International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

MEDICAL DATA PRIVACY USING CLOUD COMPUTING

Satheesh Kumar S[1], Vigneshkumar A[2]

[1]*Post Graduate in Computer Science and Engineering, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, India*
[2]*Associate Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, India*

Abstract - In most existing schemes, there's only one authority in the system that authority issue all the public keys and private keys, which incurs cipher text size,In encryption and decryption operations there will be computation costs rely a least linearly on the number of attributes involved in the access policy. We counseled an efficient multi-authority CP-ABE scheme in which there is no interact of authorities to generate public information while system initialization phase. Our scheme provide constant cipher text length and a constant number which pairing computations. Scheme can be proven CPA-secure in random oracle model under the decision q-BDHE assumption.There is user's attributes revocation,when it occurs the scheme transfers most re-encryption work to the cloud service provider, it reducing the data owner's computational cost on the premise of security. Finally the analysis and simulation result show that the schemes proposed in this thesis ensure the privacy and secure access of sensitive data stored in the cloud server, and be able to cope with the dynamic changes of users' access privileges in large-scale systems. Besides, the multi-authority ABE eliminates the key escrow problem, achieves the length of cipher text encryption and decryption

Key Words: q-BDHE, CPA-Secure, Ciper text..

1. INTRODUCTION

Data owner outsource their data to the cloud in cloud computing service then it provide the data access to the users. The data access service and new data escrow mode separates the data owner from the role of data provider. The data owner and the client won't have an immediate association in the arrangement of data service.Then again, the data owner stores the sensitive information in the cloud server for proficiency and economic benefit, then again, the owner needs to ensure data confidentiality if there should arise an occurrence of being taken in the new service model. Access control, which is an important method of realizing user data confidentiality and privacy protection in cloud computing, can protect resources from an unidentifiable system and the unauthorized users because it grants access rights to certain users and forbids other users to access the data. A feasible solution is to encrypt the data by a specific encryption technology in local, and then submitted the ciphertext to the cloud storage, the decryption key is only distributed to the authorized users. The unauthorized users and the cloud server can not decrypt the ciphertext because they have no decryption key. This method has been widely adopted in some existing schemes which store sensitive data on unreliable servers. Although the method can provide secure access control, but in order to provide different roles or users with different access services according to the access policy, the data files need to be encrypted by different keys. The key management becomes very complex when the number of users in the system increases. In addition, the system needs to backup different ciphertexts according to authorized users with different decryption keys. In this case, the cost of storage and computing brought by the ciphertext and the keys has a linear relation with the number of users in the system. Therefore, how to obtain the fine-grained, scalability and data confidentiality without introducing high complexity of key management and data encryption is still a problem faced by the data access control in cloud computing.

2. RELAED WORK

In the basic CP-ABE [1-3] schemes, the size of the ciphertext increases linearly with the number of attributes in access policy. For example, the size of ciphertext is $n+O(1)$ in [1] and $2n+O(1)$ in [2]. In addition, the number of pairing operation is also linearly with the number of attributes in access policy during decryption, which increases the computation overhead on receiver. These limit the usage of ABE in real life applications to a large extent, especially for the scenarios where bandwidth issues and computing resources are of great importance.

Memon, I., Memon, H proposed (2017) an efficient user based authentication protocol [3] for location based services to secure address configuration for IPv6-based mix-zones over the road network. This protocol authenticates to scrutinize vehicles actions confidentially and have the following characteristics (1) Anonymous authentication: a message issuer can be authenticated. (2) Privacy: Communication content is confidential. The cost must be condensed through the address configuration scheme to improve the scalability. (3) Efficiency: it attains rapid message verification, low storage requirements, and in case of a dispute, provides cost efficient identity tracking. Vehicles movement, the distinction of velocity and distance are considered to maintain as many common users as possible by reducing the cost. The performance assessment and cost analysis show that our framework can reduce the cost and gain outperformed results. This model can

accomplish reliability and efficiency with packet rate information. This user legitimate key establishment protocol has comparatively shorter time response, diminishes cost, less packet loss information and enhanced privacy preservation against malicious attacks compared with existing methods.

Shubhra Rana, Dr. P. anthi Thilagam (2014) proposed a novel mechanism for performing PPDARM [5] on horizontally distributed databases. Pattern Count tree structure has been used to improve the scalability of the DARM algorithm as PC tree requires only one scan for construction and provides a compact and complete representation of the database. Paillier cryptosystem used for additive homomorphic properties leaks negligible information about the private data. The HHE scheme enhances the scalability of the PPDARM approach by using a tree aggregation structure which minimizes the number of messages exchanged. The proposed scheme can be extended to be secure under a malicious adversarial assumption. Key generation mechanism can be made more robust by including Zero Knowledge Proof mechanisms and allowing distributed key generation.

Lin, C.W., Hong, T.P., Yang, K.T., et al (2015)GA-based framework with two optimization algorithms [10] is proposed for data sanitization. A novel appraisal function with three apprehensive factors is designed to find the appropriate transactions to be deleted in order to hide sensitive itemsets. Experiments are then conducted to evaluate the performance of the proposed GA-based algorithms with regard to different factors such as the execution time, the number of hiding failures, the number of missing itemsets, the number of artificial itemsets, and database dissimilarity.

Cheng, P., Roddick, J.F., Chu, S.C., et al (2016) another twisting based technique [10] is proposed which shrouds touchy guidelines by expelling a few things in a database to decrease the keep up or certainty of delicate standards underneath indicated limits. So as to lessen symptoms on data, the data on non-delicate item sets contained by every exchange is utilized to sort the supporting exchanges. The applicants that contain littler amount non-touchy itemsets are chosen for change ideally. So as to diminish the twisting degree on information, the base number of exchanges that should be adjusted to hide a delicate guideline is determined. Similar tests on certifiable datasets demonstrated that the new technique can accomplish palatable outcomes with less reactions and information misfortune.

2.1 **PROPOSED METHODOLOGY**

2.1.1 **Advanced encryption standard algorithm**: The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cyber security and electronic data protection.

The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce cipher text. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 258-bit key size has 14 rounds.AES is the Advanced Encryption Standard, a standard for cryptography that is used to encrypt data to keep it private. AES is a symmetric, block cipher which means that blocks of text of a certain size (128 bits) are encrypted, as opposed to a stream cipher where each character is encrypted one at a time.

2.1.2 **Cryptography algorithm :**Cryptographic algorithms are used for important tasks such as data encryption, authentication, and digital signatures, but one problem has to be solved to enable these algorithms: binding cryptographic keys to machine or user identities. Cryptographic algorithms are the most frequently used privacy protection method. Many cryptographic tools have been applied in practice. Unfortunately, traditional encryption mechanisms with overly computational complexity cannot meet the new requirements for smart applications, especially for those systems that consist of many resource-constraint devices. Consequently, how to develop lightweight yet effective encryption algorithms is of significant practical value.

The main challenge in designing an attribute based encryption algorithm is to prevent against attacks from colluding users. In the CP-ABE, the secret sharing value s is embedded into the Cipher text.

2.1.3 Encryption algorithm:

The encryption algorithm takes as input a message M, an access structure and the W corresponding to the involved attributes in PK. It outputs the cipher text CT. We assume that the cipher text implicitly contains the access structure W.Cryptanalyst's goal is to derive keys used to encrypt or the encryption algorithm, and decrypt any new messages encrypted with that key.

The encryption algorithm encrypts a message under the access structure. The algorithm first selects a random number and aggregates all the public key elements corresponding to the attribute values for each.

2.1.4Decryption algorithm:

The algorithm takes as input the cipher text CT which contains an access structure W and the user's global identity GID. If the set of attributes L access structure W then the algorithm will decrypt the cipher text and return the message *M*, or it outputs. The decryption algorithm

aggregates the private key elements corresponding to the attribute values in *W* to generate.

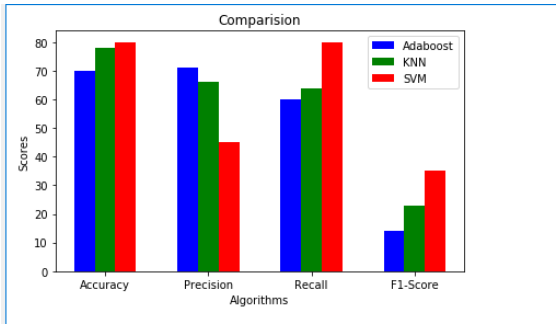

Fig1:Algorithm comparision

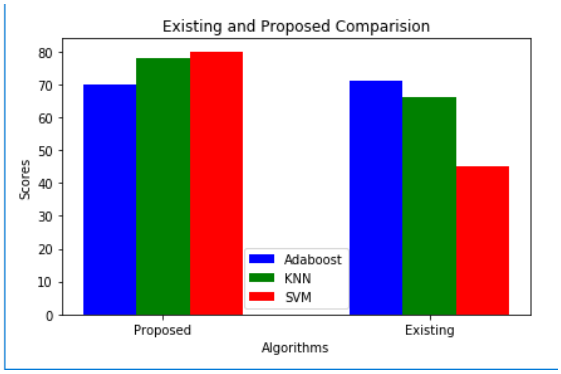

Fig2: Comparision of KNN and SVM

3. CONCLUSIONS

In this paper, we present a CP-ABE access control for multi-authority systems with constant size cipher text in cloud computing. Both the length of cipher text and the number of pairing operations in decryption are constant and independent of the number of attributes involved in the access structure, which reduce the communication and computing cost of the system. Additionally, the application of multi authorities solves the key escrow problem in the single authority system. The security of our scheme can be proven CPA-secure in random oracle model under the decision q-BDHE assumption. When the revocation happens, most of the heavy computational tasks are shifted from the owner to the cloud without revealing the secret information to the cloud thanks to proxy re-encryption, such that it can eliminate the huge communication overhead between data owners and cloud server, and the heavy computation cost on data owners.

REFERENCES

[1] Goyal V, Pandey O, Sahai A, et al. "Attribute-based encryption for fine-grained access control of encrypted data," Proc. Thirteenth ACM Conference on Computer and Communications Security, pp. 89-98, 2006.

[2] Bethencourt J, Sahai A, and Waters B, "Ciphertextpolicy attribute-based encryption", Proc. IEEE Symp. Security and Privacy (SP'07), pp. 321-334, May. 2007, doi:10.1109/SP.2007.11.

[3] Waters B, "Ciphertext-policy attribute-based encryption: An expressive, ef cient, and provably secure realization," Public Key Cryptography— Fourteenth International Conference on Practice and Theory in Public Key Cryptography, D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, eds., Lecture Notes in Computer Science F6571, International Association for Cryptologic Research, pp. 53-70 2011.

[4] Emura K, Miyaji A, and Nomura A, "A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length," Information Security Practice and Experience—Fifth International Conference, F. Bao, H. Li and G. Wang, eds., Lecture Notes in Computer Science F5451, Berlin: Springer-Heidelberg, pp. 13-23, 2009.

[5] Herranz J, Laguillaumie F, and Ràfols C, "Constant size ciphertexts in threshold attributebased encryption," Public Key Cryptography— Thirteenth International Conference on Practice and Theory in Public Key Cryptography, P.Q. Nguyen and D. Pointcheval, eds., Lecture Notes in Computer Science F6056, International Association for Cryptologic Research, pp. 19-34 2010.

[6] Attrapadung N, Libert B, and Pana eu E.D, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," Public Key Cr yptography—Fourteenth International Conference on Practice and Theory in Public Key Cryptography, D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, eds., Lecture Notes in Computer Science F6571, International Association for Cryptologic Research, pp. 90-108 2011.

[7] Chen Cheng, Zhang Zhenfeng, and Feng Dengguo, "Efficient ciphertext policy attributebased encryption with constant-size ciphertext and constant computation-cost," Provable Security—Fifth International Conference, X. Boyen, and X. Chen, eds., Lecture Notes in Computer Science F6980, GmbH Berlin: Springer-Verlag, pp. 84-101 2011.

[8] Cheung Land Newport C, "Provably secure ciphertext policy ABE," Proc. Fourteenth ACM Conference on Computer and Communications S e c u r i t y (CC S ' 0 7) , p p . 4 5 6 - 4 6 5 , 2 0 0 7 , doi:10.1145/1315245.1315302.

[9] Doshi N and Jinwala D, "Constant Cipher text Length in CP-ABE," IACR Cryptology ePrint Archive, 2012, 2012: 500.

[10] Ge Aijun, Zhang Rui, and Chen Cheng, "Threshold cipher text policy attribute-based encryption with constant size ciphertexts,"Information Security and Privacy—Seventeenth Australasian Conference, pp. 336-349, 2012, doi:10.1007/978- 3-642-31448-3_25.