Multi-keyword Searchable Encryption System against Insider Keyword-Guessing Attack in Cloud computing

Vikas ghodke[1], Tanmay Khade[2], Aadhish Chavan[3], Akash Malkar[4], Dr. V.V. Puri.[5]

[1] *Vikas Ghodke, Information Technology Engineering, Anantrao Pawar college of Engineering and Research, Maharashtra, India*
[2] *Tanmay Khade, Information Technology Engineering, Anantrao Pawar college of Engineering and Research, Maharashtra, India*
[3] *Aadhish Chavan, Information Technology Engineering, Anantrao Pawar college of Engineering and Research, Maharashtra, India*
[4] *Akash Malkar, Information Technology Engineering, Anantrao Pawar college of Engineering and Research, Maharashtra, India*

ABSTRACT

Searchable Encryption (SE) is a type of encryption that lets cloud tenants search for encrypted data while keeping their data safe. Insider Keyword-Guessing Attacks are still a problem for a lot of search engine solutions. This means that the internal hackers can figure out the candidate keywords off-line and use them to search for them. Also in existing SE solutions, a semi-honest- but-curious cloud server may deliver incorrect search results by performing only a fraction of retrieval operations honestly. This system can withstand the inside KGA and achieve verifiable search ability. After introducing the basic version of VSEF, we then show how the enhanced version of VSEF can search for multiple keywords, encrypt multiple keys, and make dynamic changes to data at the same time. This shows how important it is for SE to be practical and scalable in real-world applications using advanced encryption techniques.
Keywords– Advanced encryption, insider keyword- guessing attack, multi-keyword search, multi-key encryption.

I. INTRODUCTION

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot services are provided by the cloud service providers which helps to reduce costs needed for various resources. Cloud storage is one of the most vital service in cloud computing. Scalability is another attracting factor which allows user to scale up and scale down the resources as required. Cloud computing also provides convenient and flexible ways for data sharing. There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to-many pattern. As the data shared on the cloud is valuable, various security methods are provided by cloud. In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption. Symmetric-key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology. In existing system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack. Another gap is that a user is not allowed to upload multiple files of same name.

Literature Review

Sr No	Paper Details	Advantages	Algorithm/ Techniques	Limitations	Summary
1	C. Ge, W. Susilo, J. Wang, and L. Fang, "Identity-based conditional proxy re-encryption with fine grain policy," Computer Standards & Interfaces, vol. 52, pp. 1–9, 2017.	This work, for the first time, answers the aforementioned open problems affirmatively by presenting an identity-based proxy re-encryption with fine grain policy.	identity-based conditional proxy re-encryption scheme (IB-CPRE)	open problem to construct a key-private IB-CPRE scheme	Authors formulated the security model of IB-CPRE-FG and proved its IND-CCA security. In this scheme, the access policy is described by an access structure. First, it is interesting to construct an IB-CPRE scheme supporting AND or OR gates directly. Second, as many proxy re-encryption schemes [36, 37] have been proposed to capture the key-private property
2	C. Ge, W. Susilo, J. Wang, and L. Fang, "Identity-based conditional proxy re-encryption with fine grain policy," Computer Standards & Interfaces, vol. 52, pp. 1–9, 2017.	This work, for the first time, answers the aforementioned open problems affirmatively by presenting an identity-based proxy re-encryption with fine grain policy.	identity-based conditional proxy re-encryption scheme (IB-CPRE)	open problem to construct a key-private IB-CPRE scheme	Authors formulated the security model of IB-CPRE-FG and proved its IND-CCA security. In this scheme, the access policy is decscribed by an access structure. First, it is interesting to construct an IB-CPRE scheme supporting AND or OR gates directly. Second, as many proxy re-encryption schemes [36, 37] have been proposed to capture the key-private property
3	C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for drobox data sharing system," Designs, Codes and Cryptography, pp. 1–17, 2018.	Author proposes the notion of key-policy attribute-based proxy re-encryption, which supports any monotonic access structures on users' keys. This scheme is proved against chosen-ciphertext attack secure in the adaptive model	key-policy attribute-based proxy re-encryption (KP-ABPRE)	How to construct a multi-hop attribute-based proxy re-encryption scheme remains to be an interesting problem	In this paper, author introduced a new notion of key-policy attribute-based proxy re-encryption and presents an adaptively CCA-secure KP-ABPRE scheme. this scheme extends the notion of proxy re-encryption to key-policy attribute-based encryption setting.
4	H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, "Cp-abse: A ciphertext-policy attribute-based searchable encryption scheme," IEEE Access, vol. 7, pp. 5682–5694, 2019.	Author proposes an attribute-based searchable encryption scheme by leveraging the ciphertext-policy attribute-based encryption technique	Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE)	Not support dynamic, forward secure, and anonymous attributed-based searchable encryption scheme	This scheme allows the data owner to conduct a fine-grained search authorization for a data user. The main idea is that a data owner encrypts an index keyword under a specified access policy, if and only if, a data user's attributes satisfy the access

					policy, the data user can perform search over the encrypted index keyword.
5	Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, "Privacy-preserving attribute-based keyword search in shared multi-owner setting," IEEE Transactions on Dependable and Secure Computing, 2019.	1. Author Propose Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports fine-grained access control over encrypted data in the cloud. 2. CP-ABKS schemes were designed to support unshared multi-owner setting, and cannot be directly applied in the shared multi-owner setting (where each record is accredited by a fixed number of data owners), without incurring high computational and storage costs	Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS)	1. limitation of the proposed ABKS-SM systems is that as the number of system attributes increases, so does the computational and storage costs 2. Not focus on expressive search	In the paper, author presented a practical attribute-based keyword search scheme supporting hidden access policy in the shared multi-owner setting. Furthermore, they demonstrated how the basic ABKS-SM system can be extended to support traceability (i.e., tracing of malicious DUs) in the modified ABKS-SM system, if desired
6	C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles," The Computer Journal, vol. 59, no. 7, pp. 970–982, 2016.	1. This scheme achieves the goals (1) scalable and finegrained access control for PHRs by using multi-authority ABE scheme, and (2) efficient on-demand user/attribute revocation and dynamic policy update. 2. This scheme supports efficient and on-demand lazy user revocation, which reduce the overhead a lot	attribute-based encryption (ABE)	Security is less	In this paper, authors propose a privacy-preserving PHR, which supports fine-grained access control and efficient revocation. When encrypting PHRs, patient can associate an expressive access tree structure with the ciphertext, thus achieving fine-grained access control. Authors also achieve privacy-preserving by using anonymous key issuing protocol.

7	K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X.Phuong, and Q. Xie, "A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.	Author propose a KP-ABPRE scheme which is CCAsecure under the 3-weak decisional bilinear Diffie–Hellman inversion assumption without random oracles.	key-policy attribute-based proxy re-encryption (KP-ABPRE)	Not designed non-interactive KP-ABPRE schemes, and KP-ABPRE schemes without pairings	In this paper, Author solve the problem left by Fang, Susilo, Ge and Wang by proposing a KP-ABPRE scheme without random oracles. this scheme enhances the security model by making some improvements of the re-encryption key query and reencryption query
8	B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFO COM 2014-IEEE Conference on Computer Communications, pp. 2112-2120, IEEE, 2014.	1. In this scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. 2. the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given	Deterministic finite automata-based functional PRE (DFA-based FPRE).	Not support DFA-based FPRE in the prime order bilinear group	In this paper for the first time author defined the notion of DFA-based FPRE, and meanwhile proposed a concrete scheme satisfying the new notion. Furthermore author proved the scheme, which is the first of its type, to be adaptively CCA secure in the standard model by employing Lewko et al.'s dual encryption technology
9	Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in Infocom, 2014 proceedings IEEE, pp. 522–530, IEEE, 2014.	1. Author proposes a novel multi-keyword fuzzy search scheme by exploiting the locality-sensitive hashing technique. 2. proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file	Bloom filter and locality-sensitive hashing (LSH)	Not efficient	In this paper, author tackled the challenging multi-keyword fuzzy search problem over the encrypted data. Author proposed and integrated several innovative designs to solve the multiple keywords search and the fuzzy search problems.
10	K. Liang and W. Susilo,	(i) search over the data	verifiable attribute-	This system focusses	Author introduced a novel

	"Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1981–1992, 2015.	owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations.	based keyword search (VABKS)	on static data. Not support accommodate dynamic data	cryptographic primitive called verifiable attribute-based keyword search for secure cloud computing over outsourced encrypted data. This primitive allows a data owner to control the search of its outsourced encrypted data according to an access control policy, while the authorized data users can outsource the search operations to the cloud and force the cloud to faithfully execute the search (as a cheating cloud can be held accountable).

II. OPEN ISSUES: -

Lot of work has been done in this field because of its extensive usage and applications. In this section, some of the approaches which have been implemented to achieve the same purpose are mentioned. These works are majorly differentiated by the techniques for multi-keyword search and group sharing systems.

- In previous technology in which Searchable Encryption (SE) is used to preventing data confidentially and securelybut most of them are still susceptible to insider Keyword-Guessing Attacks (KGA), which implies that the internal attackers can guess the candidate keywords successfully in an off-line manner.
- In SE, cloud server may deliver incorrect search results by performing only a fraction of retrieval operations honestly (e.g., to save storage space).

CONCLUSION

It was first proposed in this system that a basic VSEF could be used to prevent the malicious CS from giving out bad search results. It could also be used to protect against insider KGA attacks. Then, the basic VSEF was made better to be able to search for multiple keywords, encrypt multiple keys, and update dynamically at the same time in the enhanced VKSF. We showed that basic or enhanced VSEF is safe against the insider KGA, and that it is both correct and sound.

REFERENCES

[1] L. Zhang, G. Hu, Y. Mu, and F. Rezaeibagha, "Hidden ciphertextpolicy attribute-based encryption with fast decryption for personal health record system," IEEE Access, vol. 7, pp. 33202–33213, 2019.

[2] C. Ge, W. Susilo, J. Wang, and L. Fang, "Identity-based conditional proxy re-encryption with fine grain policy," Computer Standards & Interfaces, vol. 52, pp. 1–9, 2017.

[3] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A cca-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system," Designs, Codes and Cryptography, pp. 1–17, 2018.

[4] H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, and K. Li, "Cp-abse: A ciphertext-policy attribute-based searchable encryption scheme," IEEE Access, vol. 7, pp. 5682–5694, 2019.

[5] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, J. Li, H. Li, and J. Ma, "Privacy-preserving attribute-based keyword search in shared multi-owner setting," IEEE Transactions on Dependable and Secure Computing, 2019.

[6] C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang, and Y. Ren, "A key- policy attribute-based proxy re-encryption without random oracles," The Computer Journal, vol. 59, no. 7, pp. 970–982, 2016.

[7] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X.Phuong, and Q. Xie, "A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, 2014.

[8] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud," in IEEE INFO COM 2014-IEEE Conference on Computer Communications, pp. 2112-2120, IEEE, 2014.

[9] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in Infocom, 2014 proceedings IEEE, pp. 522–530, IEEE, 2014.

[10] K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1981–1992, 2015.