ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Multi-Authority Attribute-Based Search for Securing Encrypted Cloud Data

Mr. K. Hari Krishna [1],Mohd Altaf (20S11A1221) [2], Mohommad asif (21S15A1204) [3], M. Nayan (20S11A1224) [4], K. Nikhil (21S15A1206) [5],
ASSISTANT PROFESSOR [1], UG STUDENTS [2,3,4,5],
DEPARTMENT OF INFORMATION TECHNOLOGY
MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE,
Maisammaguda, Medchal (M), Hyderabad-500100, Telangana.

ABSTRACT

Searchable Encryption (SE) is an important technique to guarantee data security and usability in the cloud at the same time. Leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword-based retrieval and fine-grained access control simultaneously. However, the single attribute authority in existing CP-ABKS schemes is tasked with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our rigorous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models. Our experimental results using real-world datasets demonstrate the efficiency and utility of the MABKS system in practical applications.

INTRODUCTION

WITH the convergence of cloud computing and Internet of Things (IoT) [1], cloudassisted outsourcing services [2], [3], [4], [5] are becoming more commonplace. For example, outsourcing significant volume of data to a third-party cloud server, resource-limited devices (e.g., mobile terminals, sensor nodes) can minimize local data storage and computation requirements and facilitate the sharing of data (e.g., health records in a healthcare context) with other data users. However, privacy leakage is an inherent risk in data outsourcing. Hence, one typically deploys the encryption-before-outsourcing mechanism to achieve both data security and privacy in the semi-trusted or compromised cloud environment. This, however, restricts retrieval/searching over encrypted cloud data. Hence, the searchable encryption (SE) schemes 11 [6], [7], [8], [9], [10], [11] have gained in popularity, since SE schemes allow one to securely search and selectively retrieve encrypted cloud data of interest based on user-specified keywords. Apart from the privacy-preserving information retrieval functionality, the fine-grained access control is also an essential functionality in cloud systems. Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme, for example, is a viable tool to achieve fine-grained access control and keyword-based ciphertexts retrieval simultaneously. Most existing CP-ABKS schemes [4], [5], [12], [13], [14] are designed for single attribute authority scenarios, where the single attribute authority needs to perform time-consuming user certificate verification [15] and secret key distribution. This also results in the single attribute authority being the single-point performance bottleneck (e.g., poor robustness and inefficiency) in large-scale distributed cloud systems. Should this single attribute authority be compromised or offline, then the cloud service will also be affected (e.g., being unavailable during that period). For example, data users may be stuck in the waiting queue for a long time before obtaining their corresponding secret keys. Such a singlepoint performance bottleneck can potentially degrade secret key generation performance, and affect CP-ABKS scheme availability. Traditional multiauthority ABE schemes [16], [17] in which each authority separately manages disjoint attribute sets also incur the same issue. For example, in multi-authority CP-ABE schemes, the DU's attributes (i.e., job, skill, health, etc.) are managed by various attribute authorities (i.e., talent market, authentication center, hospital, etc.). However, the DU still suffers from the above issue if one of the attribute authorities breaks down. Furthermore, simply combining previous multiauthority schemes also poses security concerns. For example, tracing a malicious authority that has issued, intentionally or unintentionally, incorrect secret keys for data users can be challenging. The RAAC (Robust and Auditable Access Control) scheme [18] with heterogeneous architecture allows multiple Attribute Authorities (AAs) to independently conduct user certificate verification and generate the intermediate secret keys for data users on behalf of the Central Authority (CA). However, this scheme cannot support keywordbased ciphertexts retrieval. The latter is an extremely useful feature in information retrieval systems, to mitigate the issue of systems returning many irrelevant search results and resulting in bandwidth and computation resource wastage.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

LITERATURE SURVEY

Searchable Encryption (SE) is an important technique to guarantee data security and usability in the cloud at the same time. Leveraging Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme can achieve keyword- based retrieval and fine-grained access control simultaneously. However, the single attribute authority in existing CP-ABKS schemes is tasked with costly user certificate verification and secret key distribution. In addition, this results in a single-point performance bottleneck in distributed cloud systems. Thus, in this paper, we present a secure Multi-authority CP-ABKS (MABKS) system to address such limitations and minimize the computation and storage burden on resource-limited devices in cloud systems. In addition, the MABKS system is extended to support malicious attribute authority tracing and attribute update. Our rigorous security analysis shows that the MABKS system is selectively secure in both selective-matrix and selective-attribute models.

Existing system

In the context of Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which is a technique used for secure data access control in cloud storage systems, the term “single attribute authority” refers to a scenario where there is only one authority responsible for verifying user attributes and distributing secret keys. A single attribute authority system for key distribution and verification is a cryptographic approach where access control and authentication are managed based on a single attribute or characteristic possessed by users. In this system, each user is assigned a unique attribute or characteristic, such as a specific role, membership status, or level of authorization. This attribute serves as the basis for granting access to resources and verifying the identity of users. For example, in a single attribute authority system for a company's network, users may be assigned attributes such as "employee," "manager," or "administrator." Access to different network resources would be granted based on these attributes, and users would authenticate themselves by presenting their assigned attribute try to make the disadvantages and anlyaze the existing system.

Disadvantages of Existing System

- Single Point of Failure Issue:Centralizing the verification of user attributes and distribution of secret keys creates a single point of failure. If the attribute authority is compromised, the security of the entire system is at risk.
- Scalability Challenges Issue: A single attribute authority may become overwhelmed as the number of users grows and the demand for key management and attribute verification increases. This can lead to performance bottlenecks.
- Limited Access Control Flexibility Issue: Relying on single attributes for access control policies restricts the system's ability to enforce more complex, nuanced access conditions that may be required for sophisticated data protection strategies.

Proposed System

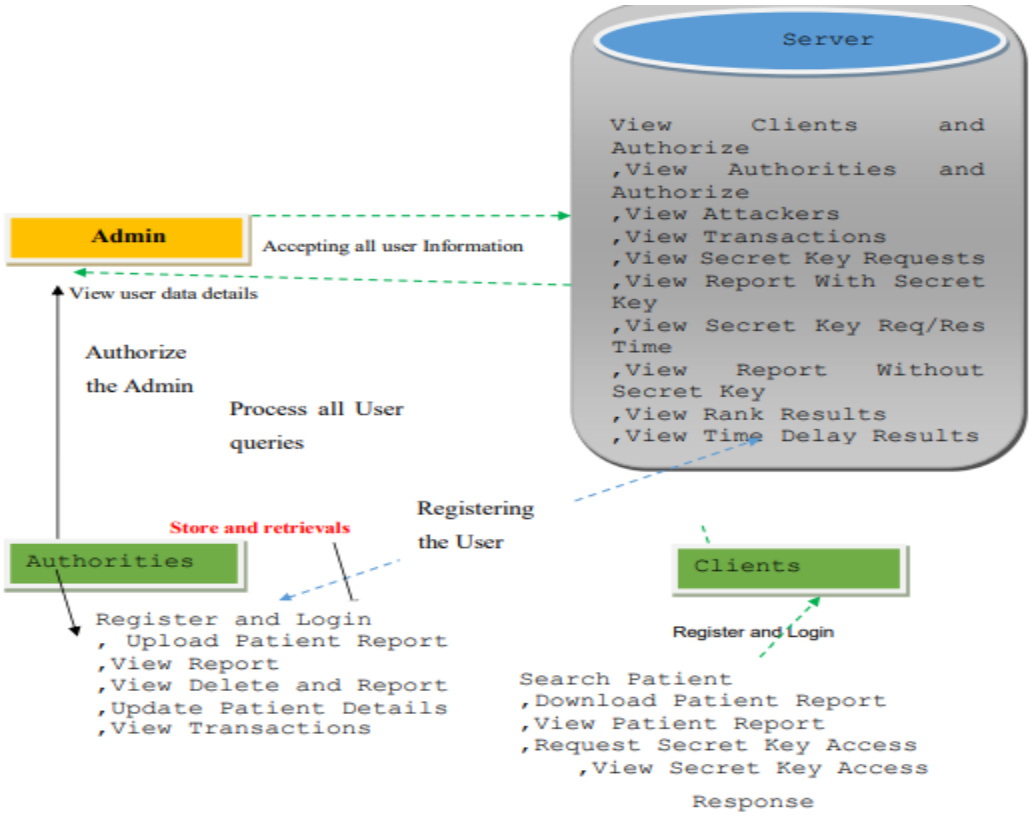
As businesses and individuals increasingly rely on cloud storage solutions for data storage and sharing, ensuring the security and privacy of sensitive information stored in the cloud has become paramount. Traditional encryption methods provide data confidentiality but lack the ability to perform efficient and secure searches over encrypted data. To address this challenge, we propose a Multi-Authority Attribute-Based Search (MA-ABS) system for securing encrypted cloud data while enabling efficient and secure search operations based on user-defined attributes. Traditional encryption techniques provide a foundational layer of security by encrypting data before uploading it to the cloud. However, while encryption ensures data confidentiality, it also renders the data unusable for search operations unless decrypted first. This limitation poses a significant challenge for users who need to perform efficient and secure searches over their encrypted data stored in the cloud. To address this challenge, we propose a novel approach: the Multi-Authority Attribute-Based Search (MA-ABS) system. This system combines the strengths of attribute-based encryption (ABE) and multi-authority key management to provide a comprehensive solution for securing encrypted cloud data while enabling efficient and secure search operations based on user-defined attributes.

Advantages of Proposed System

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

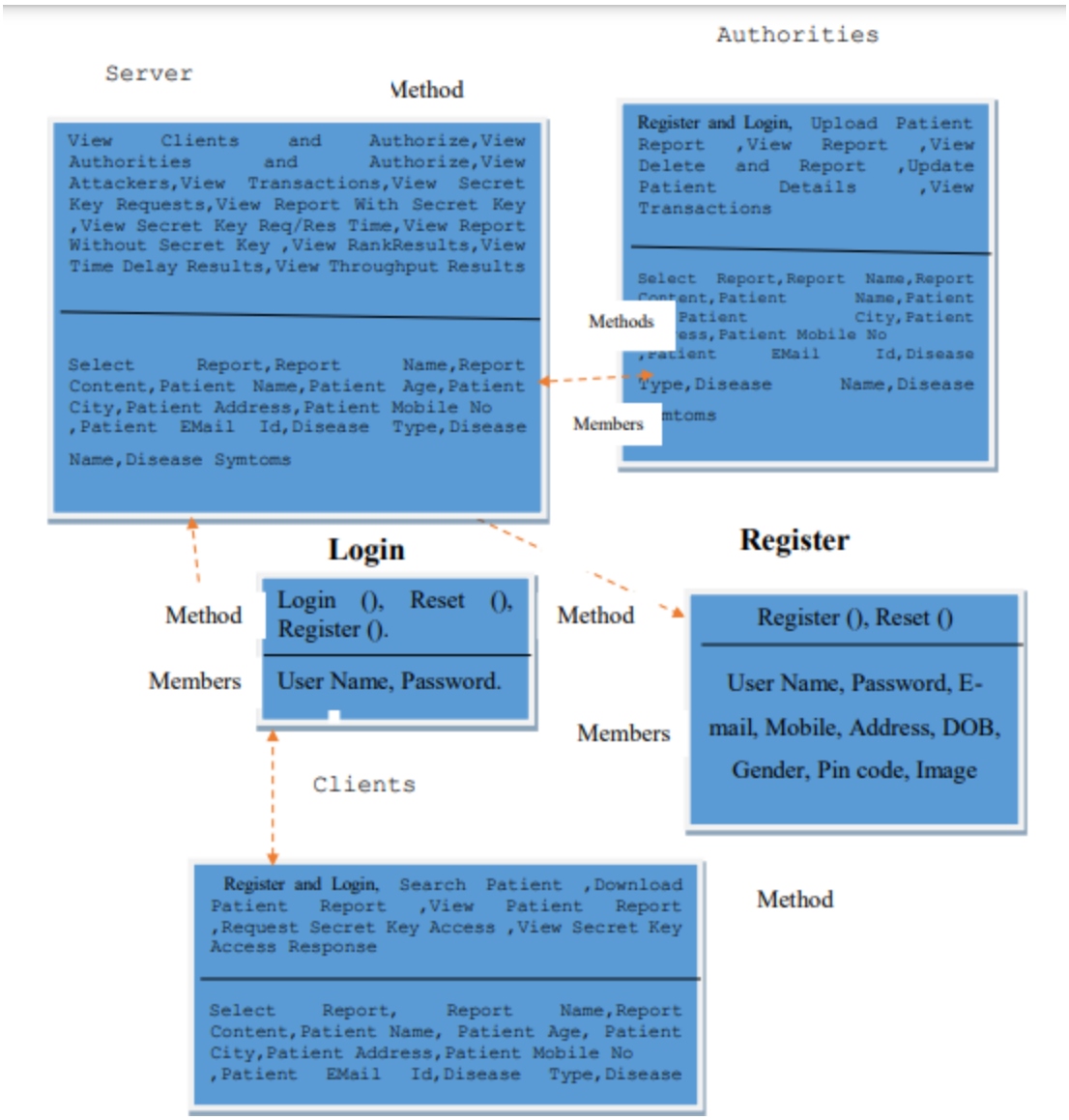
- Enhanced Data Confidentiality: The MA-ABS system employs attribute-based encryption (ABE), allowing data to be encrypted based on user-defined attributes. This granular approach ensures that only users with the requisite attributes can decrypt and access specific data objects, thereby enhancing data confidentiality.
- Fine-Grained Access Control: By leveraging attribute-based access control policies, the MAABS system enables fine-grained control over data access. Users can define access policies based on attributes such as roles, departments, or project affiliations, ensuring that only authorized individuals can access relevant data.
- Efficient and Secure Search Operations: Unlike traditional encryption methods that render data unusable for search operations, the MA-ABS system facilitates efficient and secure searches over encrypted data. Users can submit search queries based on attributes associated with the 10 encrypted data, allowing them to retrieve relevant information without compromising data confidentiality.
- Flexibility and Scalability: The MA-ABS system offers flexibility in managing access policies and attributes, accommodating changes in user roles and permissions dynamically. Additionally, its multi-authority architecture enhances scalability by distributing key management responsibilities among multiple attribute authorities, ensuring resilience and scalability as the system grows.
- Reduced Risk of Data Breaches: By encrypting data and enforcing access control based on user-defined attributes, the MA-ABS system mitigates the risk of data breaches and unauthorized access. Even if an attacker gains access to the encrypted data, they would still need the appropriate attributes and decryption keys to decipher the information, significantly reducing the likelihood of successful data exfiltration.
- Compliance with Regulatory Requirements: The MA-ABS system helps organizations comply with stringent regulatory requirements concerning data privacy and security. By implementing robust encryption and access control mechanisms, organizations can demonstrate adherence to regulatory standards and protect sensitive data from unauthorized access or disclosure

SYSTEM DESIGN



Class Diagram :

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024



Hardware Requirements

- Processor - intel core i3
- RAM - 4 GB (min)
- Hard Disk - 20 GB

Software Requirements:

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

- Operating System - Windows 11
- Coding Language - Java/J2EE (jsp, servlet)
- Front End - HTML, css, javascript.
- Back End - MySQL.

INPUT AND OUTPUT DESIGN

INPUT DESIGN:

The input design for the "Multi-Authority Attribute-Based Search for Securing Encrypted Cloud Data" system encompasses several critical elements. Users are prompted to input their credentials, comprising a username, password, and a set of attributes defining their access privileges. This input is facilitated through a user-friendly login interface, ensuring clarity and ease of use. Additionally, users submit search queries, including keywords or specific attributes, along with parameters such as search scope and sorting preferences. The system also processes attribute verification requests, which entail specifying attributes for validation and providing relevant authority information for multi-authority verification. Encrypted cloud data serves as input for the search and retrieval processes, contributing to the overall security of the system.

OUTPUT DESIGN:

Output side, the system provides various responses and information to facilitate user interaction and decision-making. Foremost among these outputs are encrypted search results, tailored to match the user's query, and accompanied by metadata such as file names and timestamps. Users receive notifications regarding their authorization status, including confirmations of successful attribute verification or denials if access is refused based on the provided credentials. Additionally, decrypted data may be provided for viewing or further processing by the user, enhancing the utility of the system. To maintain user engagement and clarity, error messages are designed to be informative, guiding users on how to address encountered issues effectively. Moreover, the system is engineered to ensure robustness through graceful degradation, minimizing disruptions in the event of errors or failures, thereby enhancing overall user satisfaction and system reliability. Output side, the system provides various responses and information to facilitate user interaction and decision-making. Foremost among these outputs are encrypted search results, tailored to match the user's query, and accompanied by metadata such as file names and timestamps. Users receive notifications regarding their authorization status, including confirmations of successful attribute verification or denials if access is refused based on the provided credentials.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

RESULTS

Home Page

Figure 1 Home page

Client login

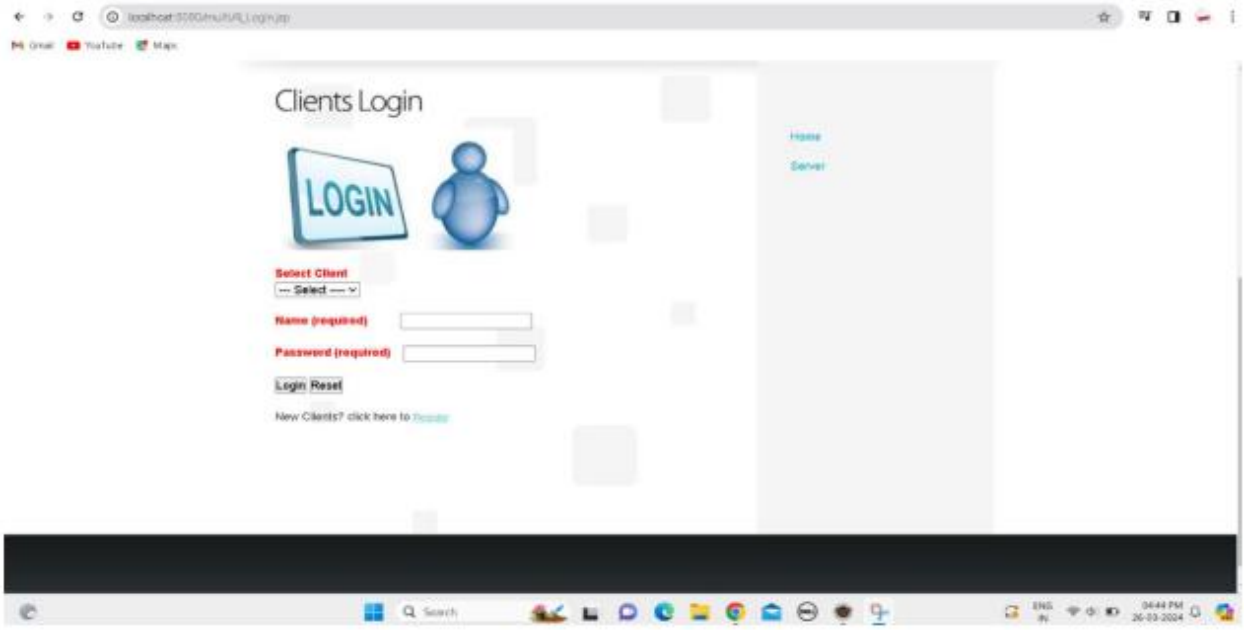


Figure 2 clients login

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Client operations

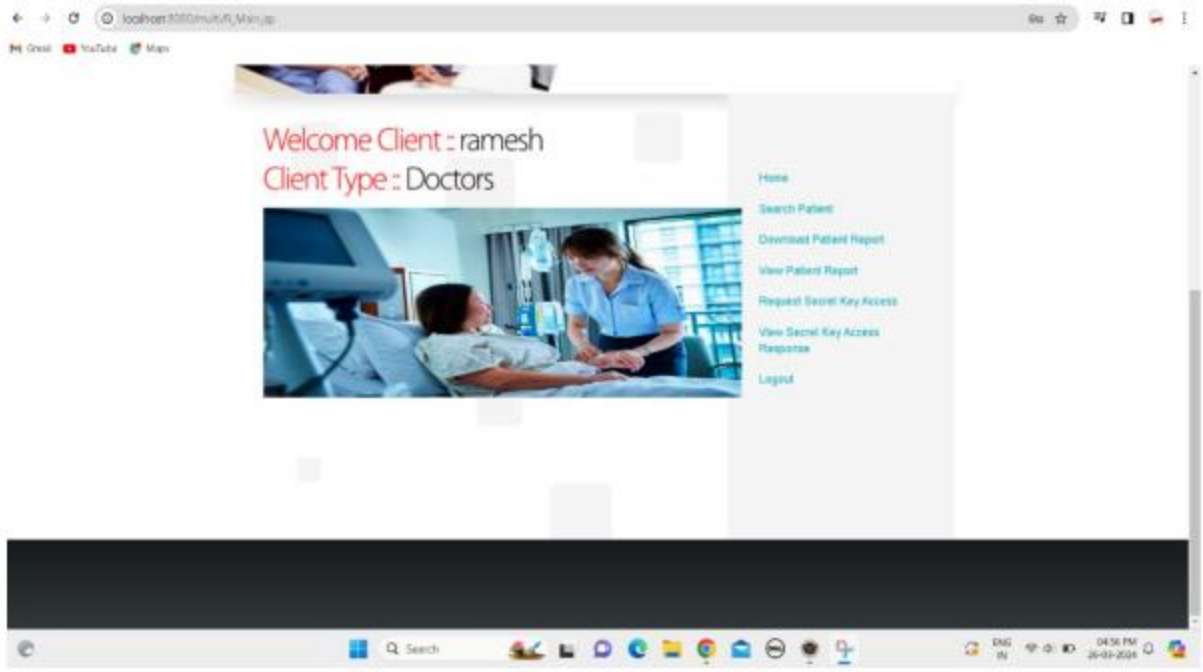


Figure 3 clients operations

Authorize login

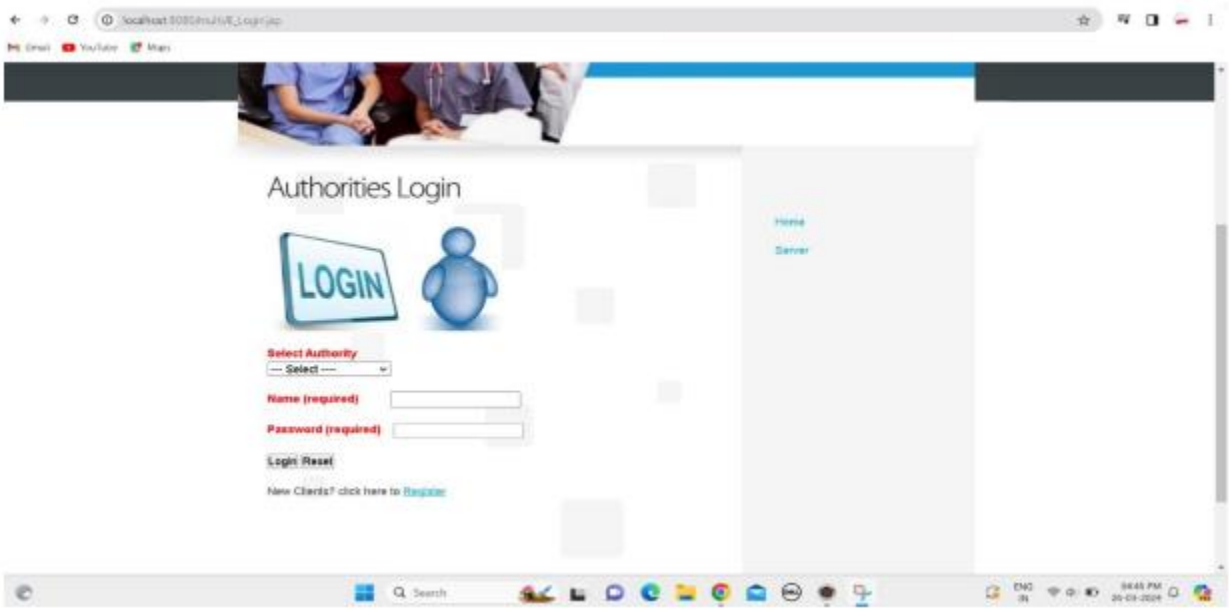


Figure 4 authorize logins

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Server login

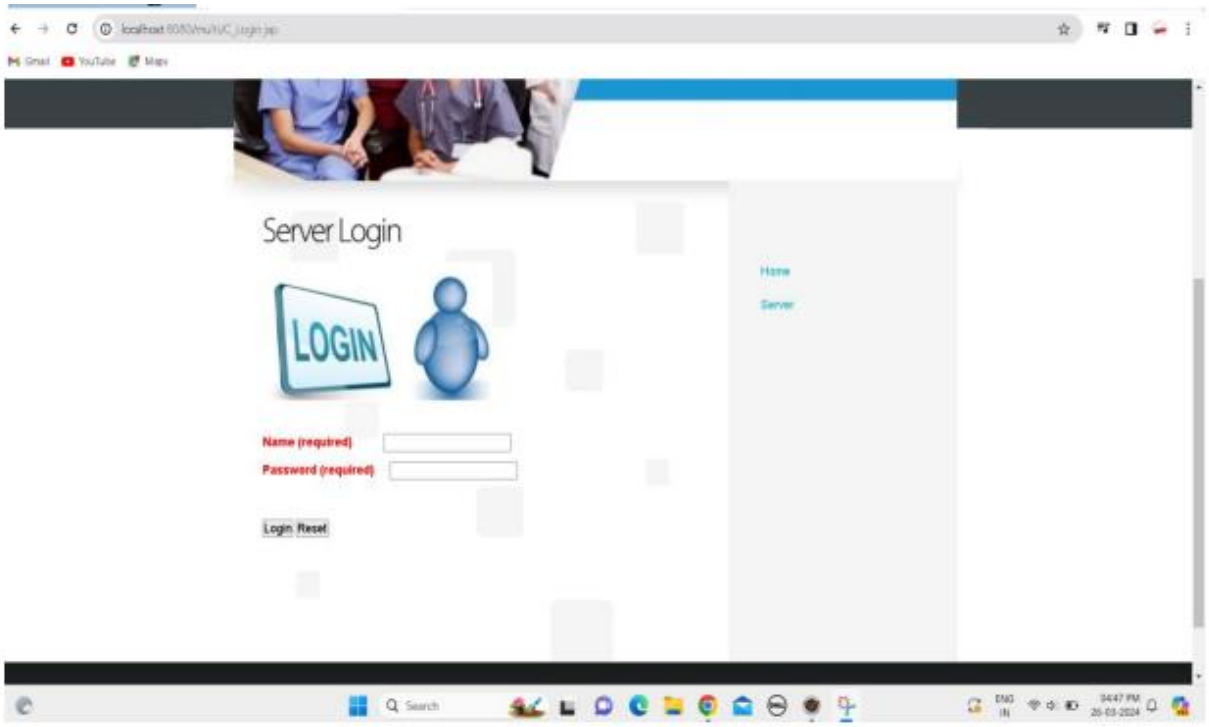


Figure 5 server login

Server operations

Figure 6 server operations

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Encrypted patient report

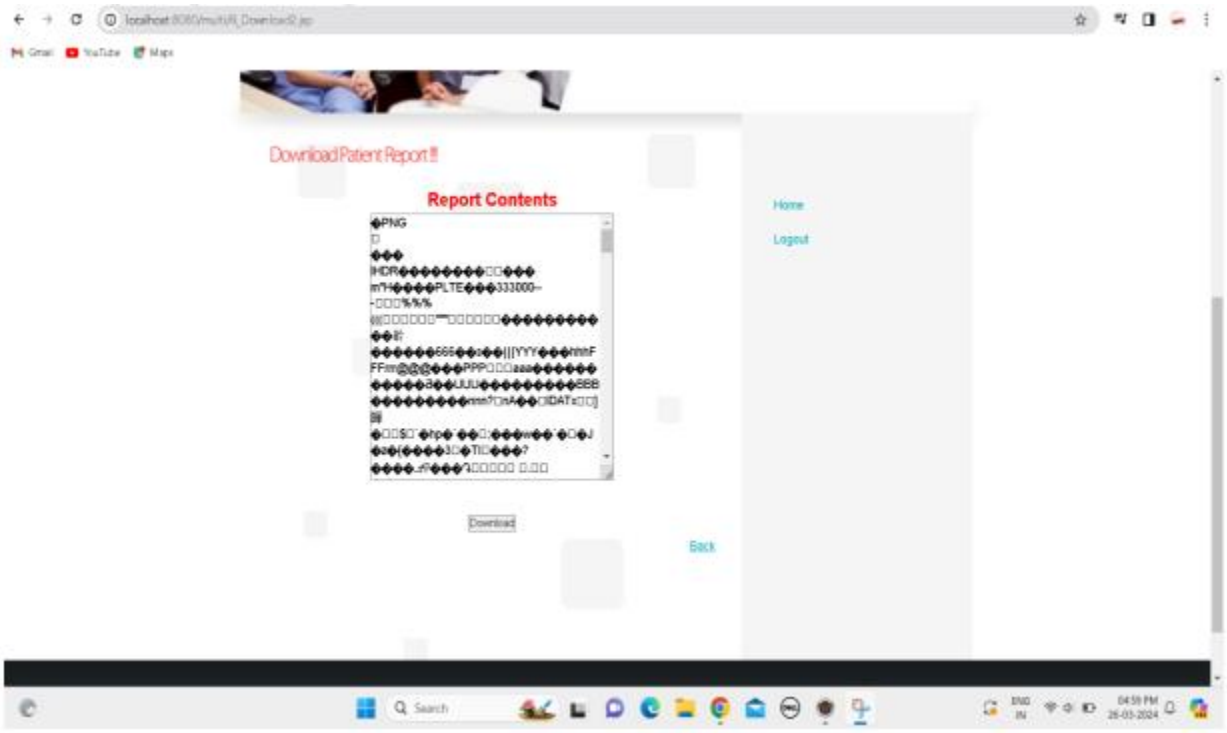
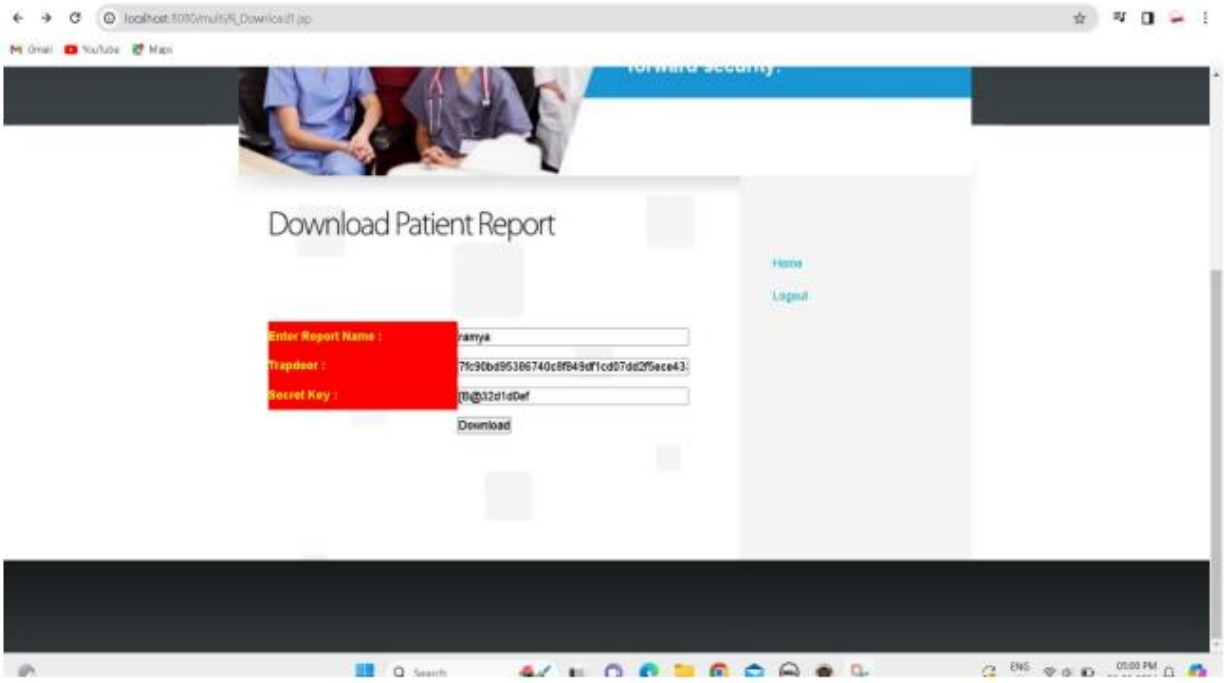


Figure 7encrypted report

Download encrypted report



ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Figure 8 download report

CONCLUSION & FUTURE ENHANCEMENT

Conclusion:

In this paper, we proposed an efficient and feasible MABKS system to support multiple authorities, in order to avoid having performance bottleneck at a single point in cloud systems. Furthermore, the presented MABKS system allows us to trace malicious AAs (e.g., to prevent collusion attacks) and support attribute update (e.g., to avoid unauthorized access using outdated secret keys). We then demonstrated the selective security level of the system in selective-matrix and selective-attribute models under decisional q-parallel BDHE and DBDH assumptions, respectively. We also evaluated the system's performance and demonstrated that significant computation and storage cost reductions were achieved, in comparison to prior ABKS schemes. However, the main flaw is that the MABKS system cannot support expressive search queries such as conjunctive keyword search, fuzzy search, subset search and so on. The future work will focus on building an efficient and flexible index construction so that the MABKS system is capable of supporting various search requests.

Future Enhancement:

Unfortunately, merely removing unique identifiers of users cannot protect their privacy, as databases can be linked to each other based on their quasi-identifiers. Doing so, adversaries can reveal sensitive information about the users and compromise their privacy. In this section, we review the existing approaches for the anonymization of spatiotemporal datasets.

BIBLIOGRAPHY

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 healthcare 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," IEEETransactions 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, "Attributebased keyword search over hierarchical data in cloud computing," 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 attack 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 proxyoriented 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.

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

12) Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, "Practical attributebased 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 attributebased 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 attributebased keyword search with fine-grained owner-enforced search authorization in the cloud," IEEE Transactions on Parallel 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.
16) M. Chase, "Multi-authority attribute-based encryption," in Proc.IACR Theory of Cryptography Conference (TCC'07), 2007, pp. 515–534.
17) K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multiauthority cloud storage," IEEE transactions on parallel and distributed systems, vol. 25, no. 7, pp. 1735–1744, 2014.
18) K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "Raac: Robust and auditable access control with multiple attribute authorities for public cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.
19) V. K. A. Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "Efficient decentralized multiauthority attribute based encryption for mobile cloud data storage," Journal of Network and Computer Applications, vol. 129, pp. 25–36, 2019.
20) J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1274–1288, 2015.
21) Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, "Efficient traceable authorization search system for secure cloud storage," IEEE Transactions on Cloud Computing, vol. PP, pp. 1–14, 2018.
22) J. Ning, Z. Cao, X. Dong, and L. Wei, "White-box traceable cp-abe for cloud storage service: how to catch people leaking their access credentials effectively," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 883–897, 2018.
23) Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221,2011.