Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting

Akash Karkhile , Nayan Mote , Sumit Kulkarni , Samadhan Dhanave, Prof.Nitin Shivale
Department of Computer Engineering JSPM's, Bhivarabai Sawant Institute of Technology Research, Wagholi, Pune

Abstract— Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports fine-grained access management over encrypted knowledge within the cloud. However, previous CP-ABKS schemes were designed to support single multi-owner setting, and can't be directly applied within the shared multi-owner setting (where every record is commissioned by a set variety of information owners), while not acquisition high process and storage prices. Additionally, thanks to privacy issues on access policies, most existing schemes square measure susceptible to off-line keyword-guessing attacks if the keyword house is of polynomial size. what is more, it's tough to spot malicious users United Nations agency leak the key keys once quite one knowledge user has a similar set of attributes. during this paper, we tend to gift a privacy-preserving CP-ABKS system with hidden access policy in Shared Multi-owner setting (basic ABKS-SM system), and demonstrate however it's improved to support malicious user tracing (modified ABKS-SM system). we tend to then prove that the projected ABKS-SM systems bring home the bacon selective security and resist off-line keyword-guessing attack within the generic additive cluster model. we tend to conjointly appraise their performance mistreatment real-world datasets.

Keywords Ciphertext-policy attribute-based encryption, *shared* multi-owner setting, hidden access policy, user tracing, Time Server, Ranking.

I. INTRODUCTION:

Searchable coding (SE) schemes change knowledge users to firmly search and by selection retrieve records of interest over encrypted knowledge (outsourced to the cloud), per user-specified keywords. There are, however, alternative fascinating properties once managing encrypted knowledge outsourced to the cloud. for instance, once encrypting important volume of knowledge, typical coding approaches suffer from limitations thanks to having multiple copies of ciphertexts (e.g., publically key coding schemes) and sophisticated and expensive key management (e.g., in centrosymmetric coding schemes). Ciphertext-Policy Attribute-Based coding (CP-ABE) schemes square measure designed to mitigate these 2 limitations, additionally as enhancing access permissions in multi-user setting and facilitating one-to-many coding.

However, in normal CP-ABE schemes, associate access policy in plaintext is related to a ciphertext might lead to outflow of sensitive data. for instance, in associate e-health system, hospital A encrypts a patient's electronic anamnesis (EMR) victimisation CP-ABE with associate access policy, like ("ID: 1788" AND "Hospital: Hospital A") OR ("Doctor: Cardiologist" AND "Hospital: Hospital B") thence, one will simply infer from the user attribute set ("Cardiologist", "Hospital B") that patient ("ID: 1788") in Hospital a possible suffers from a cardiopathy. Such privacy outflow is clearly not applicable, significantly if the medical condition is a lot of sensitive (e.g., sexually transmitted diseases like Chlamydia, gonorrhea, and human nonmalignant neoplasm virus infections). additionally, medical organizations square measure subject to exacting regulative oversight in most developed jurisdictions. Hence, there are efforts to style CP-ABE theme with hidden access policies.

There have additionally been efforts to style schemes that permit an information owner to delegate his/her search capability during a fine grained manner, that permits alternative knowledge users to look, retrieve and rewrite encrypted knowledge of interest. Examples embody Ciphertext-Policy Attribute-Based Keyword Search.

However, in several applications, knowledge records square measure co-owned by variety of knowledge homeowners, instead of one knowledge owner. that's to mention, every file is encrypted by multiple knowledge homeowners, and also the knowledge User will access the file, if and given that, he/she obtains authorizations from many knowledge homeowners. for instance, the EMR for

an explicit patient is controlled by multiple departments (e.g., clinical departments like infectious diseases and psychiatry) and/or medical organizations (e.g., metropolis activity health care Hospital, Lone-Star State Center for communicable disease, and Lone-Star State communicable disease Institute). Deploying CP-ABKS schemes within the separate multi-owner setting (where multiple knowledge homeowners manage totally different knowledge records) incur important process and storage prices. Another realistic, however a lot of complicated, setting is that the shared multi-owner setting, wherever every record is co-owned by multiple knowledge homeowners.

Most CP-ABKS schemes don't think about the case wherever dishonest knowledge users might share their secret keys with unauthorized entities, leading to unauthorized entities having identical privileges as dishonest knowledge users. Thus, it's necessary to support traceability in CP-ABKS schemes, so as to trace malicious knowledge users World Health Organization sell or leak their secret keys .

II. LITERATURE SURVEY:

1. Paper Name: Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting
Author: Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo

Description: Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports fine-grained access management over encrypted information within the cloud. However, previous CP-ABKS schemes were designed to support exclusive multi-owner setting, and can't be directly applied within the shared multi-owner setting (where every record is authorised by a hard and fast range of information owners), while not acquisition high process and storage prices. additionally, thanks to privacy considerations on access policies, most existing schemes ar susceptible to off-line keyword-guessing attacks if the keyword house is of polynomial size. what is more, it's tough to spot malicious users United Nations agency leak the key keys once over one information user has constant set of attributes. during this paper, author gift a privacy-preserving CP-ABKS system with hidden access policy in Shared Multi-owner setting (basic ABKS-SM system), and demonstrate however it's improved to support malicious user tracing (modified ABKS-SM system). Here prove that the ABKS-SM systems attain selective security and resist off-line keyword-guessing attack within the generic linear cluster model. we tend to additionally assess their performance exploitation real-world datasets.

2. Paper Name: Certificateless public integrity checking of group shared data on cloud storage

Author: J. Li, H. Yan, and Y. Zhang

Description: Cloud storage service provides individuals with associate economical technique to share information at intervals a bunch. The cloud server isn't trustworthy, therefore variant remote information possession checking (RDPC) protocols square measure planned and thought to be an efficient thanks to make sure the information integrity. However, most of RDPC protocols square measure supported the mechanism of ancient public key infrastructure (PKI), that has obvious security flaw and bears huge burden of certificate management. To avoid this disadvantage, identity-based cryptography (IBC) is usually chosen to be the idea of RDPC. sadly, IBC has associate inherent disadvantage of key written agreement. to unravel these issues, here utilize the technique of certificateless signature to gift a replacement RDPC protocol for checking the integrity of information shared among a bunch. during this theme, user's non-public key includes 2 parts: a partial key generated by the cluster manager and a secret worth chosen by herself/himself. to make sure the correct public keys square measure chosen throughout the information integrity checking, the general public key of every user is related to her distinctive identity, for instance the name or phone number. Thus, the certificate isn't required and therefore the downside of key written agreement is eliminated too. Meanwhile, the information integrity will still be audited by public voucher while not downloading the entire data.

3. Paper Name: User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage

Author: Jiguo Li, Wei Yao, Jinguang Han

Description: Attribute-based encoding (ABE) will guarantee confidentiality and accomplish fine-grained knowledge access management in an exceedingly cloud storage system. thanks to the very fact that each attribute in ABE is also shared by multiple users and every user holds multiple attributes, any single-attribute revocation for a few user might have an effect on the opposite users with identical attribute within the system. Therefore, a way to revoke attribute expeditiously is a crucial and difficult drawback in ABE schemes. so as to resolve higher than issues, here first provides a concrete attack to the present ABE theme with attribute revocation. Then, formalize the definition and security model, that model collusion attack dead by the present users cooperating with the revoked users. Finally, author gift a user collusion turning away ciphertext-policy ABE theme with economical attribute revocation for the cloud storage system. the matter of attribute revocation is solved expeditiously by exploiting the construct of AN attribute cluster. once AN attribute is revoked from a user, the cluster manager updates alternative users' secret keys.

4. Paper Name: Lightweight Fine-Grained Search over Encrypted Data in Fog Computing

Author: Yinbin Miao, Jianfeng Ma, Ximeng Liu, Jian Weng, Hongwei Li, and Hui Li

Description: Fog computing, as AN extension of cloud computing, outsources the encrypted sensitive knowledge to multiple fog nodes on the sting of web of Things (IoT) to decrease latency and network congestion. However, the present ciphertext retrieval schemes seldom concentrate on the fog computing atmosphere and most of them still impose high process and storage overhead on resource-limited finish users. during this paper, gift a light-weight Fine-Grained ciphertexts Search (LFGS) system in fog computing by extending Ciphertext-Policy Attribute-Based encoding (CP-ABE) and Searchable encoding (SE) technologies, which may deliver the goods fine-grained access management and keyword search at the same time. The LFGS will shift partial process and storage overhead from finish users to chosen fog nodes. moreover, the fundamental LFGS system is improved to support conjunctive keyword search and attribute update to avoid returning unsuitable search results and contraband accesses. The formal security analysis shows that the LFGS system will resist Chosen-Keyword Attack (CKA) and Chosen-Plaintext Attack (CPA), and also the simulation employing a real-world dataset demonstrates that the LFGS system is economical and possible in apply.

5. Paper Name: Personalized Search over Encrypted Data with Efficient and Secure Updates in Mobile Clouds

Author: H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu

Description: Mobile cloud computing has been concerned as a key facultative technology to beat the physical limitations of mobile devices towards climbable and versatile mobile services. within the mobile cloud surroundings, searchable cryptography, that allows directly search over encrypted information, could be a key technique to take care of each the privacy and value of outsourced information in cloud. On addressing the problem, several analysis efforts resolve to victimization the searchable cruciate cryptography (SSE) and searchable public-key cryptography (SPE). during this paper, authors improve the prevailing works by developing a a lot of sensible searchable cryptography technique, which may support dynamic change operations within the mobile cloud applications. Specifically, here build the efforts on taking the benefits of each point and SPE techniques, and propose PSU, a customized Search theme over encrypted information with economical and secure Updates in mobile cloud. By giving thorough security analysis, we have a

tendency to demonstrate that PSU can do a high security level.

III. EXISTING SYSTEM:

Existing Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) facilitates search queries and supports fine-grained access management over encrypted information within the cloud. However, previous CP-ABKS schemes were designed to support single multi-owner setting, and can't be directly applied within the shared multi-owner setting (where every record is commissioned by a set range of knowledge owners), while not acquisition high process and storage prices. additionally, because of privacy issues on access policies, most existing schemes area unit prone to off-line keyword-guessing attacks if the keyword area is of polynomial size. what is more, it's troublesome to spot malicious users WHO leak the key keys once over one information user has identical set of attributes. However, in commonplace CP-ABE schemes, associate access policy in plaintext is related to a ciphertext could lead to run of sensitive info.

Disadvantages:

1. It cannot be directly applied in the *shared* multi-owner setting , without incurring high computational and storage costs.

2. Existing schemes are vulnerable to off-line keyword-guessing attacks.

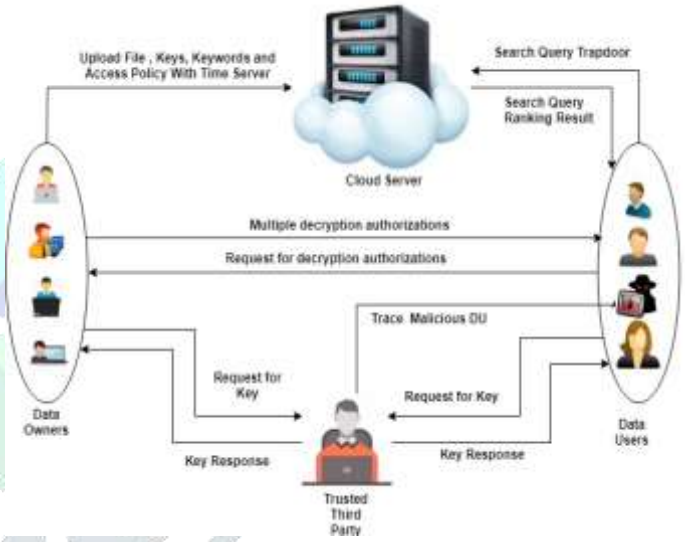
IV. PROPOSED SYSTEM:

Shared multi-owner setting. each ABKS-SM systems take into account the shared multi-owner setting and modify knowledge house owners to supply increased access management over their shared knowledge with multiple permissions. Hidden access policy. each ABKS-SM systems offer hidden access policy, in order that the access structure connected to the ciphertexts doesn't leak sensitive data concerning the encrypted knowledge and its privileged recipients. Tracing of malicious knowledge users. to forestall dishonest knowledge users from leaky their secret keys to others (e.g., for profits), the changed ABKS-SM system provides traceability by firmly embedding their identity data within the secret keys. we have a tendency to formally prove that the fundamental and changed ABKSSM systems guarantee the protection of shared knowledge and access policies, bring home the bacon selective security, and resist off-line keyword-guessing attack within the generic linear cluster model.

Advantages:

1. It achieve selective security and resist off-line keyword-guessing attack.

V. SYSTEM ARCHITECTURE:



VI. System Requirements:

Software Requirements

- Operating system: Windows 07 and above
- Language: Java
- Professional Environment: Eclipse
- Database: MySql, Xamp Server

Hardware Requirements

- System Type: 64-bit or 32-bit
- Processor: Intel core i5, 2 GHz
- Random Access Memory (RAM): 8 GB
- Storage Capacity: 1 TB

- IO device: mouse and keyboard
- Device Name: Lenovo Laptop Computer

CONCLUSION:

In the paper, we have a tendency to conferred a sensible attribute-based keyword search theme supporting hidden access policy within the shared multi-owner setting. what is more, we have a tendency to incontestable however the fundamental ABKS-SM system may be extended to support traceability (i.e., tracing of malicious DUs) within the changed ABKS-SM system, if desired. The formal security analysis showed that the fundamental and changed ABKS-SM systems accomplish selective security and resist off-line keyword guess attack within the generic linear cluster model. we have a tendency to additionally incontestable the utility of the projected ABKS-SM systems by evaluating their performance victimization 3 real-world datasets and on a testbed together with eleven mobile terminals and a superior digital computer server. One limitation of the projected ABKS-SM systems is that because the range of system attributes will increase, therefore will the procedure and storage prices. Thus, we have a tendency to shall improve the potency of the ABKS-SM systems within the future. Also, to facilitate the economical locating of search results and minimizing the amount of impertinent search results, we are going to concentrate on communicative search (e.g., multi-keyword search and fuzzy keyword search) in our future work.

REFERENCES:

[1] J. K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-Preserving Multi-Channel Communication in Edge-of-Things ," Accepted Manuscript, S0167-739X(18)30003-7
DOI: https://doi.org/10.1016/j.future.2018.03.043, 2018.
[2] JA. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach," Contents lists available at ScienceDirect Future Generation Computer Systems, 2014
[3] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE Transactions On Parallel And Distributed Systems Vol:24 No:1 Year 2013.
[4] A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Sham-shirband, , "Incremental proxy re-encryption scheme for mobile cloud computing environment ," © Springer Science Business Media New York 2013.
[5] A. Abbas andS. U. Khan , "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds ," IEEE Journal of Biomedical and Health Informatics ,vol. PP, no. 99, pp. 1–1, 2013.
[6] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches 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 Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 312–325, 2016.
[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. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symposium on Security and Privacy (SP 2007)*, 2007, pp. 321–334.