IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Policy-Based Authorization For Enhanced Data Sharing In Databases

[1]Dr. B.Santhosh Kumar , [2]Banala Pavani , [3] Harshith Gundela, [4] Bushigampala Swetha

[1]Professor and HOD ,[2] Student
[1,2,3,4] Department of CSE , Guru Nanak Institute of Technology , Ibrahimpatnam , Hyderabad ,RR District

Abstract: Within cloud environments, Searchable Encryption (SE) serves as a vital tool for protecting data while maintaining its accessibility. The Cipher text-Policy Attribute-Based Keyword Search (CP-ABKS) relies on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to allow for keyword retrieval and precise access control. However, existing CP-ABKS setups face challenges due to their dependence on a single attribute authority for user certificate validation and secret key distribution. This reliance leads to performance bottlenecks in distributed cloud setups. To address this issue, our research introduces a secure Multi-authority CP-ABKS (MABKS) system. This system aims to overcome these limitations and reduce computational and storage overhead on resource-constrained devices within cloud infrastructures. Additionally, enhancements have been made to the MABKS system to enable the detection of fraudulent attribute authorities and facilitate attribute updates.

Index Terms - Cipher text-Policy Attribute-Based Encryption, MABKS, , Multi-authority CP-ABKS

I. INTRODUCTION

With the convergence of cloud service and IoT [1], cloud-based outsourcing services [2], [3], [4], [5] are becoming more and more common. For example, by outsourcing a significant amount of data to a third-party cloud server, resource-constrained devices (eg, mobile terminals, sensor nodes) can minimize local data storage and data processing requirements and facilitate data sharing (eg, health data sharing).). in the context of treatment) with other data users. However, data security breaches are an inherent risk in data outsourcing. Therefore, encryption is usually implemented before outsourcing to achieve both data security and privacy in a semi-trusted or compromised cloud environment. However, this limits the search/retrieval of encrypted cloud data. Therefore, searchable encryption (SE) methods have become increasingly popular, as SE systems can be used to securely search and selectively retrieve encrypted cloud data of interest based on user-specified keywords. In addition to the data search function that protects privacy, fine-grained access control is also an important function in cloud systems. For example, the CP-ABKS (Ciphertext-Policy Attribute-Based Keyword Search) model is a useful tool for precise access control and simultaneous keyword-based ciphertext searches. Most existing CP-ABKS systems are designed for single attribute approval scenarios. , where a single attribute authority must perform time-consuming user certificate verification and secret key distribution. This also results in single-attribute authority being a performance bottleneck for large distributed cloud systems (e.g. poor reliability and performance). If this single-owner authorization is compromised or offline, the cloud service will also be affected (eg not available at the time). For example, data users may be stuck in a queue for a long time before receiving the corresponding secret keys. . Such a single-point performance bottleneck can potentially degrade the efficiency of secret key generation and affect the availability of the CP-ABKS system. Traditional multi-agency ABE systems, where each agency manages separate sets of attributes, also present the same problem. For example, in multi-agency CPABE systems, DU attributes (ie, work, skill, health, etc.) are managed by different attribute agencies (ie, talent market, authentication center, hospital, etc.). However, DU suffers from the above problem when any of the properties are open. In addition, simply combining previous multi-agent systems also creates security issues. For example, it can be difficult to track down a malicious entity that has intentionally or unintentionally provided fake secret keys to data users. A RAAC (Robust and Auditable Access Control) system with a heterogeneous architecture allows multiple attribute authorities (AA) to independently verify user certificates and generate intermediate secret keys for data users on behalf of a central authority (CA). However, this model does not support keyword-based encryption search. The latter is a very useful feature in information retrieval systems to alleviate the problem of systems returning many irrelevant search results, which wastes bandwidth and computing resources. In addition, most existing CP-ABKS systems focus on defining an expressive access structure, but the storage and computational costs in these systems increase almost linearly with the number of system attributes instead of user attributes. Therefore, such systems are not suitable for deploying resource-constrained devices. In addition, malicious As provided by third parties can perform inappropriate actions (eg, AAs can maliciously or incorrectly generate an intermediate key for a suspected data user, as shown in Section 5. 2), and malicious downstream users can access sensitive data using outdated data. data secret keys when their properties are updated in dynamic applications

II. LITERATURE SURVEY

X. Zhang, C. Xu, R. Xie, and C. Jin proposed a "model-based search strategy for inventory management systems". Inventory management is critical to human spaceflight operations. We currently use the Inventory Management System (IMS) to track goods on the International Space Station (ISS). One challenge is finding lost or misplaced items when IMS cannot locate them due to human factors. This article illustrates a model-based retrieval strategy called Semantic Inventory Management for the ISS (SIMISS), which calculates possible locations of missing objects based on contextual properties in three dimensions: (1) spatial; (2) temporal; and (3) a person. This includes ontologies, databases, machine learning algorithms and ubiquitous client applications. We implemented and tested SIMISS with sample IMS data, operational data files and internal short-term planning experiments were conducted in several simulation scenarios
C. Huang, R. Lu, H. Zhu, J. Shaoja X. Lin studied the development of the healthcare industry and the electronic health records (EHR), one of the digital health records stored and managed by patients, offers more advantages. EHR devices allow patients to conveniently share health information with doctors and create a complete picture of their health. However, due to the sensitivity of EHRs, ensuring the security and privacy of EHRs becomes one of the most important concerns for patients. In this article, you can address these privacy concerns, such as specifying access controls for shared EHR devices, maintaining the confidentiality of EHR data stored in the cloud, reviewing EHR data, and finding the right one. doctors for patients. we propose a fine-grained EHR sharing system using similarity-based recommendation accelerated by Locality Sensitive Hashing (LSH) in a cloud-based healthcare system called FSSR. Specifically, our proposed system allows patients to securely share their EHR data with any appropriate physician through detailed privacy access controls. A detailed security analysis confirms its security richness. In addition, extensive simulations are performed to develop the FSSR prototype, and performance evaluations show the effectiveness of FSSR in terms of computation, storage, and communication costs while minimizing privacy exposure.

J. Shaoja, C. Huang, R. Lu, and H. Zhu According to X. Lin's research on the evolution of the healthcare sector, the electronic health record (EHR), a digital health record that is kept and controlled by the patient, has additional benefits. EHR devices facilitate the easy exchange of medical records between patients and physicians, enabling the creation of a comprehensive health picture. But since EHRs are so sensitive, one of the most significant worries for patients is making sure their data is secure and private. These privacy problems, including defining access restrictions for shared EHR devices, protecting the privacy of EHR data stored in the cloud, evaluating EHR data, and selecting the appropriate one, may all be addressed in this article. physicians for their patients. In the cloud-based healthcare system known as FSSR, we present a fine-grained EHR sharing system utilizing similarity-based recommendation accelerated by Locality Sensitive Hashing (LSH). In particular, our suggested system's comprehensive privacy access restrictions enable patients to safely exchange their EHR data with any qualified doctor. Its security richness is confirmed by a thorough security investigation. Furthermore, a great deal of simulation is used to create the

FSSR prototype, and performance assessments demonstrate how successful FSSR is in reducing computing, storage, and communication costs while maintaining privacy.

III. DESIGN

Initially, users can log in to this application data. The user can search the database's files after logging in. The database contains all of the client answers that the data user can view. The database's search terms are visible to data users. Data users may see every detail about the attacker. The data owner is able to log in. The file owner can upload it. All uploaded files are visible to the data owner in the database. A cloud server may log in.The user's queries can all be viewed by the cloud server. Files can also be seen via the cloud server. A matching keyword may exist for a cloud server. Users' data from the database can be seen by the cloud server. Data owners may be viewed by the cloud server from the database. Conversely, data owners have the ability to safely log in and upload files with ease, and they can access a handy list of all submitted items in the database. Cloud servers are crucial in the meanwhile; they log in to handle user requests, retrieve data, and apply sophisticated keyword matching algorithms. In addition, the servers offer insight into data owners and users, promoting a comprehensive comprehension of the dynamics of the system. Because of its strong design, cloud servers, data owners, and users may work together in a secure and efficient manner to manage and protect the data that is stored.

IV. METHODOLOGY

This paper delves into the software language and tools utilized for project development, with JAVA as the chosen platform. JAVA, along with J2EE and J2ME, serves as the primary languages. Initially developed by James Gosling at Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform, JAVA inherits syntax from C and C++, featuring a simpler object model and fewer low-level facilities. Applications written in Java are compiled to bytecode, enabling execution on any Java Virtual Machine (JVM) irrespective of computer architecture. Known for its general-purpose, concurrent, class-based, and object-oriented nature, Java aims for minimal implementation dependencies, allowing developers to "write once, run anywhere." Widely regarded as one of the most influential programming languages of the 20th century, Java finds extensive usage across various domains, from application software to web applications. Its platform independence simplifies internet application development. The versatility, efficiency, platform portability, and security of Java technology render it ideal for network computing, extending its reach from laptops to data centers, game consoles to scientific supercomputers, cell phones to the Internet.

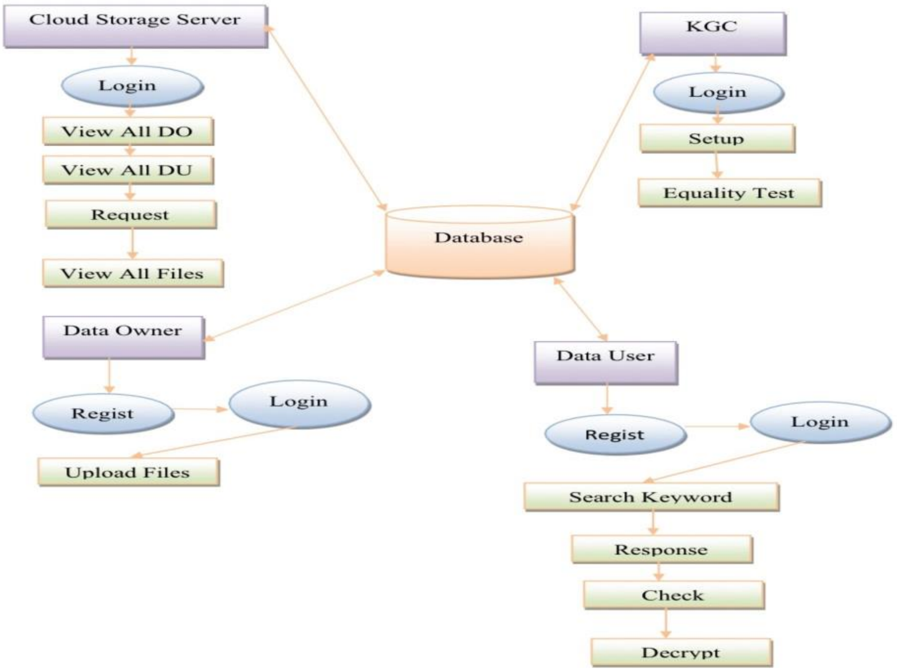


Fig 4.1: System Architecture

V. RESULTS AND DISCUSSION

The research article explores various techniques employed in a project implementation, focusing on the development of a web application using COREJAVA. The server-side processes are managed using SOCKET & SERVERSOCKET, while the design aspect is handled by Cascading Style Sheets (CSS). The article details the structure and functionality of the project's home page, which serves as the entry point for users and provides an overview of its objectives. Key features include user authentication, navigation menus for accessing data repositories and collaboration areas, a search function for locating relevant datasets, and highlighted updates or announcements. Additionally, the article discusses user profiles, activity feeds, and call-to-action buttons for facilitating user engagement and common tasks. It also outlines the roles and responsibilities of various entities within the system, such as data owners, data users, and the Key Generation Center (KGC). Furthermore, it defines the term "data user" and elaborates on their role in interacting with and leveraging data within the system. The article also describes the "search request page" interface, which enables users to initiate searches for specific information and provides features such as real-time autosuggestions and navigation elements for seamless exploration of search results. Finally, the article briefly discusses the concept of the "CSS homepage" in the context of web development projects, emphasizing its importance in managing styles and ensuring a consistent visual design across the application.

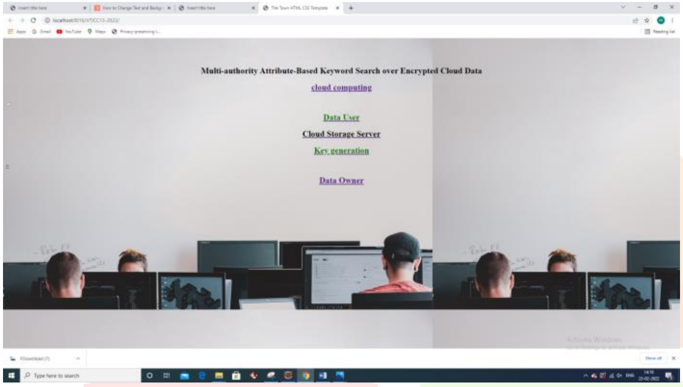

Multi-authority Attribute-Based Keyword Search over Encrypted Cloud Data
cloud computing
Data User
Cloud Storage Server
Key generation
Data Owner

Fig. 5.1 Home Layout

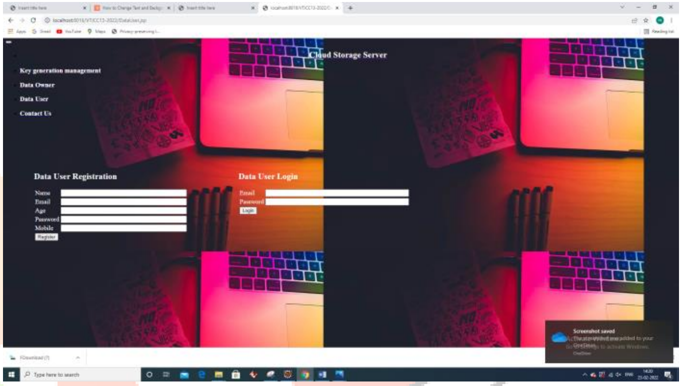


Fig. 5.2 User Layout

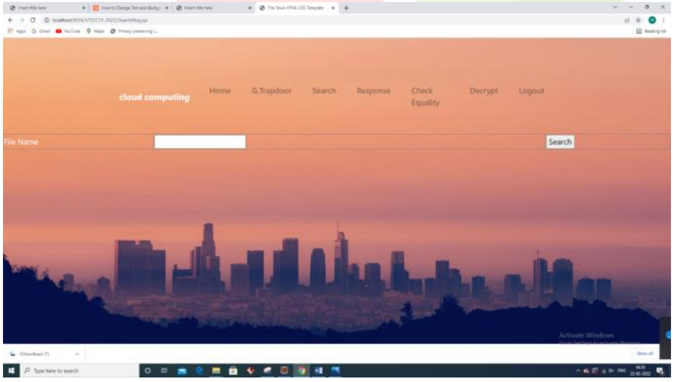
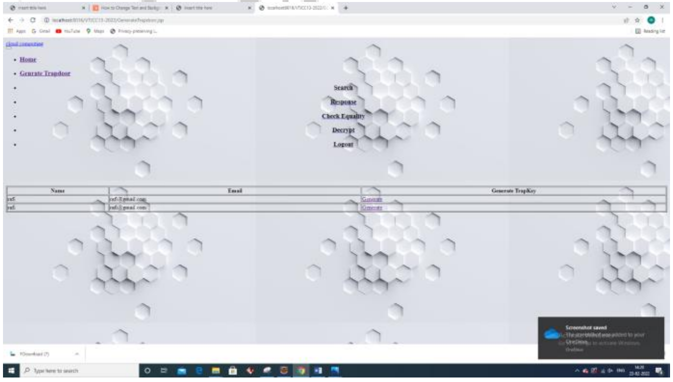


Fig. 5.3 Search Layout



Name	Email	Generate TrapKey
rafi	rafi.l@gmail.com	Generate
rafi	rafi@gmail.com	Generate

Fig. 5.4 Trapdoor Generation

VI. CONCLUSION

The research article presents an efficient Multi-Authority Attribute-Based Keyword Search (MABKS) system designed to mitigate performance bottlenecks in cloud systems by distributing authority across multiple entities. It addresses challenges such as collusion attacks and outdated secret keys by enabling the tracing of malicious Attribute Authorities (AAs) and supporting attribute updates. The system demonstrates selective security levels and achieves notable reductions in computational and storage costs compared to previous schemes. While acknowledging limitations in supporting expressive search queries, the paper provides a clear roadmap for future improvements, focusing on constructing an efficient and flexible index. This forward-looking perspective positions the MABKS system as a promising solution with potential for growth and adaptation, laying the groundwork for future research in secure and scalable attribute-based keyword search systems.

VII. FUTURE WORK

The future endeavors for the Multi-Authority Attribute-Based Keyword Search (MABKS) system will concentrate on constructing an efficient and flexible index to enhance its overall functionality. This includes refining the indexing mechanism to adapt to different data types, optimizing data structures and access methods for quicker and more accurate search results, and fine-tuning search algorithms to reduce latency. The goal is to develop the MABKS system into a versatile tool that can cater to evolving search requirements, ensuring its relevance and usability across diverse contexts. Additionally, integrating cutting-edge technologies such as machine learning algorithms and distributed computing frameworks will further augment the system's capabilities, while advancements in encryption techniques will bolster its security aspects. By prioritizing these developments, the MABKS system aims to excel in scalability, adaptability, and user satisfaction, positioning itself as a dynamic and forward-looking solution in the domain of secure and efficient attribute-based keyword search systems.

VIII. REFERENCES

1. Y. T. Demey and M. Wolff, “Simiss: A model-based searching strategy for inventory management systems,” IEEE Internet of Things Journal, vol. 4, no. 1, pp. 172– 182, 2017.

2. C. Huang, R. Lu, H. Zhu, J. Shao, and X. Lin, “Fssr: Finegrainedehrs sharing via similarity- based recommendation in cloud-assisted E-health care system,” in Proc. ACM on Asia Conference on Computer and Communications Security (AsiaCCS’16), 2016, pp. 95– 106.

3. Y.Miao, J.Weng, X.Liu, K.-K.R.Choo, Z.Liu, and H.Li, “Enabling verifiable multiple keywords search over encrypted cloud data,” Information Sciences, vol. 465, pp. 21–37, 2018.

4. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, “Lightweight fine-grained search over encrypted data in fog computing,” IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2018

5. Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, “Attributebasedkeywordsearchoverhierarchicaldatainclou dcomputing,” IEEE Transactions on Services Computing, vol. PP, no. 1, pp. 1–14, 2017.

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’00), 2000, pp. 44–55.

7. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT’04), vol. 3027, 2004, pp. 506–522.

8. H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, “Personalized search over encrypted data with efficient and secure updates in mobile clouds,” IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 97– 109, 2018.

9. J.Ning, J.Xu, K.Liang, F.Zhang, and E.-C.Chang, “ Passive attacks against searchable encryption,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 789– 802, 2019.

10. X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, “Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage,” Information Sciences, vol. PP, pp. 1–15, 2019.

11. J. Li, Y. Huang, Y. Wei, S. Lv, Z. Liu, C. Dong, and W. Lou, “Searchable symmetric encryption with forward search privacy,” IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1–15, 2019.

12. Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, “Practical attribute based multi-keyword search scheme in mobile crowdsourcing,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3008– 3018, 2018

13. Q. Zheng, S. Xu, and G. Ateniese, “Vabks: verifiable attribute based keyword search over outsourced encrypted data,” in Proc. IEEE Conference on Computer Communications(INFOCOM’14),2014, pp. 522–530.

14. W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, “Protecting your right: verifiable attribute- based keyword search with fine-grained owner-enforced search authorization in the cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187– 1198, 2016.

15. L. Harn and J. Ren, “Generalized digital certificate for user authentication and key establishment for secure communications,” IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011. K. Ren, ``Towardef_cient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Trans. Inf. Forensics Security, vol. 11, no. 12,pp. 2706_2716.