IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Keyword Search And Access Control Over Cloud

[1]Mrs.Zeenath Jaha Begum, [2]Bethapudi Sandeep, [3]Lankavalasa Chandra Mahesh, [4]Gudipally Maniker Reddy, [5]Byagari
Sai Kiran

[1]Assistant Professor, [2]Student, [3]Student, [4] Student, [5] Student
[1]Computer Science & Engineering,
[1]Hyderabad Institute of Technology & Management, Hyderabad, India

Abstract: The project revolves around tackling the issue of keyword search with access control over encrypted data in cloud computing. A scalable framework has been proposed, allowing users to locally derive a search capability based on their attribute values and a search query. File retrieval is permitted only when the keywords match the query, and the user's attribute values pass the policy check. To enforce fine-grained access control and enable multi-field query searches, the project utilizes hierarchical predicate encryption, a recent cryptographic primitive. The implemented scheme, named keyword search with access control, addresses the challenges associated with searching encrypted data while maintaining access control . The scheme also accommodates search capability deviation and ensures efficient access policy updates and keyword updates without compromising data privacy. In an effort to enhance privacy, the keyword search with access control introduces noise into the query, concealing users' access privileges . The project conducts thorough evaluations on real-world datasets to validate the practicality of the proposed scheme. The results demonstrate the scheme's effectiveness in protecting user access privileges and itsapplicability in real-world scenarios.

Keywords **– Keyword Search, Access Control, Encrypted Data, Hierarchical Predicate Encryption**

I. INTRODUCTION

The cloud has emerged as a pivotal platform for data storage and processing, offering centralized access to virtually limitless resources such as storage capacity and elastic services for end users. Despite its advantages, challenges persist, particularly in the realms of data security and user privacy. An illustrative scenario involves the storage of sensitive data, like electronic health records, in the cloud. In this context, it is imperative to prevent unauthorized disclosure to cloud administrators and other entities lacking the data owner's explicit permission. Therefore, ensuring data confidentiality (to safeguard the plaintext from unauthorized access) and implementing data access control (to regulate user privileges) become essential considerations in the storage of data in the cloud.

Encryption stands out as a widely adopted approach for safeguarding data confidentiality. Nevertheless, the conventional plaintext keyword search approach necessitates retrieving all encrypted data files from the cloud and conducting the search post- decryption. This methodology proves highly impractical, particularly in the context of traditional networks and is exacerbated in resource-constrained environments such as wireless networks (e.g., wireless sensor networks and mobile networks). These networks grapple with limitations in resources such as energy, bandwidth, and computational capabilities.

.

FEASIBILITY STUDY: This phase involves a comprehensive examination of the project's viability, presenting a business proposal that outlines a broad project plan along with initial cost estimates. The system analysis phase focuses on conducting a feasibility study for the proposed system, a crucial step to ascertain that its implementation does not pose an undue burden on the company. To conduct a thorough feasibility analysis, it is imperative to gain a clear understanding of the primary system requirements. This ensures that the proposed system aligns seamlessly with the company's needs and resources.

Three critical factors considered in the feasibility analysis include:

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

2. LITERATURE SURVEY

J. Shu, Z. Shen and W. Xue, "Shield: A Stackable Secure Storage System for File Sharing in Public Storage," published in the Journal of Parallel and Distributed Computing (vol. 74, no. 9, pp. 2872-2883, Sep. 2014), introduces the concept of a trust domain to efficiently manage a large number of users with varied attributes in a cloud environment. The trust domain specifies the level of granularity for file sharing, treating users within the same domain similarly. Shield is specifically crafted to ensure the secure storage and sharing of data within a trust domain (e.g., an organization or department) within shared network and storage environments involving multiple parties. The system aims to alleviate the challenges associated with data management by providing security without necessitating complete trust in the cloud server. In an effort to streamline key management and reduce client-side burdens, Shield centralizes security control information (comprising user access permissions, integrity details, and decryption keys) for each data file.

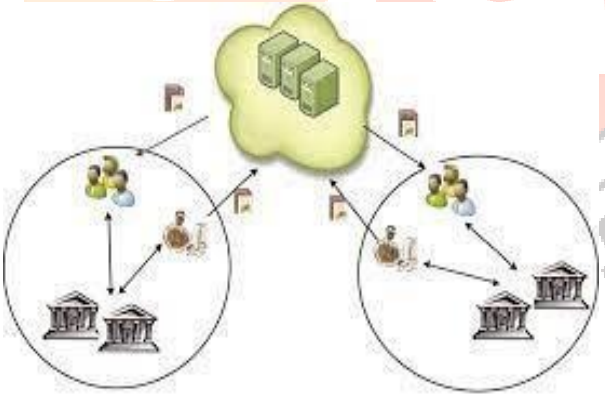
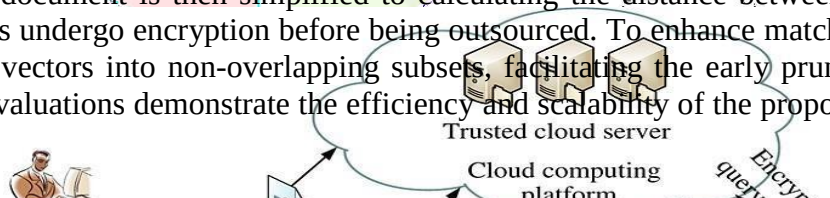


Figure 2.1: Stackable secure storage

J. Cao, F.-Y. Rao, M. Kuzu, E. Bertino and M. Kantarcioglu, " The paper named "Efficient Tree Pattern Queries on Encrypted XML Documents," showcased during the Joint EDBT/ICDT Workshops in March 2013, (pp. 111-120), addresses the challenges of outsourcing encrypted XML documents while maintaining efficient query processing. Existing approaches to this issue have either compromised structural information or lacked support for searches with constraints on XML node content. Moreover, they commonly employ a filtering-and-refining framework, necessitating users to eliminate false positives from query results.To tackle these issues, the paper proposes a solution for the effective evaluation of tree pattern queries (TPQs) on encrypted XML documents. A domain hierarchy is established, enabling the embedding of each XML document. Assigning a position to each node in the hierarchy results in the creation of a vector for each document, encoding both structural and textual information. Similarly, a vector is generated for a TPQ. The matching process between a TPQ and a document is then simplified to calculating the distance between their vectors. To uphold privacy, these vectors undergo encryption before being outsourced. To enhance matching efficiency, a k-d tree is utilized to partition vectors into non-overlapping subsets, facilitating the early pruning of non- matchable documents. Extensive evaluations demonstrate the efficiency and scalability of the proposed solution, particularly with large



datasets.

Figure 2.2: Efficient Privacy-Preserved Data Query over Cipher Text

D. Boneh, A. Raghunathan and G. Segev, In the paper titled 'Function-Private Identity-Based Encryption: Concealing the Function in Functional Encryption,' which was presented at the Advances in Cryptology (CRYPTO) conference in 2013, (pp. 461-478), a novel concept called function privacy is introduced within the context of identity-based encryption and, more broadly, in functional encryption. The underlying idea is that decryption keys should, intuitively, disclose minimal information about their associated identities, only revealing the absolute essential details. This notion stems from the necessity to ensure predicate privacy in public-key searchable encryption. However, formally defining such a concept presents challenges since, given a decryption key, there is always a potential to glean some information about the corresponding identity by testing its efficacy in decrypting ciphertexts specifically intended for certain identities.

T. Okamoto and K. Takashima, " In the paper presented at the ASIACRYPT conference in 2009, (pp. 214-231) titled "Hierarchical Predicate Encryption for Inner-Products," a novel scheme for Hierarchical Predicate Encryption (HPE) is introduced. Specifically designed for inner-product predicates, this scheme is asserted to be secure, featuring selectively attribute-hiding properties within the standard model. Crucially, this security is achieved under novel assumptions that are non-interactive and of fixed size in the number of adversary's queries (non-"q-type"). These assumptions are rigorously demonstrated to hold in the generic model. Importantly, this work represents a noteworthy advancement as it is identified as the inaugural HPE (or delegatable Predicate Encryption) scheme designed for inner-product predicates that attains security within the standard model.

3. PROPOSED SYSTEM

In the envisioned system, a scalable framework is introduced, as depicted in this model, which combines multi-field keyword search with fine-grained access control. Within this framework, each user authenticated by an authority receives a set of keys, referred to as credentials, representing their attribute values. Every file residing in the cloud is associated with an encrypted index that serves to label keywords and define the access policy.

Figure 3.1: Design of Encrypted Cloud Search Architecture

Each user has the ability to employ their credentials along with a search query to autonomously create a search capability locally.Subsequently, this capability is submitted to the cloud server, which undertakes the tasks of search execution and access control. The user ultimately obtains the data files corresponding to their search query, facilitating authorized access. This architectural approach effectively tackles the initial challenge by maximizing the computational capabilities of the cloud server.

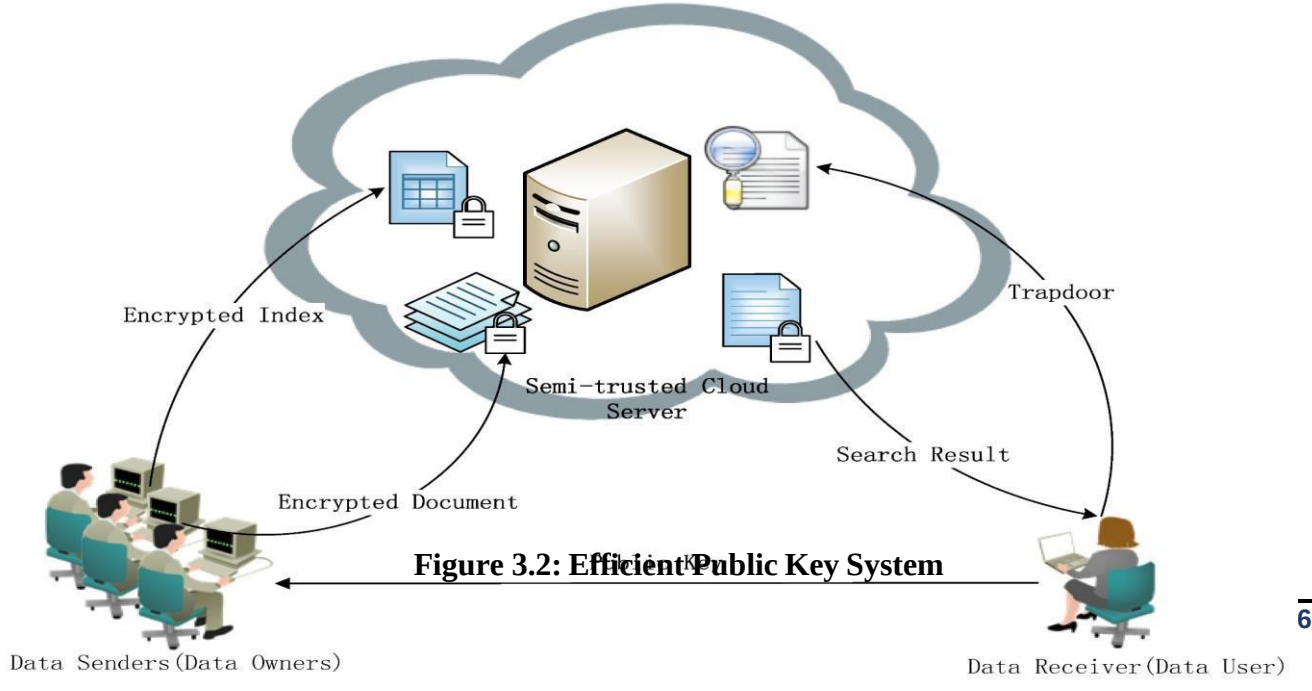


Figure 3.2: Efficient Public Key System

Next, to facilitate this framework, a distinctive approach is taken by innovatively leveraging Hierarchical Predicate Encryption(HPE) for the generation of search capabilities. Building upon HPE, our proposed scheme, named KSAC, is introduced. KSAC not only enables both keyword search and access control across multiple fields but also facilitates the efficient updating of access policies and keywords. Moreover, KSAC incorporates random values to augment the safeguarding of user access privacy. To our knowledge, KSAC stands out as the initial solution to concurrently accomplish the objectives outlined above**.**

ADVANTAGES

- Enhanced Data Security through the Implementation of Hierarchical Predicate Encryption.

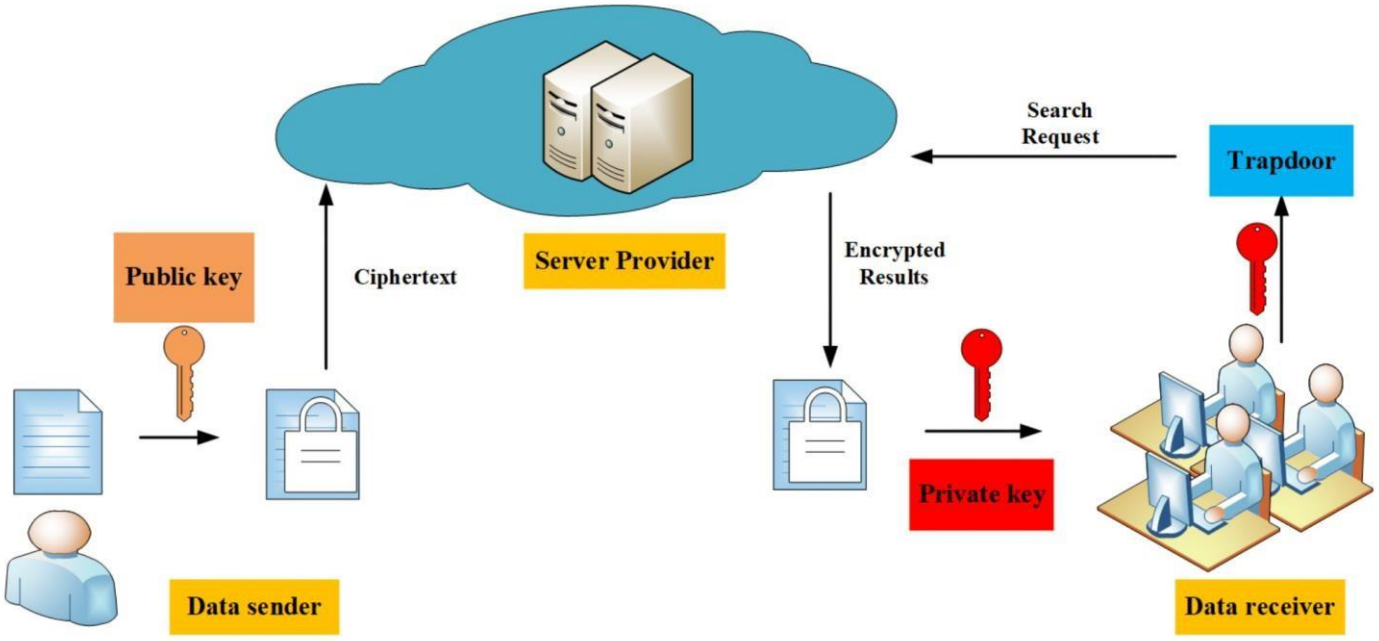


Figure 3.3: Public Key Encryption Model with Keyword Search Design

- More data security due to Data Confidentiality and Index Privacy.

4. RESULTS & DISCUSSION

In this research paper, we introduce a scalable framework enabling users to autonomously derive search capabilities by leveraging both their credentials and a search query. Hierarchical Predicate Encryption (HPE) is then employed to operationalize this framework, leading to the development of our scheme, KSAC. KSAC achieves fine-grained access control and multi-field keyword search, facilitates efficient updates of both access policies and keywords, and ensures the protection of user access privacy. The outcomes of our experiments indicate that KSAC requires only 1.08 seconds for each capability generation and 0.12 seconds for matching assessments between a search capability and an encrypted index. To summarize, this investigation provides significant insights into the domain of keyword search access control over encrypted cloud data. Despite prevailing challenges, the advancements made in this study lay the foundation for more robust, secure, and practical solutions in securing sensitive information while enabling efficient data retrieval in cloud-based environments.

REFERENCES

[1] Z. Shen, J. Shu, and W. Xue, "Secured Keyword Search with Access Control on Encrypted Data in Cloud Computing," inProc. IEEE/ACM IWQoS, May 2014, pp. 87–92.

[2] J. Shu, Z. Shen, and W. Xue, "Shield: A Secure Stackable Storage System for Public File Sharing," Journal of Parallel andDistributed Computing., vol. 74, no. 9, pp. 2872–2883, Sep. 2014.

[3] M. Tinghuai et al., "Enhancing Collaborative Recommender System through Social Network and Tag Sources Integration,"IEICE Trans. Inf. Syst., vol. 98, no. 4, pp. 902–910, 2015.

[4] Y. Ren, J. Shen, J. Wang, J. Han, and S.-Y. Lee, "Mutual Verifiable Provable Data Auditing in Public Cloud Storage," Journalof Internet Technology., vol. 16, no. 2, pp. 317–323, 2015.

[5] J. Shu, Z. Shen, W. Xue, and Y. Fu, "Secure Storage Systems and Key Technologies" presented at the 18th Asia South PacificDesign Automation Conferenc".. (ASP-DAC), Jan. 2013, pp. 376–383.

[6] P. Golle, J. Staddon, and B. Waters, "Protected Conjunctive Keyword Search on Encrypted Data," in Proc. ACNS, Jun. 2004,pp. 31–45.

[7] Y.-C. Chang and M. Mitzenmacher, "Preserving Privacy in Keyword Searches on Distant Encrypted Data
," in Applied Cryptography and Network Security. Berlin, Germany: Springer Verlag, 2005.

[8] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Encryption with Keyword Search using Public Key," in Proc.Eurocrypt, 2004, pp. 506–522.

[9] E. Shi, J. Bethencourt, T.-H. H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in Proc.IEEE Symp. Secur. Privacy, May 2007, pp. 350–364.

[10] D. X. Song, D. Wagner, and A. Perrig, "Practical Approaches for Searches on Encrypted Data," in Proc. IEEE Symp. Secur.Privacy, May 2000, pp. 44–55.

[11] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Protected Ranked Keyword Search on Encrypted Cloud Data," in Proc.IEEE ICDCS, Jun. 2010, pp. 253–262.

[12] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Proc. NDSS,2004, pp. 1–11.