Computing CloudCrypt: Enhancing Keyword Search and Data Sharing Security in Cloud

SANDEEP V D, Gunasekaran

AMC ENGINEERING COLLEGE

ABSTRACT

The passage discusses the benefits of cloud infrastructure in terms of cost reduction for hardware and software resources in computing. It also highlights the importance of encrypting information before outsourcing it to the cloud to ensure security. However, encrypted data can be difficult to search for and distribute compared to plain data. To address these issues, the passage proposes a solution called "ciphertext-policy attribute-based approach with keyword search and data sharing" (CPAB-KSDS) for encrypted cloud data.The CPAB-KSDS approach allows for secure keyword searches and data sharing while maintaining data confidentiality. The passage mentions that the security model of this approach is discussed, and a specific technique is presented, which is demonstrated to be secure in the random oracle model. It is also noted that the technique is resistant to chosen ciphertext and chosen keyword attacks, enhancing the overall security of the solution.Lastly, the passage points out that the proposed CPAB-KSDS construction is efficient and feasible, and a performance and property comparison indicates its superiority over other methods.

Overall, the focus of the passage is on proposing a secure and efficient approach for searching and sharing encrypted data in cloud infrastructures to address the challenges posed by encryption while ensuring data confidentiality and accessibility for cloud service users.

INTRODUCTION:

Yes, your description of cloud computing is accurate. Cloud computing is a paradigm that allows individuals, businesses, and organizations to access and utilize computing resources, such as hardware (e.g., servers, storage) and software (e.g., applications, databases), over the Internet or a network. This model eliminates the need for users to own and maintain physical infrastructure, as all the resources are hosted and managed by third-party service providers.

The cloud computing infrastructure is often represented as a cloud-shaped symbol in diagrams, symbolizing the complex and distributed nature of the underlying infrastructure that is hidden from the end-users. This infrastructure consists of large clusters of interconnected computers, which may include low-cost consumer PC technology with specialized connections to ensure scalability and efficiency.

Cloud computing services are typically provided through different models, including:

Infrastructure as a Service (IaaS): Offering virtualized computing resources over the internet, such as virtual machines, storage, and networking capabilities. Users can deploy and manage their applications on these virtualized resources.

Platform as a Service (PaaS): Providing a platform and environment for developers to build, deploy, and manage applications without worrying about the underlying infrastructure.

Software as a Service (SaaS): Delivering software applications over the internet on a subscription basis, eliminating the need for local installation and maintenance.

Function as a Service (FaaS)/Serverless Computing: Allowing developers to run individual functions or tasks without managing the underlying servers. They pay for the resources consumed by each function execution.

One of the significant benefits of cloud computing is its ability to scale resources up or down according to demand, enabling efficient resource utilization and cost-effectiveness. Virtualization techniques play a crucial role in maximizing the power of cloud computing by abstracting physical resources and creating virtual environments for users.Cloud computing has revolutionized the way businesses and individuals handle data,

perform computational tasks, and deliver services. Its flexibility, cost-effectiveness, and scalability have made it an essential technology for various industries, ranging from startups to large enterprises.

Characteristics and Services Models:

According to the National Institute of Standards and Terminology's (NIST) definitions, the key aspects of cloud computing are given below. Consumers can autonomously provision computing resources, including server time and network storage, as needed automatically without involving the providers of those services in any direct communication.

LITERATURE SURVEY:

Identity-based encryption with fuzziness: We provide Fuzzy Identity-Based Encryption, a novel Identity-Based Encryption (IBE) technique. In Fuzzy IBE, an identity is viewed as a collection of descriptive qualities. If and only if the identities and ′ are close to one another as determined by the "set overlap" distance metric may a private key for an identity,, decipher a ciphertext encrypted with an identity, ′. It seems like you have provided a description of a research work or paper related to Fuzzy Identity-Based Encryption (IBE) schemes. Fuzzy IBE is a cryptographic primitive that allows for encryption and decryption using biometric inputs as identities, accommodating the inherent noise in biometric samples. The error-tolerance property of Fuzzy IBE makes it suitable for handling the variations and inconsistencies present in biometric data.The description mentions that the work introduces two constructs of Fuzzy IBE schemes, which enable encryption based on fuzzy identity-defining criteria. This means that the encryption process takes into account multiple fuzzy attributes or criteria to define the identities that can access the encrypted message.

The key features of the Fuzzy IBE schemes presented in the work include:

Error-Tolerance: The schemes are designed to handle errors and noise in biometric inputs, making them suitable for practical use with biometric identities.

Secure Against Collusion Attacks: The schemes are resistant to attacks involving multiple attackers colluding to break the encryption.

Non-Reliance on Random Oracles: The fundamental design of the schemes does not rely on random oracles, which enhances their security.

Selective-ID Security: The integrity of the schemes is demonstrated under the concept of Selective-ID security, ensuring their robustness against chosen identity attacks.

Overall, the work seems to focus on developing efficient and secure Fuzzy IBE schemes that can be used in various applications involving biometric-based encryption.

2) For fine-grained access control of encrypted data, attribute-based encryption:

There will be a need to encrypt data saved at these sites as more sensitive data is shared and stored by third-party websites on the Internet. Encrypting data has the disadvantage that only coarse-grained sharing is possible (i.e., sharing your private key with a third party). We create Key-Policy Attribute-Based Encryption (KP-ABE), a new cryptosystem enabling precise exchange of encrypted data. Our cryptosystem uses sets of attributes to identify ciphertexts, and private keys are linked to access structures that regulate which ciphertexts a user can decipher. We use the sharing of audit-log data and broadcast encryption to show how our construction can be used in these scenarios. Our design enables the delegation of private keys, which incorporates HIBE (hierarchical identity-based encryption).

3) Encryption Using Ciphertext-Policy Attributes:Ciphertext-policy attribute-based encryption (CP-ABE) is a cryptographic system that allows for fine-grained access control on encrypted data. It addresses the limitations of traditional access control mechanisms, such as the reliance on trusted servers, by providing a more secure and flexible approach.

In CP-ABE, data is encrypted in a way that it can only be decrypted by users possessing specific attributes or credentials. These attributes could be anything from roles, qualities, or any other relevant information that defines the user's access rights. The encryption policy is associated with the ciphertext, and it dictates which attributes are required for decryption.

Here's how CP-ABE works:

Encryption: The data is encrypted using a cryptographic key, and an access policy is associated with the ciphertext. The access policy specifies the attributes required by a user to be able to decrypt the data.

Key generation: When a user needs access to the encrypted data, they request a decryption key from a trusted authority. The key generation process is based on the user's credentials and the access policy associated with the ciphertext.

Decryption: Users who possess the necessary attributes can use their decryption keys to decrypt the data, but those who do not have the required attributes will not be able to access the data even if they get hold of the encrypted ciphertext.

The advantages of using CP-ABE are:

Fine-grained access control: CP-ABE allows for highly granular access control, enabling different users to have access to different parts of the data based on their specific attributes.

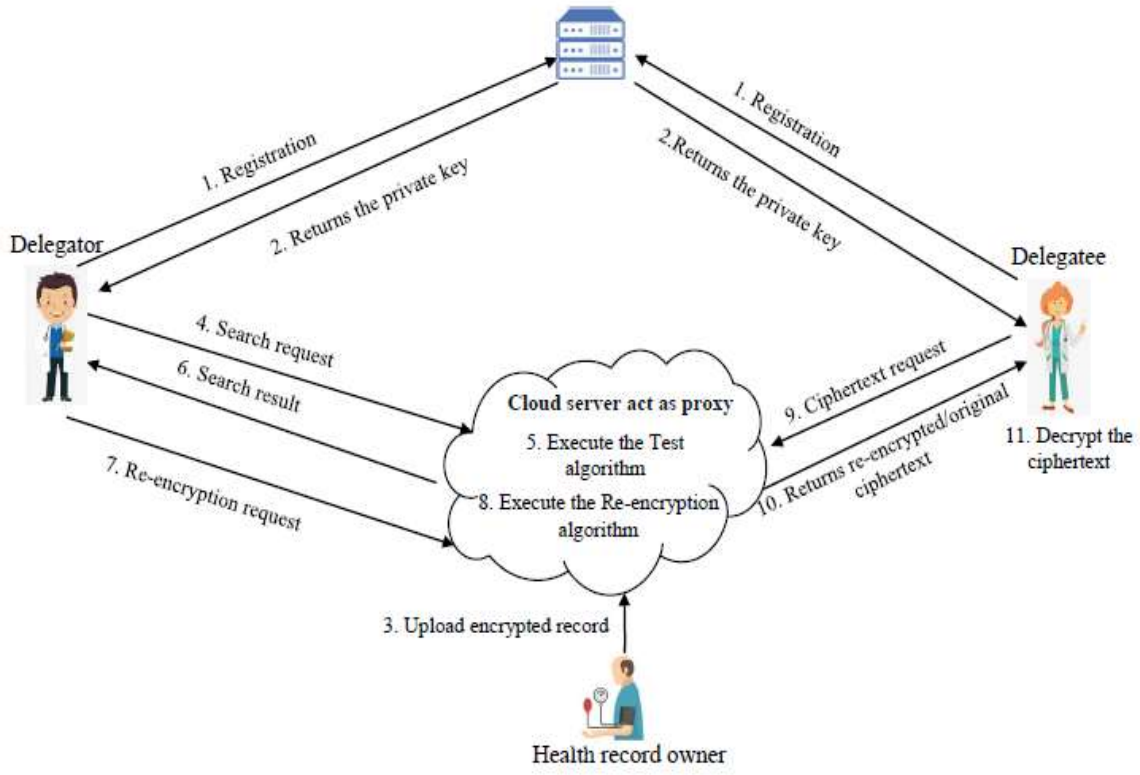
Secure against collusion: Even if multiple compromised servers or users attempt to collude to gain unauthorized access to the data, the encryption scheme remains secure, ensuring the confidentiality of the data.

Decentralization: CP-ABE reduces the reliance on a single trusted server for access control, as the access control policies are embedded in the ciphertext itself, making it more resilient to server compromises.

Flexibility: The access policies can be easily updated or modified without re-encrypting the entire dataset, making it easier to adapt to changing access requirements.

Overall, ciphertext-policy attribute-based encryption provides a robust solution for enforcing complicated access control on encrypted data, even in distributed systems where the confidentiality of the data might be at risk due to potential server compromises.SYSTEM

ARCHITECTURE:



EXISTING SYSTEM:

In an ABE-KS system, each piece of data is encrypted under a set of attributes, and an access policy is associated with the ciphertext. Only users with the right set of attributes (matching the access policy) can decrypt the data. Additionally, the scheme allows for keyword search on the encrypted data, which means that users can search for specific keywords in the encrypted data without having to decrypt it first. This way, sensitive information is protected, and the data owner can still search and share data selectively based on keywords and attributes.To sum up, in a PHR system, an Attribute-Based Encryption with Keyword Search (ABE-KS) method is preferred over the mentioned KP-ABPRE scheme as it grants the data owner more control over shared information while still maintaining privacy and security.

PROPOSED SYSTEM:

- 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) security in the random oracle model. The proposed construction is demonstrated practical and efficient in the performance and property comparison.

ADVANTAGES OF PROPOSED SYSTEM:

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

IMPLEMENTATION:

MODULES:

- Health Record owner
- Delegator
- Delegate
- Cloud Server
- PKG

MODULES DESCRIPTION:

Health Record Owner:

Initially, the record owner must register their information in the health record owner module. Following a successful registration, the record owner can log in and upload files using encrypted keywords and hashing algorithms to a cloud server. He or she can see the cloud-uploaded files. The owner of the health record can accept or deny the file request made by data consumers. Following request approval, the owner of the data will mail the secret key and verification object.

Delegator:

In the Delegator module, the Delegator must first register their information before logging in and verifying their login with a secret key. All the files that health record owners upload can be searched by Delegator. He or she can send a request to the files, which will then be sent to the owners of the health records.

Cloud Server (CS):

Cloud Provider can examine all file details in the Cloud Server module. Cloud has access to all data analysis.

PKG:

PKG may examine all delegator details and all delegates details in the PKG module.

CONCLUSION:

It appears that the text you provided describes a research study introducing a new concept called "Ciphertext-Policy Attribute-Based Keyword Searchable Data Sharing" (CPABKSDS) method. The main goal of this method is to enable keyword searching and data sharing while ensuring security. Below is a summary of the key points mentioned in the text:

Concept of CPABKSDS: The study introduces the concept of CPABKSDS, which likely combines attribute-based encryption, keyword searching, and data sharing to achieve the desired functionality.

Real-world Scheme and Security: The researchers have implemented a real-world CPABKSDS scheme and demonstrated its security against chosen-ciphertext attacks (CCA1) in a scenario involving a random oracle. This indicates that the proposed method is practical and secure under specific conditions.Performance and Property Comparison: The proposed CPABKSDS scheme is compared with existing methods in terms of performance and properties. It seems that the new scheme outperforms or exhibits favorable properties when compared to other related approaches.

Addressing a Difficult Challenge: The study addresses the challenging task of designing an attribute-based encryption scheme that allows keyword searching and data sharing without the need for a Proxy Key Generator (PKG) during the sharing phase. This is a significant step forward in the field of attribute-based encryption.

Inspiring Further Research: The proposed approach raises new research possibilities, such as developing a CPAB-KSDS scheme without relying on random oracles (which are idealized cryptographic components) or introducing a new framework to facilitate the process.

Overall, the study seems to have made valuable contributions to the field of attribute-based encryption with keyword searching and data sharing, and it has addressed some difficult challenges while inspiring further research in the area.

REFERENCE:

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457–473, Springer, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98, Acm, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Security and Privacy, 2007. SP’07. IEEE Symposium on, pp. 321–334, IEEE, 2007.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in International Workshop on Public Key Cryptography, pp. 53–70, Springer, 2011.

[5] H. Qian, J. Li, Y. Zhang, and J. Han, “Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation,” International Journal of Information Security, vol. 14, no. 6, pp. 487–497, 2015.

[6] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption,” Future Generation Computer Systems, vol. 52, pp. 67–76, 2015.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, “Interactive conditional proxy re-encryption with fine grain policy,” Journal of Systems and Software, vol. 84, no. 12, pp. 2293–2302, 2011.

[8] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A ciphertext-policy attribute-based encryption scheme with constant ciphertext length,” in International Conference on Information Security Practice and Experience, pp. 13–23, Springer, 2009.

[9] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public-Key Cryptography–PKC 2013, pp. 162–179, Springer, 2013.

[10] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in Advances in Cryptology–CRYPTO 2012, pp. 180–198, Springer, 2012.