a semi-anonymous attribute-based privilege control scheme AnonyControl and fully-anonymous attribute-based privilege control scheme Anony Control-F to address the user privacy problem in a cloud storage server. In this paper author proposed schemes achieve not only fine-grained privilege control but also identity information.
Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahammad, and Ataullah Ghafoor. [6], proposed a Attribute-Based Encryption(ABE) is public key cryptographic technique that works in a one-to-many fashion and is also called fuzzy encryption. Public key encryption methods store encrypted data on third party servers, while distributing decryption keys to authorized users.
L. A. Dunning and R. Kresman. [14],Trusted third party an optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration.

Jain Zhao, Haiying Gao and Junqi Zhang. [15], proposed Key-Policy Attribute-Based Encryption (KP-ABE) scheme for circuit of any arbitrary polynomial on lattices, and prove that the scheme is secure against chosen plaintext attack in the selective model under the Learning With Errors(LWE) assumption.

Cong Wang, Qian Wang, Kui Ren and Wenjing. [17], we address the above-mentioned privacy issue to propose privacy preserving authentication protocol for the cloud data storage, based on cloud storage which gives authentication and authorization without conceding private information.

III.PROPOSED WORK

Architecture of Privacy and Shoulder Surfing Attack Preserving Anonymous Attribute Based Encryption Scheme is shown in Figure 1.

A. System Architecture

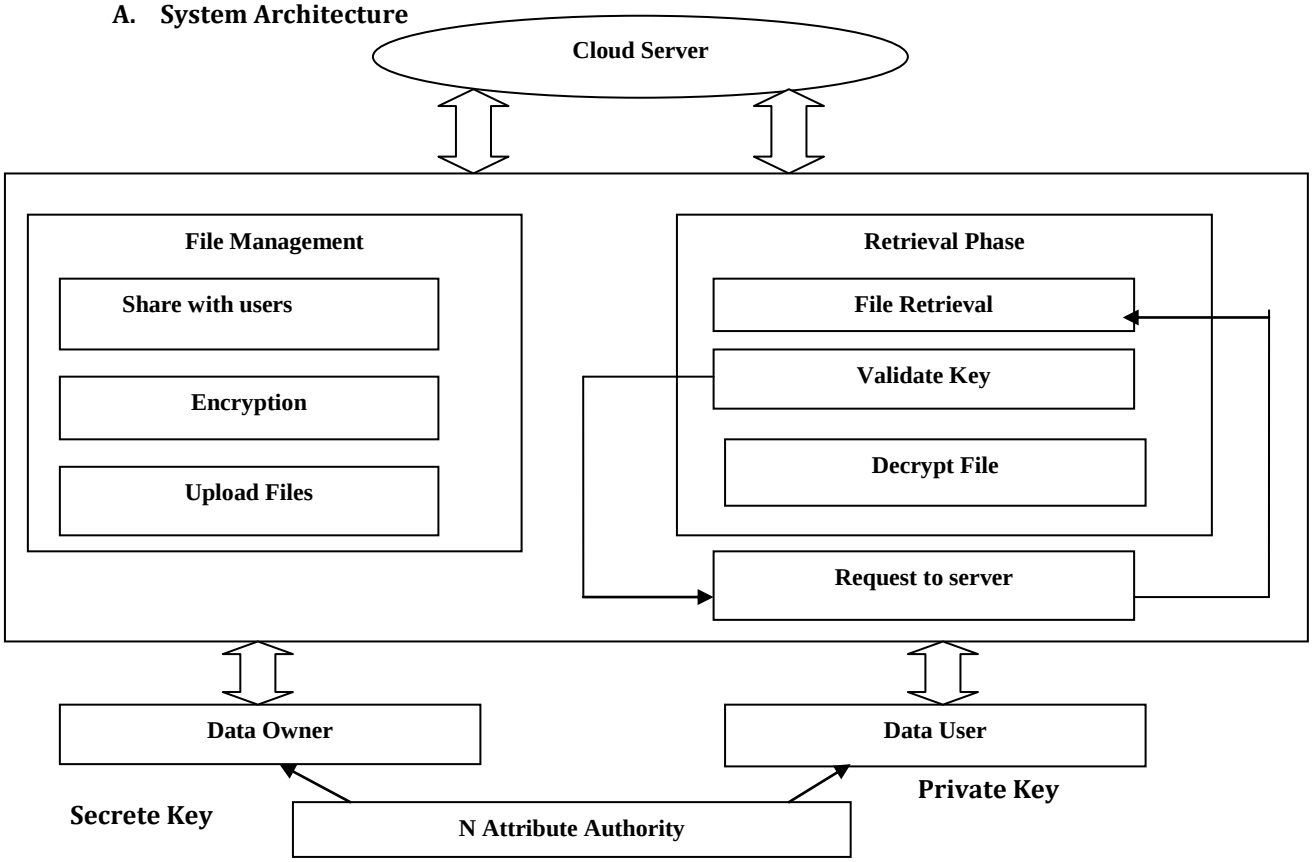

Fig 1: Architecture of Privacy and Shoulder Surfing Attack Preserving Anonymous Attribute Based Encryption Sche

The proposed architecture consists of four modules.

1. File Management

Encryption algorithm takes as input the public key PK, a message M, and set of privilege trees $\{T_p\}_{pe\{0,....,r-1\}}$,by where r is determined by the encrypter. It will encrypt the message M and returns a ciphertext CT and verification set VR so that the user can execute specific operation on the ciphertext if and if only his attribute satisfy the corresponding privilege tree T_p privilege to read the file.

2. Shoulder Surfing

Shoulder surfing is direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing will be provided within the system with attribute based encryption.

3. Data De-duplication

De-duplication will be added where the server will store only a single copy of each file, regardless of how many users asked to store that file, depending upon the disk space of cloud servers.

4. File Retrieval

In this module, Decryption will be used at file controlling (e.g. reading, modification, and deletion). It takes as input the public key PK, a ciphertext CT, and a private key SK_u, which has a set of attributes A^u and corresponds to its holder's GID_u. A^u satisfies any tree in the set $\{T_p\}_{pe\{0,....,r1\},}$ the algorithm returns a message M or a verification parameter.

V. CONCLUSION

In this paper we study anonymous attribute based encryption and proposed a new system shoulder surfing. Attribute based access control is adopted to realize that the user can only access its own data fields; proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. , cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext.

REFERENCES

[1] Techo Jung, Xiang-Yang, "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous attribute-Based Encryption", IEEE Transaction 2015.
[2] M satish kumar, B Uday Kumar, Ch. Arun Kumar, "Attribute Based Data Sharing with Attribute Revocation to Control Cloud Data Access", International Journal of Computational Science, Mathematics and Engineering, February-2016.
[3] Praveen N.R and Renju Samuel, "Enhanced Efficient User Revocation Mechanism on Top of Anonymous Attribute Based Encryption", International Journal of Emerging Technology in Computer Science & Electronics, AUGUST 2016.
[4] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing, National Institute of Standards and Technology", USA, 2009.
[5] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges", IEEE Communications Magazine, vol. 50, no.9, pp, 24-25, 2012.
[6] Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahammad, and Ataullah Ghafoor, "Analysis of Classical Encryption Techniques in Cloud Computing", ISSN 1007-0214 09/10 pp102-119 Vol. 21, Number 1, February 2014.
[7] K. Hwang and D. Li,-Trusted Cloud Computing with Secure Resources and Data Coloring, IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.
[8] J. Chen, Y. Wang, and X. Wang,-On-Demand Security Architecture for Cloud Computing, Computer, vol. 45, no. 7, pp. 73-78, 2012.
[9] Y. Zhu, H. Hu, G. Ahn, and M. Yu,-Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.
[10] H. Wang-Proxy Provable Data Possession in Public Clouds, IEEE Transactions on Services Computing,[online] ieeexplore.ieee.org 2012.
[11] Ming Li, Shucheng Yu, Yao Zheng,-Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, 2013.
[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li,-Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp.847-859, 2011.
[13] C. Wang, K. Ren, W. Lou, J, Lou,-Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, vol. 24, no.4, pp.19-24, 2010.
[14] L. A. Dunning and R. Kresman,- Privacy Preserving Data Sharing With Anonymous ID Assignment, IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.
[15] Jain Zhao, Haiying Gao and Junqi Zhang, -Attribute-Based Encryption for Circuits on Lattices, ISSN 1007-0214 05/13 pp463-469 Vol. 19, Number 5, October 2014.
[16] Xinhua Dong, Ruixuan Li, Heng He, Wanwan Zhou, Zhengyuan Xue and Hao Wu,-Secure Sensitive Data Sharing on a Big Data Platform, ISSN 1007-0214 08/11 pp72-80 Vol. 20, Number 1, February 2015.
[17] Allim Swami, -Privacy Preserving Data Sharing With Anonymous ID Assignment Using AIDA Algorithm, IJCERT, Vol. 1, Issue 1, PP 23-29, July 2014.