STRENGTHNING CLOUD COMPUTING SECURITY MECHANISM FORSECURE KEYWORD SEARCH AND DATA SHARING

[1] Dr. A. Laxmikanth,[2] I.Akshay,[3] K.Pooja,[4] B.Ajay Reddy,[5] K.Uday Kumar
[1] Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

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 dominated Information Technology industries. It is unavoidable that cloud computing also suffers from security and privacy challenges. Encryption is the basic method for enabling data confidentiality and attribute-based encryption is a prominent representative due to its expressiveness in user's identity and data [1]– [4]. After the attribute- based encrypted data is uploaded in the cloud, authorized users face two basic operations: data searching 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.

I. INTRODUCTION

The project "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" 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.

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloudshaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing

All the existing cloud servers try to store the data in a plain text manner rather than in a

encrypted manner. If the encryption key is exposed, the data can be easily accessed by the intruder. In the existing system there is no security for the data even it is encrypted because there is only single cipher key is generated for that data.

As organizations increasingly migrate their data and operations to cloud computing environments, ensuring robust security mechanisms becomes paramount to safeguard sensitive information and maintain the trust of users. Among the critical aspects of cloud security, implementing measures for secure keyword search and data sharing is crucial. This involves protecting data confidentiality, integrity, and accessibility, especially when dealing with sensitive information. In this context, the following strategies are proposed to strengthen cloud computing security mechanisms, with a focus on enhancing the security of keyword searches and facilitating secure data sharing. Thesestrategies encompass encryption, access controls, secure search methods, and proactive monitoring, aiming to create a resilient and trustworthy cloud environment for both enterprises and individual users. the adoption of cloud computing has revolutionized the way organizations manage and access data, offering unparalleled scalability and flexibility. However, the benefits of cloud computing come with the responsibility to fortify security measures, particularly concerning sensitive data, secure keyword searches, and seamless data sharing. In this era of constant cyber threats, ensuring the confidentiality and integrity of data is critical. This introduction outlines strategies to enhance cloud computing security mechanisms specifically tailored for secure keyword searches and data sharing.

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, ultimately enhancing the security and privacy of sensitive data stored and shared in cloud computing

The scope of a project focused on strengthening cloud computing security mechanisms for secure keyword search and data sharing is comprehensive, encompassing various aspects of cloud security, cryptography, access controls, and user interactions. Here's a breakdown of the potential scope for such a project:

II LITERATURE SURVEY

TITLE: "Low-cost RF based online patient monitoring using web and mobile applications".

AUTHORS: V. Goyal, O. Pandey, A. Sahai, and B. Waters

ABSTRACT: 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 encryptingdata, 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 labelled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstratethe applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

TITLE: "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient and Provably Secure Realization"

AUTHORS: B. Waters

ABSTRACT: 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. Our first system is proven selectively secure under a assumption that we callthe 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 tradeoff's to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions**.**

TITLE: " New proof methods for attribute-based encryption: Achieving full security through selective techniques "

AUTHORS: A. Lewko and B. Waters

ABSTRACT: We develop a new methodology for utilizing the prior techniques to prove selective security 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 system

TITLE: "Using Erasure Codes Efficiently for Storage in a Distributed System".

AUTHORS: M. K. Aguilera, R. Janakiraman, and L. Xu Erasure

ABSTRACT:codes provide space- optimal data redundancy to protect against data loss. A common use is to reliably store data ina distributed system, where erasure-coded data are kept in different nodes to tolerate node failures without losing data. In this paper, we propose a new approach to maintain ensure encoded data in a distributed system. The approach allows the use of space efficient k-of-n erasure codes where n and k are large and the overhead n-k is small. Concurrent updates and accesses to data are highly optimized: in common cases, they require no locks, no two-phase commits, and no logs of old versions of data. We evaluate our approach using an implementation and simulations for larger systems.

TITLE: "Secret-Sharing Schemes: A Survey,"

AUTHORS: Amos beimel.

ABSTRACT: A. Beimel, A secret-sharing scheme is a method by which a dealer distributes sharesto parties such that only authorized subsets of parties can reconstruct the secret. Secret-sharing schemes are important tools in cryptography and they are used as a building box in many secure protocols, e.g., general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control, attribute-based encryption, and generalized oblivious transfer. In this survey, we will describe the most important constructions of secret- sharing schemes, explaining the connections between secret-sharing schemes and monotone formulae and monotone span programs. The main problem with known secret-sharing schemes is the large share size: it is exponential in the number of parties. We conjecture that this is unavoidable. We will discuss the known lower bounds onthe share size. These lower bounds are fairly weak.

and there is a big gap between the lower and upper bounds. For linear secret-sharing schemes, whichis a class of schemes based on linear algebra that contains most known schemes, super- polynomial lower bounds on the share size are known. We will describe the proofs of these lower bounds.

III SYSTEM ANALYSIS

EXISTING SYSTEM

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. 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.

All the existing cloud servers try to store the data in a plain text manner rather than in a encrypted manner. If the encryption key is exposed, the data can be easily accessed by the intruder. In the existing system there is no security for the data even it is encrypted because there is only single cipher key is generated for that data.

The existing system refers to the current state of the cloud computing infrastructure, including the technologies, processes, and security measures in place for keyword search and data sharing. Understanding the strengths and weaknesses of the existing system is crucial for planning and implementing improvements. Here's an overview of elements commonly found in an existing cloud computing system:

DISADAVANTAGES

- Many existing systems may not adequately address data privacy concerns, leaving data vulnerable unauthorized access or leakage during keyword search and sharing operations.
- Ensuring the integrity of data stored in the cloud and shared among users is essential. However, existing systems may lack robust mechanisms to detect and prevent unauthorized modifications or tampering of data.
- Some systems may face scalability issues when dealing with large volumes of data or a high number of concurrent users, leading to performance bottlenecks or increased latency.
- Implementing strong security mechanisms often adds complexity to the system, making it more challenging to manage and maintain. This complexity can increase the likelihood of vulnerabilities or misconfigurations that could be exploited by attackers.
- Effective key management is critical for ensuring the security of encrypted data in the cloud. However, existing systems may struggle with key management issues, such as key distribution, rotation, and revocation, leading to potential security weaknesses.

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 ABPRE scheme andattribute-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 of the 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 cipher text-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 cipher text-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 cipher text attack (CCA) and chosen keyword attack (CKA) security in the

random oracle model. The proposed construction is demonstrated practical and efficientin the performance and property comparison.

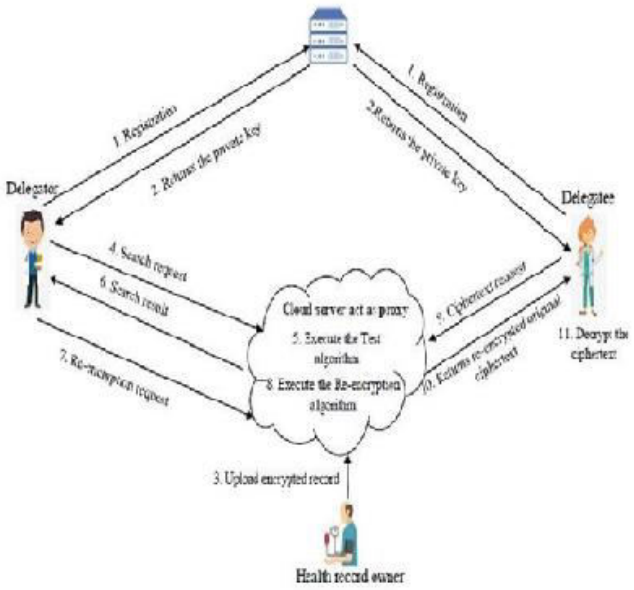
In this proposed system, we study data confidentiality against an adversary which knows the encryption key and has access to a large fraction of the cipher text blocks. The adversary can acquire the key either by exploiting flaws or backdoors in the key-generation software, or by compromising the devices that store the keys (e.g., at the user-side or in the cloud). To counter such an adversary, we propose a novel and efficient scheme which ensures that plaintext data cannot be recovered as long as the adversary has access to at most all but two ciphertext blocks, even when the encryption key is exposed.

ADVANTAGES

1. We describe the notion of CPAB-KSDS as well as its security model.
2. The proposed construction is demonstrated practical and efficient in the performance and property comparison 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
3. Here we use multiple cipher text keys for decrypting the data 2. It is very hard for the user to break the keys.
4. The proposed system is really complex and tough to break the encrypted data without having key premises

The proposed system for strengthening cloud computing security mechanisms for secure keyword search and data sharing offers several advantages over the existing system. These advantages aim to address the identified weaknesses and enhance overall security. Here are some potential advantages of the proposed system:

SYSTEM ARCHITECTURE



IV IMPLEMENTATION

MODULES

- Health record owner
- Delegatee
- Delegator PKI
- Cloud server

MODULE DESCRIPTION

Health record owner

The term "health record owner" typically refers to the individual who is the subject of a health record or a patient's health information. In the context of healthcare and medical records, the owner is the person to whom the health information pertains. Here are some key points to understand::n many jurisdictions and healthcare systems, patients are considered theowners of their health records. This ownership is grounded in the principle of patient autonomy and the right to control one's health information.

Delegatee:

In the context of healthcare, a delegatee is an individual or entity to whom certain responsibilities or tasks related to patient care or health information management are assigned by a healthcare provider or organization. This delegation is typically guidedby legal and ethical considerations, ensuring that the delegatee has the appropriate qualifications and training to perform the delegated tasks. For instance, a healthcare provider may delegate specific administrative tasks, such as appointment scheduling or data entry, to support staff within

the organization. Delegation can also extend to sharing certain patient information with other healthcare professionals involved in a patient's care, emphasizing the importance of maintaining patient privacy and confidentiality even when tasks are delegated. Effective communication and adherence to privacy laws and regulations are essential components of responsible delegation in healthcare settings.

Delegator: In healthcare, a delegator is an individual, typically a healthcare professionalor provider, who assigns specific tasks, responsibilities, or decision-making authorityto another person or entity, known as the delegatee. Delegation is a critical aspect of effective healthcare delivery, as it allows for the distribution of responsibilities among team members to optimize workflow and enhance patient care. Delegators must carefully assess the competence, qualifications, and training of potential delegatees, ensuring that they possess the requisite skills to carry out delegated tasks safely and effectively. While delegation is a practical means to streamline healthcare processes, delegators bear the ultimate responsibility for the outcomes of the delegated activities, maintaining accountability for patient well-being, compliance with regulations, and the overall quality of care provided by the healthcare team. Clear communication, trust, and a thorough understanding of legal and ethical considerations are integral to successful delegation in the healthcare domain.

PKG:

The term "pkg" can refer to various things depending on the context. In software development, particularly in macOS systems, "pkg" often stands for a package,which is a format for software distribution and installation. A package file typically contains compressed application files, scripts, and metadata necessary for the installation process. These packages simplify the deployment of software by bundling everything needed for installation into a single file, easing the distribution and installation processes for end-users. Additionally, "pkg" may also refer to "package" in a more general sense, representing a bundled set of files or resources designed for a specific purpose, such as a software library or a collection of related components. The interpretation of "pkg" depends on the specific domain, and additional context is needed for a more precise understanding.

CLOUD SERVER:

This module aims to bolster the existing security infrastructure by implementing advanced mechanisms to safeguard sensitive data and facilitate secure operations within the cloud environment.At its core, the module will employ robust encryption techniques to protect data both in transit and at rest. Utilizing state-of-the-art cryptographic algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman), data will be encrypted prior to transmission and securely stored within the cloud server.

SCREENSHOTS

FIG-1 Home page

FIG-2 Delegatee registration

FIG-2 Delegatorlogin

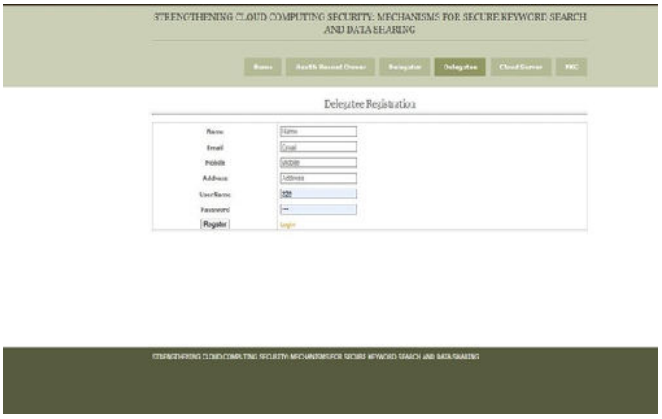


FIG-3 Delegatee registration

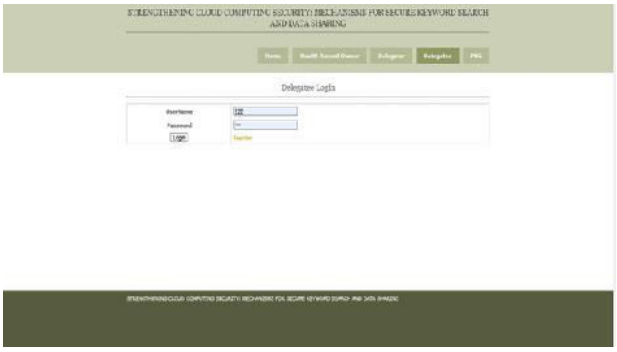


FIG-4 Delegatee login

FIG-5 Health record owner login:

VI. 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.

FUTURE SCOPE

The future scope of Java technology remains promising as it continues to evolve and adapt to the ever-changing landscape of software development. With the growing importance of cloud computing, microservices architecture, and the Internet of Things (IoT), Java's platform independence, strong security features, and scalability make it well-suited for modern application development. Additionally, advancements such as the modularization introduced in Java 9 and ongoing updates ensure that Java stays relevant in emerging technologies. Its widespread use in enterprise environments, coupled with a vibrant developercommunity and extensive ecosystem, positions Java to play a significant role in shaping the future of software development. t appears there might be a slight error in your question; "EPARA" doesn't seem to be a widely recognized term or acronym in the context of cloud computing or security. If you could provide more information or clarification about "EPARA," I would be better able to tailor my response to your specific inquiryHowever, assuming you're referring to enhancing security mechanisms in cloud computing environments, here are some general considerations and trends that might be relevant:

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 JournalIEEE, vol. 15, no. 2, pp. 2980-2988, 2021