International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

Privacy Preserving Attribute Based Keyword Search in Shared Multi Owner Setting

M. Anantha Lakshmi [1], V.Amrutha[2], M. Ravali[3], S. Jyoshna[4], M. Harini Sree [5]

Assistant Professor, Department of Computer Science & Engineering, Ravindra College of Engineering for Women, Kurnool, Andhrapradesh, India[1]

Students, Department of Computer Science & Engineering, Ravindra College of Engineering for Women, Kurnool, Andhrapradesh, India[2,3,4,5]

ABSTRACT: Cipher text-Policy Attribute-based keyword search (CP-ABKS) makes search queries simpler and supports robust access control of cloud encrypted data. Prior CP-ABKS systems, however, were designed to support unshared multi-owner setting, and can not be implemented directly in the shared multi-owner setting (where each record is certified by a fixed number of data owners), without incurring high computational and storage costs. Additionally, most existing schemes are vulnerable to off-line keyword-guessing attacks if the keyword space is of polynomial size due to privacy concerns on access policies. Additionally, when more than one data user has the same subset of attributes, it is difficult to identify malicious users who leak the secret keys. In this paper, we present in Shared Multi-owner setting (basic ABKS-SM system) a privacy-preserving CP-ABKS system with hidden access policy, and show how it is improved to support malicious user tracing (modified ABKS-SM System). We then prove that in the generic bilinear group model, the proposed ABKS-SM systems achieve selective security and resist the off-line keyword-guessing attacks.

KEYWORDS: Advanced Encryption Standard, Data Encryption Standard, Third Party Administrator.

I. INTRODUCTION

CLOUD [1],[2] is commonly used, by individuals and organizations (including government bodies) for example for the storing and processing of large quantities of data, usually encrypted before outsourcing (e.g. text, image, and video)[3], [4] and [5]. SE schemes [6] allow data users to search and selectively retrieve interest records over encrypted (cloud-excluded) data, in compliance with user specific keywords.

Nevertheless, when managing encrypted data outsourced to the cloud, there are other attractive properties. Of example, traditional encryption methods are limited when encrypting a large data volume because of several copies of cipher texts (e.g. public key encryption schemes) and difficult and expensive key management (e.g. symmetrical encryption schemes). Cipher Text Policy Attribute-based Encryption (CP-ABE) schemes are designed to ease these limitations as well as to improve multi-user access permissions and to enable one-to-one encryption.

However, in standard CP-ABE schemes, an access policy in plaintext is associated with a cipher text may result in leakage of sensitive information. For example, in an e-health system, hospital A encrypts a patient's electronic medical record (EMR) using CP-ABE with an access policy, such as ("ID: 1788" AND "Hospital: Hospital A") OR ("Doctor: Cardiologist" AND "Hospital: Hospital B") – see Fig. 1. Hence, one can easily infer from the user attribute set ("Cardiologist"," Hospital B") that patient ("ID: 1788") in Hospital A likely suffers from a heart condition. Such privacy leakage is clearly not appropriate, particularly if the medical condition is more sensitive (e.g., sexually transmitted diseases such as chlamydia, gonorrhea, and human papilloma virus infections). In addition, medical organizations are subject to exacting regulatory oversight in most developed jurisdictions. Hence, there have been efforts to design CP-ABE scheme with hidden access policies.

There have also been efforts to design schemes that allow a data owner to delegate his/her search capability in a fine grained manner, which allows other data users to search, retrieve and decrypt encrypted data of interest. Examples include Cipher text-Policy Attribute-Based Keyword Search IEEE Transactions on Dependable and Secure Computing. However, in many applications, data records are co-owned by a number of data owners, rather than a single data owner. That is to say, each file is encrypted by multiple data owners, and the data user can access the file, if and only if, he/she obtains authorizations from several data owners. For example, the EMR for a certain patient is controlled by multiple departments (e.g., clinical departments such as infectious diseases and psychiatry) and/or

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

medical organizations (e.g., San Antonio Behavioral Healthcare Hospital, Texas Center for Infectious Disease, and Texas Infectious Disease Institute).

Deploying CP-ABKS schemes [15], [16] in the unshared multi-owner setting (where multiple data owners manage different data records) incur significant computational and storage costs. Another realistic, but more complex, setting is the shared multi-owner setting, where each record is co owned by multiple data owners. The differences between unshared multi owner setting and shared multi-owner setting are described . We formally prove that the basic and modified ABKSSM systems guarantee the security of shared data and access policies, achieve selective security, and resist off-line keyword guessing attack in the generic bilinear group model. We also demonstrate performance1 of the basic ABKS-SM system using experiments on real-world datasets.

II. EXISTING MODEL

CP-ABE was designed to allow fine-grained access control over cipher texts, and CP-ABKS was designed to support both fine-grained access control and keyword search simultaneously. For example, Zheng et al. [25] presented the CP-ABKS scheme that enables data owners to grant fine-grained search permissions, Sun et al. [16] presented an owner-enforced CP-ABKS scheme that supports user revocation and is shown to be selectively secure against chosen-keyword attack. However, the computational costs of these two schemes grow linearly as the number of system attributes increases. This is not scalable in practice. To minimize computational costs and cipher text size required in such schemes, Li et al. [26] implemented a keyword search function in attribute-based encryption (ABE) scheme, by outsourcing key-issuing and decryption operations. Donget al. [27] also designed an efficient CP-ABKS scheme via an online/offline approach when considering resource constrained mobile devices.

One serious limitation of CP-ABE schemes is that the access policy embedded in the cipher texts may leak sensitive information to authorized data users, as discussed in the preceding section. Thus, Nis hide et al. [28] constructed amore practical CP-ABE scheme, which allows the encryptorto use wildcards to represent certain attributes in a hidden solution. Similarly, Phuong et al. [14] proposed a hidden access policy scheme, which supports AND-gate with wild card by utilizing inner product encryption. These prior CPABE schemes with partially hidden access policy have high computational costs and do not support keyword search over encrypted data.

To resist off-line keyword-guessing attacks, Qiu et al. [29] presented a secure CP-ABKS scheme supporting keyword search and hidden access structure. Also, as discussed earlier, such schemes generally consider only unshared multi-owner setting. For example, Zhang etal. [30] provided privacy-preserving ranked multi-keyword search in the multi-owner model and prevented attackers from eavesdropping secret keys. Miao et al. [15] designed an efficient multi-keyword search scheme with fine-grained access control. Should these schemes be deployed in a shared multi-owner setting, they will need the same random parameter for each individual data owner, which clearly is impractical in practice particularly as the number of data owners increases.

Disadvantages of Existing Model

In the existing work, while CPABKS schemes can achieve one-to-many encryption and support expressive access control, they are not capable of identifying data users leaking the secret keys if the ‘culprits’ have the same subset of attributes as other honest data users.

The existing system has one serious limitation of CP-ABE schemes which is that the access policy embedded in the cipher texts may leak sensitive information to authorized data users, as discussed in the preceding section.

III. PROPOSED MODEL

Hence, in this system the system first proposes a privacy-preserving **A**ttribute-**B**ased **K**eyword **S**earch system with hidden access policy in **S**hared **M**ulti-owner setting (basic ABKS-SM system),then extend this basic system to support traceability(modified ABKS-SM system). Specifically, the main contributions of this paper are as follows.

- **Shared multi-owner setting**. Both ABKS-SM systems consider the shared multi-owner setting and enable data owners to provide enhanced access control over their shared data with multiple permissions.
- **Hidden access policy**. Both ABKS-SM systems provide hidden access policy, so that the access structure attached to the cipher texts does not leak sensitive information about the encrypted data and its privileged recipients.
- **Tracing of malicious data users**. To prevent dishonest data users from leaking their secret keys to others (e.g., for profits), the modified ABKS-SM system provides traceability by securely embedding their identity information in the secret keys. We formally prove that the basic and modified ABKSSM systems guarantee the security of shared data and access policies, achieve selective security, and resist off-line keyword-guessing attack in the generic bilinear group model.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

Advantages of Proposed Model:

- ✓ The system is more effective since Linear Secret Sharing Schemes (LSSS) present to give more security on the system.
- ✓ The system is more secured since Cipher text-Policy Attribute-Based Encryption(CP-ABE) schemes are designed to mitigate these two limitations, as well as enhancing access permissions in multi-user setting and facilitating one-to-many encryption.

3.1. PROPOSED MODEL OF ARCHITECTURE DIAGRAM

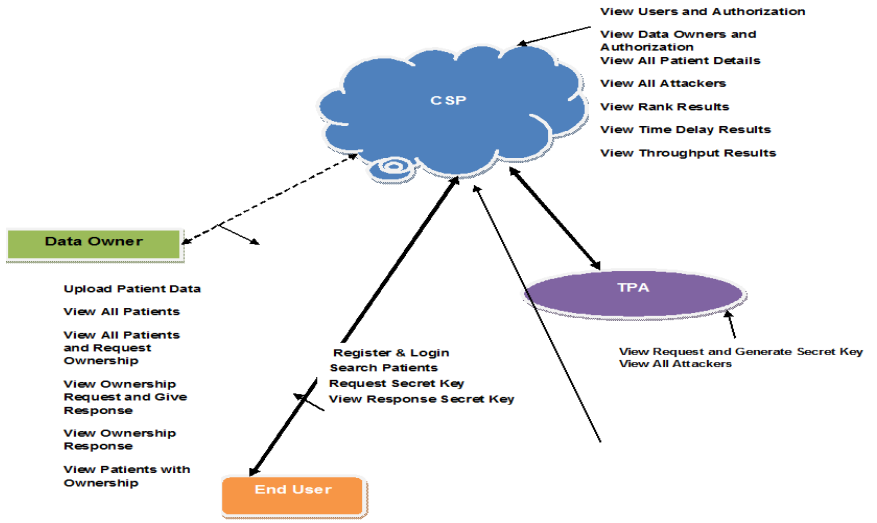


Figure 2.1: Proposed Architecture

3.2. MODULE DESCRIPTION

3.2.1. DATA OWNER

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Upload Patient Data, View All Patients, View All Patients and Request Ownership, View Ownership Request and Give Response, View Ownership Response, View Patients with Ownership.

3.2.2. CLOUD SERVER

In this module the cloud will authorize both the owner and the user and also performs the following operations such as View Users and Authorization, View Data Owners and Authorization, View All Patient Details, View All Attackers, View Rank Results, View Time Delay Results, View Throughput Results

3.2.3. TPA

In this module, the TPA performs the following operations such as View Request and Generate Secret Key, View All Attackers

3.2.4. DATA USER

In this module, the user has to register to cloud and log in and performs the following operations such as Search Patients, Request Secret Key, View Response Secret Key.

IV. IMPLEMENTATION OF THE MODEL

4.1. Symmetric key Algorithm:

Symmetric-key algorithms[1] are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to

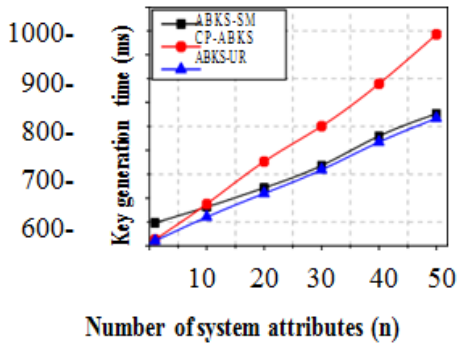
maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

4.2. Key Generation Algorithm:

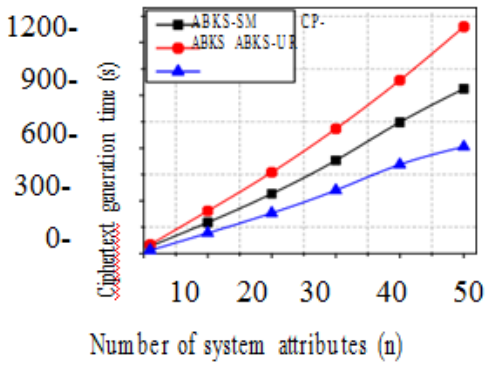
When used with asymmetric ciphers for key transfer, pseudorandom key generators are nearly always used to generate the symmetric cipher session keys. However, lack of randomness in those generators or in their initialization vectors is disastrous and has led to cryptanalytic breaks in the past. Therefore, it is essential that an implementation use a source of high entropy for its initialization.

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. A device or program used to generate keys is called a key generator or key gen.

V. EXPERIMENTAL RESULTS



(a)



(b)

Figure 5.1: Computational costs in various algorithms: (a) KeyGen algorithm; (b) Enc algorithm.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

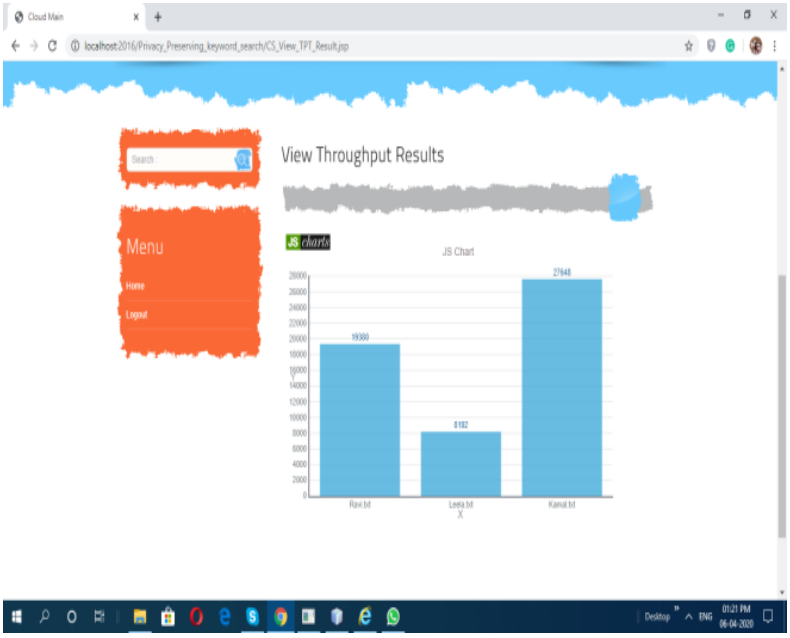


Figure 5.2: Throughput Result

VI. CONCLUSION

We presented a realistic keyword search scheme in the paper which supports hidden access policies in a shared multi-owner environment. In addition, we demonstrated how, if desired, the basic ABKS-SM system can be expanded to support traceability in the updated ABKS-SM system (i.e. malicious DU tracing). The structured security review showed that ABKS SM systems are specific and updated to achieve selective protection and resist attack on the generic bilinear community. The utility of the proposed ABKS-SM systems were demonstrated by testing their performance using three real-world data sets and a test bed including 11 mobile terminals and a high-performance workstation server. When the number of device attributes increases, the processing and storage costs often limit the proposed ABKS-SM systems. In addition, we are also planning to increase the performance of the ABKS-SM systems. We should also concentrate on explicit searches (e.g., multi-keyword search and weird keyword search) in our future research, to promote an effective search finding and to reduce the amount of irrelevant search results.

REFERENCES

[1] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine grained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 785–796, 2017.
[2] J. Li, H. Yan, and Y. Zhang, "Certificate less public integrity checking of group shared data on cloud storage," IEEE Transactions on Services Computing, vol. PP, pp. 1–1, 2018.
[3] D. Wu, J. Yan, H. Wang, D. Wu, and R. Wang, "Social attribute aware incentive mechanism for device-to-device video distribution, "IEEE Transactions on Multimedia, vol. 19, no. 8, pp. 1908–1920,2017.
[4] D. Wu, Q. Liu, H. Wang, D. Wu, and R. Wang, "Socially aware energy-efficient mobile edge collaboration for video distribution," IEEE Transactions on Multimedia, vol. 19, no. 10, pp. 2197–2209,2017.
[5] D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, 2017.
[6] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques forsearches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (SP 2000), 2000, pp. 44–55.
[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. International conference on the theory and applications of cryptographic techniques(EUROCRYPT 2004), 2004, pp. 506–522.
[8] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Transaction son Dependable and Secure Computing, vol. 13, no. 3, pp. 312–325,2016.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

[9] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "Dual-server public-key encryption with keyword search for secure cloud storage," IEEE transactions on information forensics and security, vol. 11,no. 4, pp. 789–798, 2016.
[10] J. Bethen court, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in Proc. IEEE Symposium on Security and Privacy (SP 2007), 2007, pp. 321–334.
[11] B. Waters, "Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Inter-IEEE Transactions on Dependable and Secure Computing, Issue Date:05.February.2019 14national Conference on Practice and Theory in Public Key Cryptography(PKC 2011), 2011, pp. 53–70.
[12] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," IEEE Transactions on Services Computing, vol. PP, pp. 1–1, 2017.
[13] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion Avoidancecp-abe with efficient attribute revocation for cloud storage," IEEE Systems Journal, vol. 12, no. 2, pp. 1767–1777, 2018