IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, June 2022

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

Vishal Shejwal
Student, Department of MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Cipher text-Policy Attribute-Based Keyword Search (CP-ABKS) offers fine-grained access management over encrypted knowledge in the cloud while facilitating search queries. The shared multi-owner setting (where every record is commissioned by a set variety of information owners) prevents the use of prior CPABKS schemes because they were created to serve single multi-owner settings and do not allow for the acquisition of high process and storage costs. Additionally, most current systems are vulnerable to off-line keyword-guessing assaults if the keyword house is polynomial in size because of privacy concerns with access controls. Furthermore, since each knowledge user has a similar set of characteristics, it can be difficult to identify rogue users who leak the key codes. In this research, we provide the basic ABKS-SM system, a privacy-preserving CP-ABKS system with hidden access policy, and show how it may be enhanced to facilitate malicious user tracing (modified ABKS-SM system). Then, within the general additive cluster model, we demonstrate that the proposed ABKS-SM systems deliver selective security and thwart off-line keyword-guessing attacks. Additionally, we evaluate their performance using real-world datasets.*

Keywords: User, Shared Multi-Owner Setting, Hidden Access Policy, Cypher Text-Policy Attribute-Based Encryption Time Server, Ranking and Tracing.

I. INTRODUCTION

According to user-specified keywords, searchable coding (SE) schemes enable knowledge consumers to thoroughly search and selectively obtain relevant information from encrypted knowledge (outsourced to the cloud). However, once handling encrypted data is outsourced to the cloud, there are other intriguing aspects. For example, when encrypting a significant amount of knowledge, conventional coding systems have drawbacks caused by multiple copies of the ciphertexts (such as publicly keyed coding schemes) and complex and expensive key management (e.g., in centrosymmetric coding schemes). In addition to improving access permissions in multi-user settings and easing one-to-many coding, CiphertextPolicy Attribute-Based Coding (CP-ABE) schemes are created to address these two issues.

However, in most CP-ABE schemes, relating an associate access policy in plaintext to a ciphertext may result in the leakage of sensitive information.

For instance, hospital A in an electronic health system encrypts a patient's electronic medical record (EMR) using CP-ABE with a patient access policy such as ("ID: 1788" AND "Hospital: Hospital A") OR ("Doctor: Cardiologist" AND "Hospital: Hospital B"). Inferring that patient ("ID: 1788") in Hospital a may have cardiopathy from the user attribute set ("Cardiologist," "Hospital B") is therefore a straightforward process. Such a breach of privacy is obviously unsuitable, particularly if the medical condition is highly sensitive (e.g., sexually transmitted diseases like Chlamydia, gonorrhea, and human nonmalignant neoplasm virus infections). Additionally, in the majority of industrialised jurisdictions, medical organisations are subject to strict regulatory scrutiny. Therefore, efforts are being made to style the CP-ABE theme with concealed access policies. Efforts have also been made to design methods that allow an information owner to fine-grainedly delegate his or her search power, allowing other knowledge users to hunt for, retrieve, and rewrite encrypted knowledge of interest. Examples include Attribute- Based Ciphertext Policy Keyword Search.

However, rather than having a single knowledge owner, some applications have several knowledge homeowners who jointly own the knowledge records. In addition, each file is encrypted by a number of knowledge homeowners, and the knowledge User can only read a file if numerous knowledge homeowners give their consent. For instance, many departments (for example, clinical departments like infectious diseases and psychiatry) and/or medical organisations

DOI: 10.48175/568

may have control over the electronic medical record (EMR) for a specific patient (e.g., metropolis activity health care Hospital, Lone-Star State Center for communicable disease, and Lone-Star State communicable disease Institute). When numerous knowledge homeowners handle various knowledge records, CP-ABKS deployments in separate multi-owner settings result in significant process and storage costs. The shared multi-owner arrangement, in which every record is co-owned by many knowledge homeowners, is another feasible but somewhat more difficult scenario.

Most CP-ABKS schemes fail to consider the possibility that dishonest knowledge users can divulge their secret keys to unauthorised parties, giving those parties access to the same resources as dishonest knowledge users. Thus, support for traceability in CP-ABKS schemes is required in order to track down bad knowledge users who sell or divulge their secret keys.

II. LITERATURE SURVEY

For a mobile cloud computing environment, an incremental proxy re-encryption strategy Mazhar Ali, Abdul Nasir Khan, Atta urRehman Khan, M. L. Mat Kiah, Sajjad A. Madani, and Shahaboddin Shamshirband .

The analysis community and the world are working on computationally secure methods that have the ability to offload the method- intensive info access operations to the cloud/trusted entity for execution. This is due to the limited method capabilities of mobile devices. El-Gamal cryptosystem is supported by the majority of the current security protocols, including proxy re-encryption, manager-based re- encryption, and cloud-based re-encryption, for outsourcing the method-intensive information access operation to the cloud/trusted entity. However, resource-hungry pairing-based cryptological procedures, such as secret writing and secret writing, are actively abusing the mobile device's limited processing power. Similar to this, if the owner of the knowledge wants to change the encrypted file that has been uploaded to a cloud storage, they must code and transfer the entire file to the cloud storage without taking anything into account.

The issue of privacy and electronic personal health records Li Jingquan

Customers have increased chances to control their own health and medical care thanks to personal health records (PHRs), which are central locations where they can store, manage, and exchange their personal health information electronically. It might be challenging to protect the privacy and confidentiality of health information contained in PHRs. They have examined the key characteristics of the current PHR systems and have identified particular privacy and security concerns with each form of PHR. It offers high-minded privacy principles like freelance consent management, freelance privacy and security assessments, and stringent compliance standards as part of a consumer- controlled privacy protection approach. The study offers a user-controlled system design for the web-based PHR system that incorporates these characteristics.

An analysis of incremental cryptography for mobile cloud computing environments' security protocols

Atta urRehman Khan, Samee U. Khan, Abdul Nasir Khan, M.L. Mat Kiah, Sajjad A. Madani

The mobile user should verify the confidentiality of the important data before uploading it to the cloud storage while using the cloud storage services on a mobile device with limited resources. Mobile users are restricted from penalising advanced security operations that utilise the computational power of mobile devices due to the resource limitations of those devices. A large number of current security schemes perform sophisticated security activities remotely on a cloud or reliable third party to create security schemes that are suited for mobile devices. As an alternative, a small number of the current security plans concentrate on lowering the science algorithms' procedural complexity. In order to raise the block(s) and changes operating, they have introduced Associate in Nursing incremental science version of the current security schemes, such as encryption-based theme, coding-based theme, and sharing-based theme. In comparison to the original version of identical schemes, their experiment improved resource consumption on mobile devices while conducting block insertion, deletion, and modification actions.

A Review of Modern Methods for Privacy Preservation in e-Health Clouds Samee U. Khan and Assad Abbas

The humanitarian industry as well as other corporate fields are adopting cloud computing as a new paradigm for computing. By integrating cloud services with the healthcare industry, the cloud can serve as a repository for medical

DOI: 10.48175/568

records. Moving to a cloud environment also relieves the burdensome infrastructure management chores from the assistance organisations and lowers development and maintenance costs. However, there are significant risks to information privacy associated with putting patient health data on third-party systems. Patients' privacy concerns should be given priority while developing security and privacy methods since it is possible that medical records stored and updated in the cloud will be made public. The privacy of the health information is protected in the cloud environment using a variety of techniques. The goal of this survey is to understand the innovative privacy-protective techniques utilised in e-Health clouds. Additionally, the privacy-protective methods are divided into cryptographic and non-cryptographic methods, and a taxonomy of the methods is also provided. Additionally, the advantages and disadvantages of the suggested ways are compared, and a few unresolved issues are noted.

A cloud-based recommendation system for health insurance plans: a strategy with the user in mind Kashif Bilal, Limin Zhang, Samee U. Khan, and Assad Abbas
The concept of the "Health Insurance Marketplace," which was developed to make it easier to purchase health insurance by comparing a variety of insurance plans' utility, coverage benefits, and quality, gives an important role to the insurance providers. Currently, internet-based tools available to search for insurance plans are lacking in providing tailored suggestions supported by the advantages and cost of the coverage. As a result, we have a propensity to present a cloud-based architecture that provides tailored recommendations for the insurance plans by anticipating the demands of the users. Using coverage and cost criteria like (a) premium, (b) co- pay, (c) deductibles, (d) coinsurance, and (e) most profit supplied by a set up, we have a tendency to utilise the Multi-attribute Utility Theory (MAUT) to assist customers in comparing various insurance plans. We have a propensity to give an identical illustration for the insurance plans in order to combat the challenges presumptively caused by the heterogeneous data formats and completely diverse set up representations throughout the suppliers. They learned that each supplier's information is retrieved using the knowledge as a service (DaaS). The framework is implemented using a code package.
Application of a rating method for the renowned service (SaaS) to deliver customised suggestions.

III. PROPOSED SYSTEM

Shared multiple-owner environment Each ABKS-SM system considers the shared multi- owner configuration and modifies knowledge owners to provide improved access management over their shared knowledge with various permissions. Secret access rules. In order to prevent critical information about the encrypted knowledge and its privileged recipients from being leaked, each ABKS-SM system offers a disguised access policy. tracking of knowledge users who are harmful. The modified ABKS-SM system offers traceability by firmly incorporating its users' identification data into the secret keys, preventing dishonest knowledge users from disclosing their secret keys to others (for instance, for financial gain). We aim to explicitly demonstrate that the basic and modified ABKSSM systems deliver the selective security, thwart off-line keyword- guessing attack, and ensure the protection of shared knowledge and access policies inside the generic linear cluster architecture

3.1 Advantages

1. Selective security is achieved, and an attempt to guess keywords off-line is resisted.
2. Identify Evil Users.
3. One file is shared by several data owners.

DOI: 10.48175/568

IV. SYSTEM ARCHITECTURE

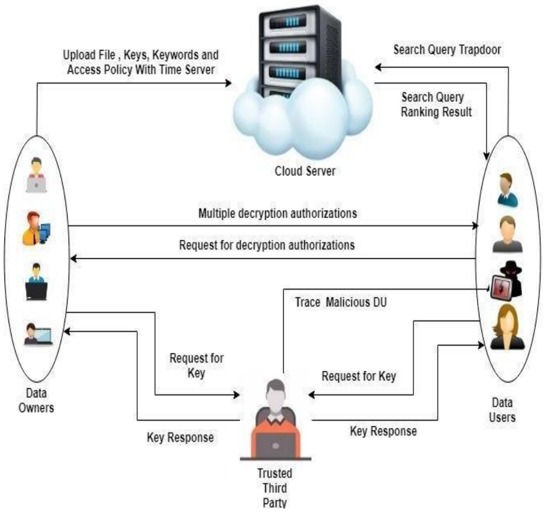
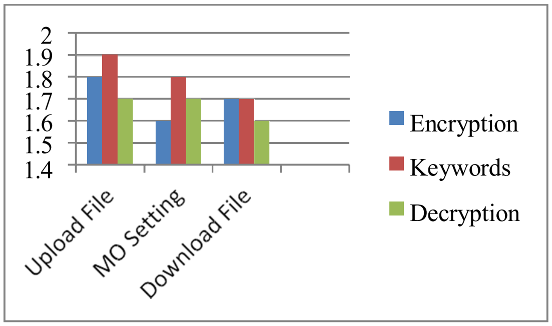
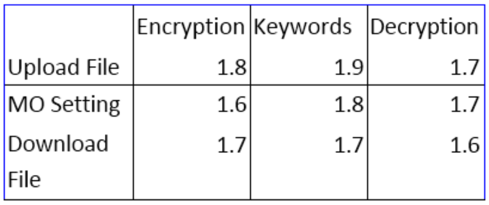

Upload File , Keys, Keywords and Access Policy With Time Server
Search Query Trapdoor
Search Query Ranking Result
Cloud Server
Multiple decryption authorizations
Request for decryption authorizations
Trace Malicious DU
Request for Key
Request for Key
Key Response
Key Response
Data Owners
Data Users
Trusted Third Party

Figure 1 System Architecture

V. RESULT AND SCREEN SHOTS





	Encryption	Keywords	Decryption
Upload File	1.8	1.9	1.7
MO Setting	1.6	1.8	1.7
Download File	1.7	1.7	1.6

VI. CONCLUSION

We tend to provide a practical attribute- based keyword search theme that supports hidden access policy in the shared multi-owner environment in the paper. Additionally, although we prefer to believe it is unquestionable, the basic ABKS-SM system may be expanded to provide traceability (i.e., tracing of malicious DUs) within the modified ABKS-SM system, if desired. The formal security study demonstrated that, within the general linear cluster model, the fundamental and modified ABKS-SM systems achieve selective security and thwart off-line keyword guess attacks. By assessing the performance of the proposed ABKSSM systems using three real-world datasets and on a test bed made up of eleven mobile terminals and an advanced digital communicative search (such as multi keyword search and fuzzy keyword search) in our future work to help with the economical locating of search results and reduce the number of impertinent search results.

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 Science Direct 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-shirb and, , "Incremental proxy reencryption scheme for mobile cloud computing environment ," © Springer Science Business Media New York 2013.

[5]. A. Abbas and S. U. Khan , "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds ,"IEEE computer server, weal so indisputable the usefulness of these systems. One drawback of the anticipated ABKS-SM systems is that as the variety of system features expands, so do the costs of procedures and storage. As a result, we plan to increase the ABKS-SM systems' effectiveness in the future. Additionally, we will focus on 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. Internationalconference 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 multikeywordsearchsupporting classifiedsubdictionaries 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 dynamiccredential generation scheme for protection of user identity in mobilecloud computing,"TheJournalof Supercomputing, pp. 1-20, 2013.

[11]. N. Fernando, S. W. Loke, and W. Rahayu, "Mobile Cloud Computing:A Survey," Future Generation Computer Systems, vol. 29, pp. 84– 106,January 2013.

[12]. K. Kumar and Y. H. Lu, "Cloud Computing For Mobile Users: CanOffloading Computation Save Energy?," IEEE Journal Computer, vol.43, pp. 51-56, April 2010.

[13]. E. Lagerspetz and S. Tarkoma, "Mobile Search and the Cloud: TheBenefits of Offloading," IEEE International Conference on PervasiveComputing and Communications Workshops (PERCOM Workshops),pp. 117–122,March 2011.[9] Q. Zhang, L. Cheng, and R.Boutaba, "Cloud computing: state-of-the-art and research challenges," Proc. IEEE Symposium on Security and Privacy (SP [19]D. Slamanig and C. Stingl, "Privacy aspects of 2007), 2007, pp. 321–334.

[14]. A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A.Madani,"TowardsSecureMobileCloud Computing: A Survey, Future GenerationComputer Systems, vol. 29, pp. 12781299, July 2013.

[15]. M. Armbrust et al., "Above the Clouds: A Berkeley View of CloudComputing", Technical e-Health," 3rd IEEE international Conference on Availability, Reliability and Security, (ARES '08), March 2008, pp.1226-1233.

[16]. "Federal Health IT Initiatives," http://www.hhs.gov , accessed December 24, 2012.

[17]. "CanadaHealth Infoway," http://www.infoway-inforoute.ca, accessed December 24, 2012. Report UCB/EECS-2009-28,EECS Department,University of California, Berkeley, Feb. 2009.

[18]. Pay-as-You-GowithCloudComputing,http://technology.inc.com/2008/05/01/p ay-as-you-go-with-cloud-

DOI: 10.48175/568

computing/, access data: 05 October, 2012.

[19]. S. Das, D. Agrawal, and A. E. Abbadi, "ElasTraS: An ElasticTransactional Data Store in the Cloud," proc. of the 2009 conference onHot topics in cloud (USENIX '09), June 2009. [15] A. N. Khan, M. M. Kiah, S. A. Madani, and M. Ali, "Enhanced

[20]. J. Dzenowagis and G. Kernen, "Connecting for health: Global vision, local insight," World Health Organization Press, Report for the World Summit on the Information Society, 2005, pp. 1-36

[21]. H. J. Cheong, N. Y. Shin, and Y. B. Joeng, "Improving Korean service delivery system in health care: focusing on national e-health system," inIEEE International conference on e-Health, Telemedicine and Social Medicine (TELEMED '09), February 2009, pp. 263–268.

[22]. L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, and D. Bell, "DACAR platform for e-Health services cloud," in 4th IEEE International Conference on Cloud Computing, July 2011, pp. 219-226.

[23]. P. G. Goldschmidt, "HIT and MIS:Implications of health information technology and medical information system," Communication of the ACM, Vol. 48, No. 10, October 2005, pp. 69–74.

DOI: 10.48175/568