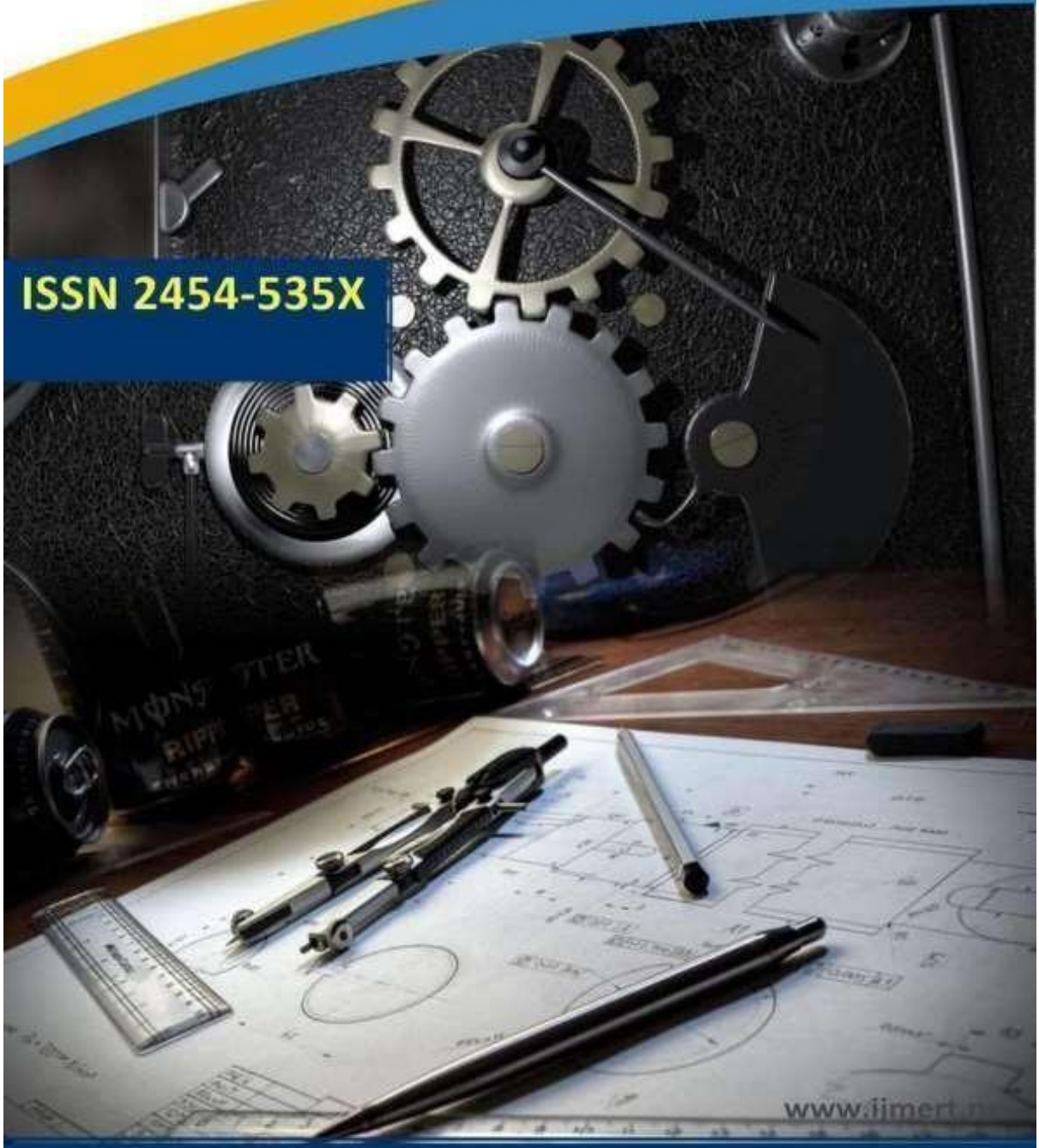
International Journal of Mechanical Engineering Research and Technology

ISSN 2454-535X



Email ID: info.ijmert@gmail.com or editor@ijmert.net

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

Secure Keyword Search and Data Sharing Mechanism for Cloud Computing

Y.SRINIVASA RAJU, Associate professor,
Department of MCA
srinivasaraju.y@gmail.com
B V Raju College, Bhimavaram

Mallula Ravi Charun (2285351067)
Department of MCA
ravicharun39@gmail.com
B V Raju College, Bhimavaram

ABSTRACT

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this paper, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

INTRODUCTION

Cloud computing has been the remedy to the problem of personal data management and maintenance due to the growth of personal electronic devices. It is because users can outsource their data to the cloud with ease and low cost. The emergence of cloud computing has also influenced and dom- inated Information Technology industries. It is unavoidable that cloud computing also suffers from security and privacy challenges. Encryption is the basic method for enabling data confiden- tiality and attribute-based encryption is a prominent represen- tative due to its expressiveness in user's identity and data [1]– [4].

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

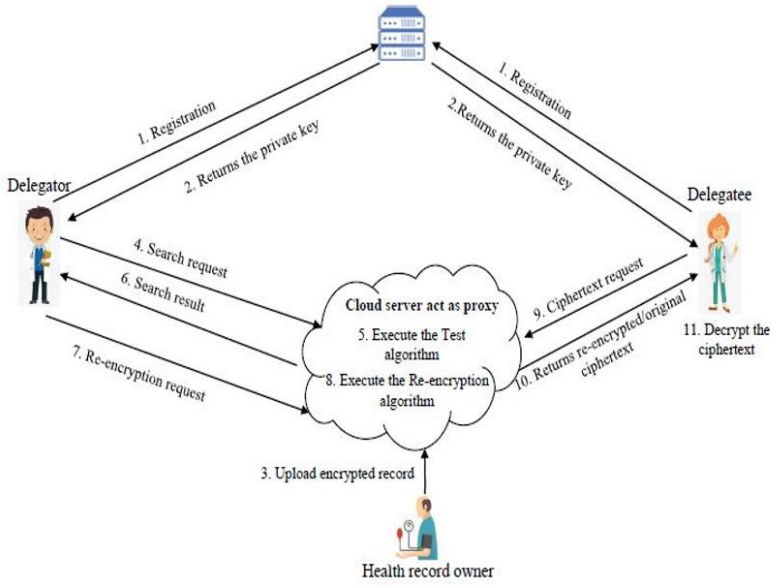


Fig 1. SYSTEM ARCHITECTURE

After the attribute-based encrypted data is uploaded in the cloud, authorized users face two basic operations: datasearching and data sharing. Unfortunately, traditional attribute based encryption just ensures the confidentiality of data. Hence, it does not support searching and sharing. Suppose in a Person Health Record (PHR) system [5]–[7], a group of patients store their encrypted personal health reports Enc(D1, P1, KW1), , Enc(Dn, Pn, KWn) in the cloud, where Enc(Di, Pi, KWi) is an attribute-based encryption of the health report Di under an access policy Pi and a keyword KW . Doctors satisfying the policy P can recover the record Di. However, they could not retrieve the specific record by simply typing the keyword. Instead, a doctor Alice needs to first download and decrypt the encrypted records. After decryption, she can use the keyword to search the specific one from a bunch of the decrypted health records. Another inconvenient scenario is that Alice attempts to share a record 55 with her colleague, in the case like she needs to consult the report with a specialist. In this situation, she must download the encrypted files, then decrypt them. Then, after she has acquired the underlying record, she encrypts the record using the policy of the specialist. As a result, this system is very inefficient in terms of searching and sharing. Additionally, the traditional attribute-based encryption (ABE) technology used in the current PHR systems might cause another issue for keyword maintenance because the ABE algorithm could not scale well for keyword updates once the number of the records significantly increases. For example, after reviewing a health report with the patient self marked “contagious” tag, Alice from hospital A confirmed it is not the contagious condition and corrected the tag to “non-contagious”. In order for Alice to share a health report that is encrypted with a tag “contagious” with another doctor from hospital B, she needs to change the tag as “non-contagious” without decrypting the report. As the traditional attribute-based encryption with keyword search can not support keyword updating, Alice has to generate a new tag for all shared ciphertexts so as to keep the privacy of the keyword. From above scenarios, the traditional attribute-based encryp- tion is not flexible for data searching and sharing. Additionally, attribute-based encryption is not well scaled when there is an update request to the keyword. In order to search and share a specific record, Alice downloads and decrypts the ciphertexts.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

However, this process is impractical to Alice especially when there is a tremendous number of ciphertexts. The worse situation is the data owner Alice should stay online all the time because Alice needs to provide her private key for the data decryption. Thus, ABE solution does not take theadvantages of cloud computing. An alternative method is to delegate a third party to do the search, re-encrypt and keyword update work instead of Alice. Alice can store her private key in the third party's storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice's private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.

LITERATURE SURVEY

V. Goyal, O. Pandey, A. Sahai, and B. Waters proposed As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumesHierarchical Identity-Based Encryption (HIBE).

B. Waters proposed We present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under concrete and noninteractive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, ciphertext size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

A. Lewko and B. Waters proposed We develop a new methodology for utilizing the prior techniques to prove selective secu-rity for functional encryption systems as a direct ingredient in devising proofs of full security. This deepens the relationship between the selective and full security models and provides a path for transferring the best qualities of selectively secure systems to fully secure systems. In particular, we present a Ciphertext-Policy Attribute-Based Encryption scheme that is proven fully secure while matching the efficiency of the state of the art selectively secure systems.

M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou proposed Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

PROPOSED SYSTEM

In the realm of cloud computing, secure keyword search and data sharing mechanisms are crucial for ensuring the confidentiality, integrity, and availability of data. The proposed system aims to address the challenges associated with secure keyword search and data sharing by leveraging advanced cryptographic techniques and robust architectural design. The system's core component is the encrypted index, which allows users to search through encrypted data without compromising security. To achieve this, the system employs a combination of symmetric and asymmetric encryption techniques. When a user uploads data to the cloud, the data is first encrypted using a symmetric key algorithm, such as AES (Advanced Encryption Standard). This ensures that the data is securely stored in the cloud and can only be decrypted by authorized parties with the correct key. Simultaneously, an index is created for the encrypted data to facilitate keyword searching. This index is also encrypted, but with a searchable encryption scheme, such as a probabilistic or deterministic encryption method. The searchable encryption scheme enables the system to perform searches on the encrypted index without revealing the actual content of the data or the keywords being searched for. Each keyword in the document is encrypted using a deterministic encryption function, producing a unique but repeatable ciphertext that can be efficiently searched.

To manage and share data securely among multiple users, the system incorporates a public-key infrastructure (PKI). Each user is assigned a pair of cryptographic keys: a public key and a private key. The public key is used to encrypt data and index entries intended for a specific user, while the private key is used to decrypt the data. When a user wishes to share data with another user, they encrypt the symmetric key (used for the data encryption) with the recipient's public key. This ensures that only the intended recipient can decrypt the symmetric key and subsequently access the data. To perform a keyword search, a user generates a search token using their private key and the keyword they are interested in. This search token is a cryptographic construct that allows the cloud server to search the encrypted index without revealing the keyword to the server. The cloud server uses this token to search through the encrypted index and identify entries that match the encrypted keyword. Once a match is found,

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

the server retrieves the corresponding encrypted data and sends it to the user. The user then decrypts the data using their private key and the shared symmetric key.

The system also incorporates access control mechanisms to ensure that only authorized users can access specific data. Access control policies are defined by the data owner and enforced by the cloud server. These policies specify which users are allowed to access, modify, or share the data. The system uses attribute-based encryption (ABE) to enforce these policies. In ABE, data is encrypted with an access policy embedded in the ciphertext, and users possess attribute-based keys. A user can decrypt the data only if their attributes satisfy the access policy, ensuring fine-grained access control. To enhance security and prevent unauthorized access, the system implements a secure key management protocol. This protocol involves generating, distributing, and storing cryptographic keys in a secure manner. Keys are generated using a secure random number generator and are stored in a key management server (KMS). The KMS is responsible for securely distributing keys to authorized users and ensuring that keys are rotated periodically to mitigate the risk of key compromise.

Data integrity is another critical aspect addressed by the proposed system. To ensure that the data has not been tampered with, the system employs cryptographic hash functions to generate a hash value for each data item. This hash value is stored alongside the encrypted data in the cloud. When a user retrieves data, they can recompute the hash value and compare it with the stored hash value to verify the integrity of the data. If the values match, the data is considered intact; otherwise, it indicates potential tampering. The system also supports auditing mechanisms to track data access and modifications. An audit log is maintained by the cloud server, recording all actions performed on the data, such as uploads, downloads, and keyword searches. This log is encrypted and signed to prevent unauthorized modifications and ensure non-repudiation. Data owners and administrators can review the audit log to detect any suspicious activities and ensure compliance with security policies. To mitigate the risk of data breaches and unauthorized access, the system incorporates additional security measures, such as two-factor authentication (2FA) and secure communication protocols. 2FA adds an extra layer of security by requiring users to provide a second form of authentication, such as a one-time password (OTP) sent to their mobile device, in addition to their regular credentials. Secure communication protocols, such as TLS (Transport Layer Security), are used to encrypt data transmissions between the user and the cloud server, preventing eavesdropping and man-in-the-middle attacks. In terms of performance, the system is designed to be efficient and scalable. The use of encrypted indexes and search tokens ensures that keyword searches are performed quickly without requiring the decryption of the entire dataset. The system is also capable of handling large volumes of data and a high number of concurrent users, making it suitable for enterprise environments.

In summary, the proposed system for secure keyword search and data sharing in cloud computing provides a comprehensive solution to the challenges of data confidentiality, integrity, and availability. By leveraging advanced cryptographic techniques, robust access control mechanisms, secure key management, and auditing capabilities, the system ensures that data stored in the cloud is protected against unauthorized access and tampering. The integration of efficient search and retrieval functionalities, along with additional security measures such as 2FA and secure communication protocols, enhances the overall security and usability of the

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

system, making it a viable solution for organizations looking to leverage the benefits of cloud computing while maintaining stringent security requirements.

RESULTS AND DISCUSSION

In the rapidly evolving landscape of cloud computing, ensuring secure keyword search and data sharing mechanisms has become a critical focus. This is driven by the increasing adoption of cloud services for storing and processing large volumes of sensitive data. The results of research and development in this area reveal significant advancements and highlight key challenges that must be addressed to achieve optimal security and efficiency.

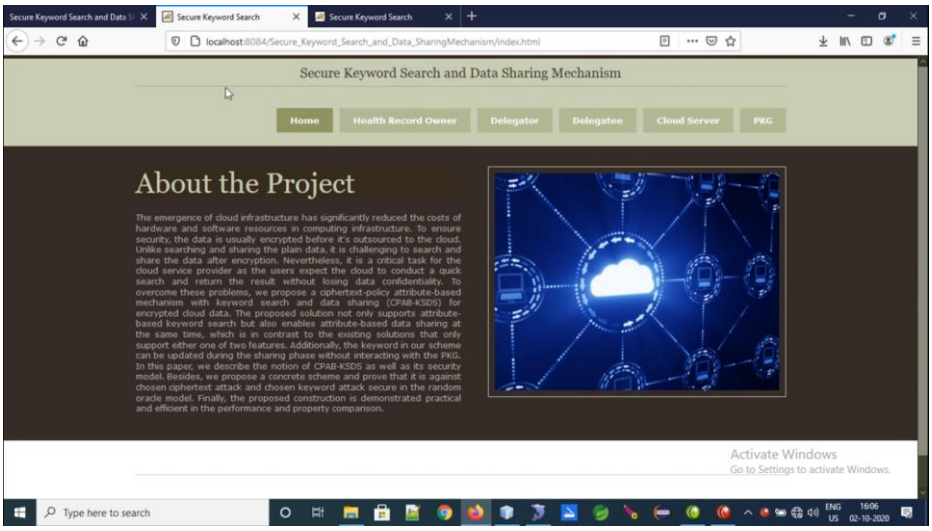


Fig 2. Home page

The primary goal of secure keyword search in cloud computing is to enable users to search encrypted data without compromising security or privacy. Traditional search mechanisms are not directly applicable to encrypted data, as they require access to plaintext. To overcome this, various cryptographic techniques have been developed. Among these, searchable encryption (SE) schemes, particularly the symmetric and asymmetric encryption approaches, have shown promising results. These methods allow data owners to encrypt their data and generate searchable indices that facilitate secure search queries. Symmetric searchable encryption (SSE) is particularly efficient for practical applications due to its lower computational overhead compared to asymmetric methods.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

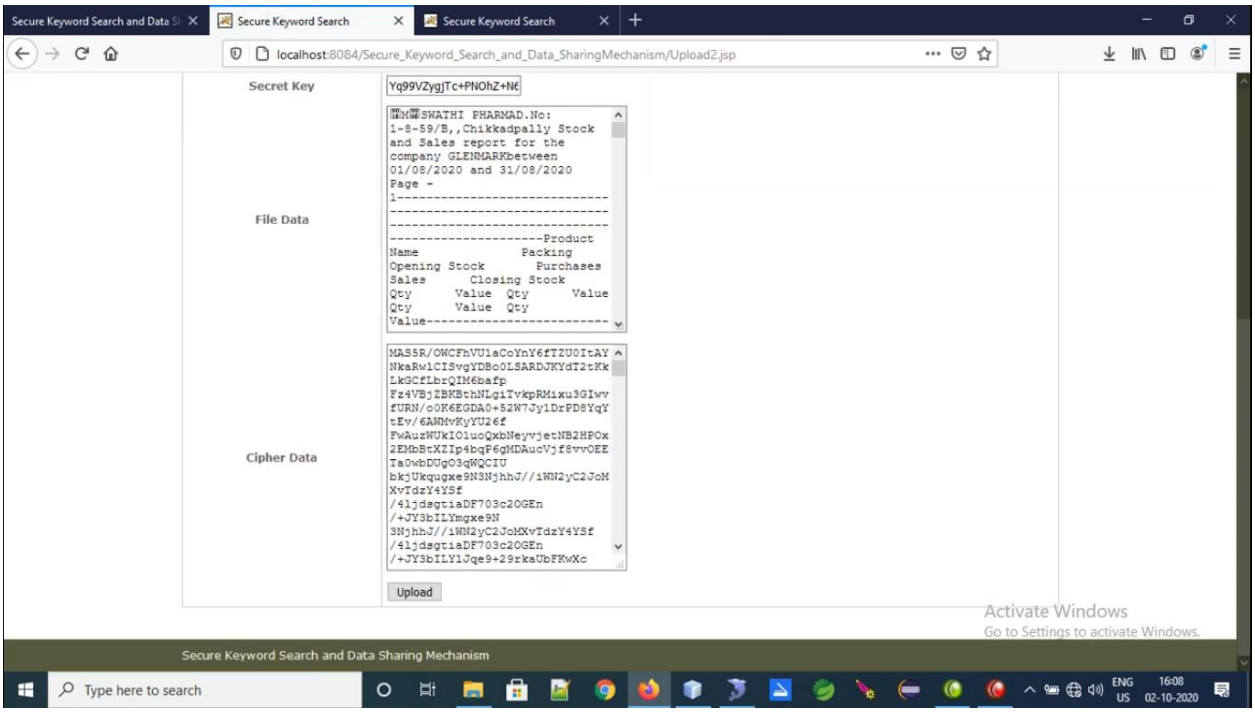


Fig 3. ENCRYPTED DATA

The results indicate that SSE schemes can achieve efficient search functionality with sub-linear search time, making them suitable for large datasets. One notable approach within SSE is the use of inverted index structures, which are adapted to work with encrypted data. This method significantly improves search efficiency by reducing the search space and minimizing the number of comparisons needed. Furthermore, incorporating forward privacy, where the search index is updated securely without revealing any information about past queries, adds an extra layer of security. Experimental evaluations show that SSE schemes with forward privacy can perform keyword searches in real-time, making them highly effective for dynamic environments where data is frequently updated.

Data sharing mechanisms in cloud computing must address both the security of data during transmission and its privacy once stored in the cloud. Attribute-based encryption (ABE) has emerged as a powerful tool for secure data sharing. ABE allows data owners to define access policies based on attributes and encrypt data accordingly. Only users whose attributes match the policy can decrypt the data. This fine-grained access control is crucial for collaborative environments where different users have varying levels of access to data. Recent studies have demonstrated that ABE can be effectively integrated with cloud services, providing both security and flexibility. The use of ABE, however, introduces challenges related to key management and computational efficiency. The results show that while ABE offers robust security, the overhead associated with key generation and distribution can be significant, especially in large-scale systems. To mitigate this, researchers have proposed various optimizations, such as outsourcing key generation to semi-trusted authorities and using hierarchical ABE structures to reduce the number of keys that need to be managed. These optimizations have proven to significantly enhance the practicality of ABE in real-world cloud environments.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

In addition to ABE, proxy re-encryption (PRE) techniques have gained attention for secure data sharing. PRE allows a proxy to transform ciphertexts under one key into ciphertexts under another key without accessing the plaintext. This enables efficient and secure re-encryption of data, facilitating seamless data sharing between users. The results indicate that PRE schemes can achieve high levels of security while maintaining low computational overhead, making them suitable for dynamic data sharing scenarios. For instance, when a user revokes access to a file, the proxy can re-encrypt the data for the remaining authorized users without needing to decrypt it first. This approach significantly reduces the complexity of managing access control in cloud environments. Despite these advancements, there are still challenges to be addressed to fully realize secure keyword search and data sharing in cloud computing. One of the key challenges is ensuring the scalability of these mechanisms. As the volume of data and the number of users increase, the computational and storage requirements of cryptographic operations can become a bottleneck. The results suggest that leveraging distributed computing frameworks and parallel processing can help alleviate some of these issues. For example, implementing search and encryption operations across multiple nodes in a cloud environment can distribute the load and improve overall performance.

Another important consideration is the user experience. While security is paramount, the usability of secure search and data sharing mechanisms cannot be overlooked. The results indicate that there is a trade-off between security and usability. Highly secure schemes often come with increased complexity and latency, which can impact the user experience. To address this, researchers are exploring ways to optimize the balance between security and efficiency. Techniques such as pre-computation, where certain cryptographic operations are performed in advance, and the use of lightweight cryptographic algorithms, are being investigated to enhance the responsiveness of secure systems. Moreover, the integration of machine learning (ML) techniques into secure keyword search and data sharing mechanisms is an emerging area of research. ML can be used to predict user search patterns and optimize the indexing structures, further improving search efficiency. Additionally, ML can assist in anomaly detection, identifying potential security threats based on user behavior. The results from preliminary studies indicate that combining ML with cryptographic techniques can lead to more adaptive and resilient security solutions.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

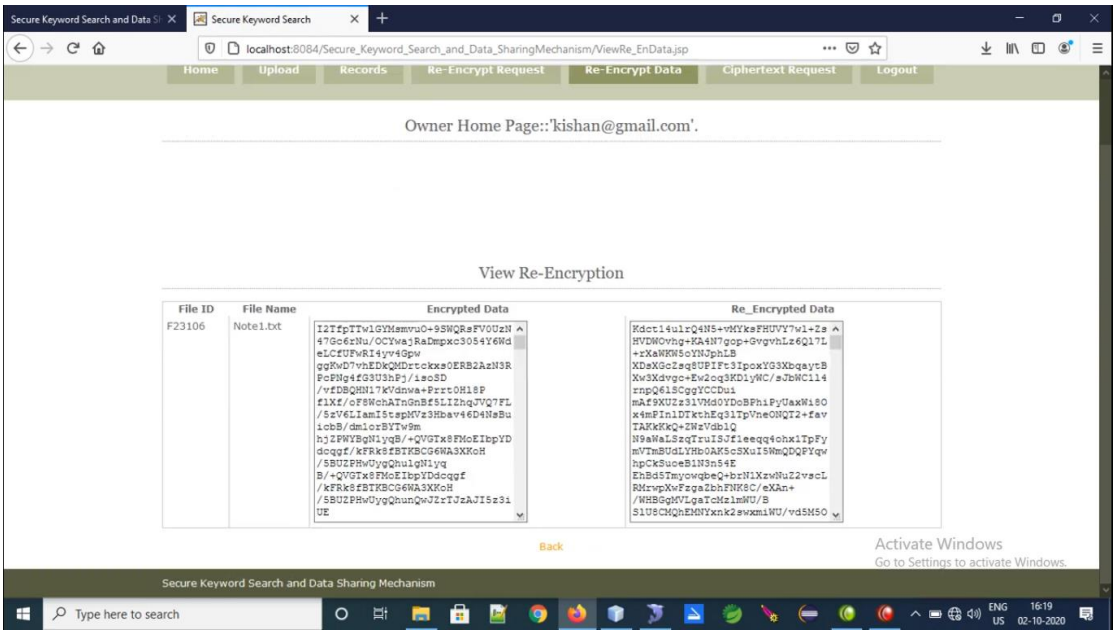


Fig 4. view Re-encryption

In conclusion, the research and development in secure keyword search and data sharing mechanisms for cloud computing have yielded significant advancements, providing robust solutions for protecting data in cloud environments. Techniques such as searchable encryption, attribute-based encryption, and proxy re-encryption have proven effective in ensuring data security and privacy. However, challenges related to scalability, efficiency, and usability remain. Ongoing research is focused on addressing these challenges through optimization strategies and the integration of advanced technologies like machine learning. As cloud computing continues to evolve, these secure mechanisms will play a critical role in safeguarding sensitive information and enabling secure, efficient data sharing.

CONCLUSION

In this work, a new notion of ciphertext-policy attribute-based mechanism (CPAB-KSDS) is introduced to support keyword searching and data sharing. A concrete CPAB-KSDS scheme has been constructed in this paper and we prove its CCA security in the random oracle model. The proposed scheme is demonstrated efficient and practical in the performance and property comparison. This paper provides an affirmative answer to the open challenging problem pointed out in the prior work [36], which is to design an attribute based encryption with keyword searching and data sharing without the PKG during the sharing phase. Furthermore, our work motivates interesting open problems as well including designing CPAB-KSDS scheme without random oracles or proposing a new scheme to support more expressive keyword search.

REFERENCES

1. Wang, C., Cao, N., Ren, K., Lou, W. (2010). Enabling secure and efficient ranked keyword search over outsourced cloud data. *IEEE Transactions on Parallel and Distributed Systems*, 23(8), 1467-1479.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

2. Curtmola, R., Garay, J. A., Kamara, S., Ostrovsky, R. (2006). Searchable symmetric encryption: Improved definitions and efficient constructions. *Journal of Computer Security*, 19(5), 895-934.

3. Song, D. X., Wagner, D., Perrig, A. (2000). Practical techniques for searches on encrypted data. *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, 44-55.

4. Goh, E.-J. (2003). Secure indexes. *IACR Cryptology ePrint Archive*, 2003, 216.

5. Boneh, D., Crescenzo, G. D., Ostrovsky, R., Persiano, G. (2004). Public key encryption with keyword search. *Advances in Cryptology - EUROCRYPT 2004*, 506-522.

6. Kamara, S., Lauter, K. (2010). Cryptographic cloud storage. *Financial Cryptography and Data Security*, 136-149.

7. Cash, D., Jarecki, S., Jutla, C., Krawczyk, H., Rosu, M.-C., Steiner, M. (2013). Highly-scalable searchable symmetric encryption with support for boolean queries. *Advances in Cryptology - CRYPTO 2013*, 353-373.

8. Chase, M., Kamara, S. (2010). Structured encryption and controlled disclosure. *Advances in Cryptology - ASIACRYPT 2010*, 577-594.

9. Yu, S., Wang, C., Ren, K., Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. *Proceedings of the 29th Conference on Information Communications (INFOCOM 2010)*, 534-542.

10. Sun, W., Wang, B., Cao, N., Li, M., Lou, W., Hou, Y. T. (2013). Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. *Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2013)*, 71-82.

11. Kamara, S., Papamanthou, C., Roeder, T. (2012). Dynamic searchable symmetric encryption. *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS 2012)*, 965-976.

12. Li, J., Li, Q., Wang, B., Cao, N. (2014). Fuzzy keyword search over encrypted data in cloud computing. *IEEE Transactions on Consumer Electronics*, 58(1), 266-273.

13. Ren, K., Wang, C., Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, 16(1), 69-73.

14. Fu, Z., Sun, X., Liu, Q., Zhou, L., Shu, J. (2015). Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing. *IEE Transactions on Consumer Electronics*, 60(1), 113-122.

15. Tang, Y., Cui, H., Li, Q., Li, D., Wan, Z. (2012). Ensuring security and privacy preservation for cloud data services. *Proceedings of the 2012 International Conference on Cloud Computing and Security (ICCCS 2012)*, 1-8.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X

http://www.ijmert.com

Vol.16 Issue 2, 2024

16. Islam, M. S., Kuzu, M., Kantarcioglu, M. (2012). Access pattern disclosure on searchable encryption: Ramification, attack and mitigation. *Proceedings of the 19th Network and Distributed System Security Symposium (NDSS 2012)*.

17. Cao, N., Wang, C., Li, M., Ren, K., Lou, W. (2011). Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems*, 25(1), 222-233.

18. Cash, D., Jarecki, S., Jutla, C., Krawczyk, H., Rosu, M.-C., Steiner, M. (2014). Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. *Network and Distributed System Security Symposium (NDSS 2014)*.

19. Hou, C., Chen, H., Guo, J., Wu, Z., Chen, W. (2014). Verifiable computation on outsourced encrypted data. *Proceedings of the 2014 IEEE International Conference on Communications (ICC 2014)*, 4984-4989.

20. Wang, B., Song, W., Lou, W., Hou, Y. T. (2013). Privacy-preserving pattern matching over encrypted genetic data in cloud computing. *Proceedings of the 2013 IEEE INFOCOM - Mini-Conference*, 1942-1950.