Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

STRENGTHENING CLOUD COMPUTING SECURITY: MECHANISMS FOR SECURE KEYWORD SEARCH AND DATA SHARING

R.Deepika,*Assistant Professor CSE, Vaagdevi College of Engineering (Autonomous), India*
A.Ashwith Sai,*UG student, CSE, Vaagdevi College of Engineering (Autonomous), India*
A.Likitha,*UG student, CSE, Vaagdevi College of Engineering (Autonomous), India*
V.Sowjith,*UG student CSE, Vaagdevi College of Engineering (Autonomous), India*
S.Nithin Sai,*UG student CSE, Vaagdevi College of Engineering (Autonomous), India*

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.

1. INTRODUCTION

PURPOSE OF THE PROJECT

The project "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" [1] aims to develop a robust system that ensures the security and privacy of sensitive data stored in cloud environments. By implementing advanced encryption, access control, and homomorphic computation techniques, the project seeks to enable authorized users to securely search for specific keywords within their encrypted data while allowing controlled sharing of encrypted content with selected parties, all while maintaining data confidentiality, integrity, and compliance with privacy regulations.

SCOPE OF THE PROJECT

The scope of the project encompasses the design and implementation of a comprehensive system for secure keyword-based search and controlled data sharing within cloud computing environments. This includes developing advanced encryption mechanisms, access control features, and efficient indexing techniques to enable authorized users to search encrypted data while maintaining confidentiality, and allowing data owners to selectively share encrypted content with specific entities. The project aims to provide a user-friendly interface, ensure data integrity, scalability, regulatory compliance, and comprehensive documentation [2], ultimately enhancing the security and privacy of sensitive data stored and shared in cloud computing.

PROBLEM DEFINITION

The project addresses the challenge of securing sensitive data storage and retrieval in cloud computing, where conventional approaches may compromise data privacy and security. Existing methods lack efficient and privacy-preserving mechanisms for users to conduct keyword-based searches and controlled sharing of encrypted data while preventing unauthorized access and exposure of the underlying content. The project aims to overcome these limitations by developing advanced techniques that ensure data confidentiality, integrity, and access control, enhancing the security posture of cloud-based data management.

2. LITERATURE SURVEY

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) [3].

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) [4] 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.

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.

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 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 [4] 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

3. PROBLEM STATEMENT

The traditional attribute-based encryption 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 cipher texts. However, this process is impractical to Alice especially when there are a tremendous number of cipher texts. 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 the advantages 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 [3]. 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.

3.1 LIMITATIONS

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.

4. PROPOSED SYSTEM

Prior work did not demonstrate that the existing attribute-based mechanisms could both support keyword search and data sharing in one scheme without resorting to PKG. Therefore, a new attribute-based mechanism is needed to achieve the goal for the above PHR scenario. One may argue that the problem can be trivially solved by combining an AB-PRE scheme and attribute-based keyword search scheme (AB-KS).However, the combination could result in two major issues: 1) the combined scheme is not CCA secure, 2) it is vulnerable to collusion attack Therefore, a secure scheme is desired to fully support keyword searching, data sharing as well as the protection ofthe privacy of keyword. All of these concerns motivate us to design a mechanism that:

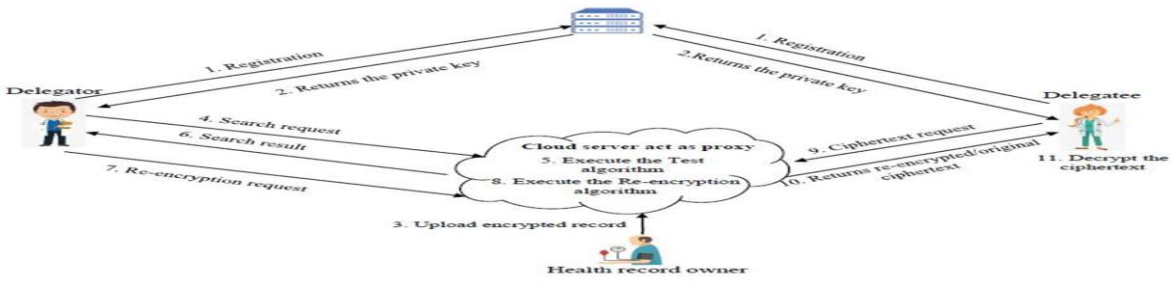
1) Allows the data owner to search and share the encrypted health report without the unnecessary decryption process. 2) Supports keyword updating during the data sharing phase. 3) More importantly, does not need the exist of the PKG, either in the phase of data sharing or keyword updating. 4) The data owner can fully decide who could access the data he encrypted.

We first introduce a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The searching and sharing functionality are enabled in the ciphertext-policy setting. Furthermore, our scheme supports the keyword to be updated during the sharing phase. After presenting the construction of our mechanism, we proof its chosen ciphertext attack (CCA) and chosen keyword attack (CKA) [5] security in the random oracle model. Theproposed construction is demonstrated practical and efficient in the performance and property comparison.

4.1 ADVANTAGES OF PROPOSED SYSTEM:

We describe the notion of CPAB-KSDS as well as its security model. The proposed construction is demonstrated practical and efficient in the performance and property comparison.

5. SYSTEM ARCHITECHURE



6. IMPLEMENTATION

6. 1.System Initialization

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024

System Initialization: This phase is executed by the PKG. The PKG generates the system public parameters that are publicly available for all the participants of the system and the master secret key which is kept private by the PKG.

6.2.Registration

Registration: The registration phase is executed by the PKG. When each user issues a registration request to the PKG, the PKG generates a private corresponds to his attribute set.

6.3. Ciphertext.

Ciphertext Upload: The personal health record owner encrypts his record with the original recipient's policy and the keyword, and then upload the encrypted record to the cloud server.

6.4. Ciphertext Search:

The recipient generates a search token and issues a search request contains the search token to the cloud server. The cloud server searches the ciphertext via the Test algorithm and returns the search result to the recipient.

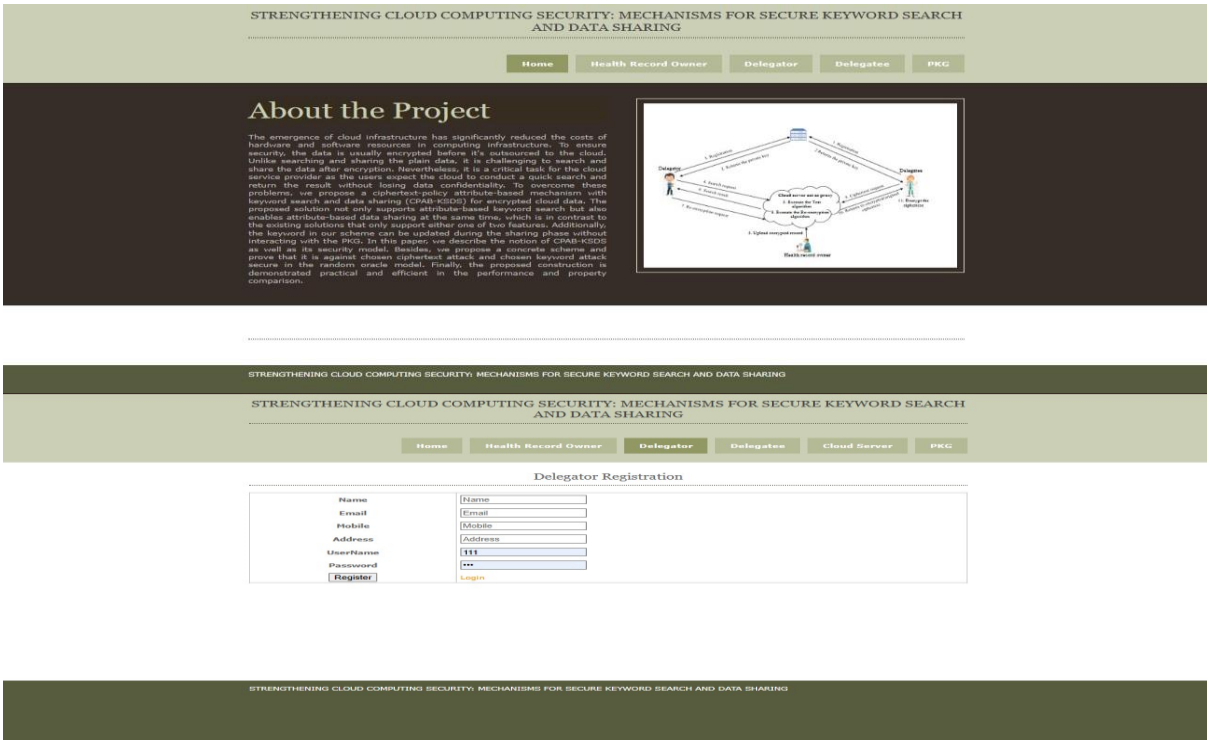
6.5. Re-encryption:

The delegator generates a re-encryption key and issues a re-encryption request contains the re-encryption key to the cloud server. The cloud server converts the original encrypted record to a re-encrypted ciphertext under a new access policy.

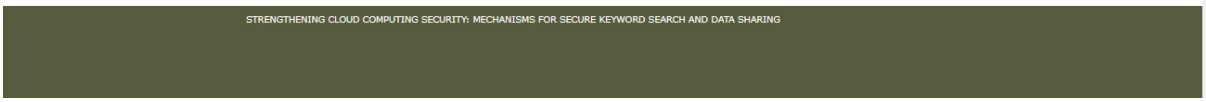
6.6. Decryption:

The recipient (a delegatee or a delegator) requests a re-encrypted (or an original) ciphertext from the cloud server and then decrypts the ciphertext with his own private key to get the underlying record. Note that, a delegatee may act as a delegator for other participants.

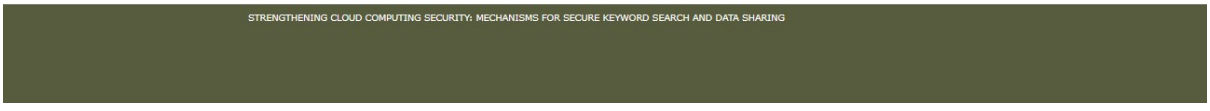
7. EXPECTED OUTCOMES



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, May : 2024



8. 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.

8.1 FUTURE SCOPE

Strengthening cloud computing security is crucial as more businesses rely on cloud services. Future scope includes advancements in encryption, multi-factor authentication, and AI-driven threat detection to enhance protection against evolving cyber threats. Additionally, there's a focus on regulatory compliance, secure coding practices, and proactive risk management strategies to mitigate potential vulnerabilities. Future scope includes implementing advanced encryption techniques like homomorphic encryption to ensure privacy during keyword searches and secure data sharing. Additionally, blockchain technology can be leveraged to establish transparent and immutable records of data access and sharing activities. Furthermore, advancements in secure data sharing protocols and access control mechanisms will play a crucial role in enhancing the overall security posture of cloud environments.

9. REFERENCES

1.Kai Zhang, Ximeng Liu, Yanping Li, Tao Zhang, Shuhua Yang, "A Secure Enhanced Key-Policy Attribute-Based Temporary Keyword Search Scheme in the Cloud", Access IEEE, vol. 8, pp. 127845-127855, 2020.

2.Hao Yan, Wenming Gui, "Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving", Access IEEE, vol. 9, pp. 45822-45831, 2021.

3.Hua Shen, Mingwu Zhang, Hao Wang, Fuchun Guo, Willy Susilo, "Efficient and Privacy-Preserving Massive Data Processing for Smart Grids", Access IEEE, vol. 9, pp. 70616-70627, 2021.

4.Jianfei Sun, Dajiang Chen, Ning Zhang, Guowen Xu, Mingjian Tang, Xuyun Nie, Mingsheng Cao, "A Privacy-Aware and Traceable Fine-Grained Data Delivery System in Cloud-Assisted Healthcare IIoT", Internet of Things Journal IEEE, vol. 8, no. 12, pp. 10034-10046, 2021.

5.Mingwu Zhang, Yu Chen, Jiajun Huang, "SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems", Systems Journal IEEE, vol. 15, no. 2, pp. 2980-2988, 2021.