International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 07 | July 2022 www.irjet.net p-ISSN: 2395-0072

SECURITY MULTIKEYWORD MAPPING AND SEARCH OVER ENCRYPTED CLOUD DATA

A .Farzana [1], B. Ananathi [2] , T.Dinesh Kumar[3]

PG Scholar[1], Assistant Professor[2] , Assistant Professor[3]
Department of Computer Science and Engineering Vivekananda College of Engineering for Women

---

ABSTRACT: Searchable encryption allows you to upload an encrypted document to a remote, honest and suspicious server and query this data on the server without first decrypting the document. With the advent of cloud computing, data owners are encouraged to move advanced data management systems from on-premises locations to commercial public clouds to reduce flexibility and costs. However, for privacy reasons, sensitive data must be encrypted prior to outsourcing, and the traditional use of data based on plaintext keyword searches has been discontinued. Therefore, it is important to implement an encrypted cloud data retrieval service. Given the large number of data consumers and documents in the cloud, it is important that search services support multiple keyword queries and result similarity rankings to meet the needs of effective data retrieval. This paper proposes a secure multi-keyword search for encrypted cloud data based on the quality and ease of use of sending and storing cloud data. We also used the Triple DES (Data Encryption Standard) algorithm for encryption and decryption keys for a secure authentication process. The encryption process uses different key sizes. Our analysis shows that the proposed approach is safe against attacks by adaptively selected keywords. This solution is very efficient, can be applied to real cloud storage systems, and also speeds up encryption and decryption.

Keyword: Cloud Computing, Data Encryption Standard, Multikeyword

1. INTRODUCTION

Searchable encryption allows you to query encrypted data in the cloud without decrypting it. However, because the relationships between variables are fundamentally different, most SE solutions focus on SQL queries and cannot be easily applied to spatial data. To enable the query service for encrypted spatial data, we have traditionally used a space-filling curve to convert the original position of the POI to a one- dimensional index value. A space-filling curve is a curve that intersects all partitions of a closed space without intersecting itself. In this way, each curve is a curve that intersects each partition of a closed space without intersecting itself. In this method, each point in multidimensional space is mapped to one- dimensional space as a value. The standard Hilbert curve (SHC), a sort of space filling curve, is employed as a building block in many schemes for spatial data processing, which can protect the confidentiality of outsourced geographical data and enable successful spatial enquiries. Users can use the transformation key and the original geographic query to create a query token to retrieve encrypted spatial data.

As a result, fine-grained validation feature approval is supported. That is, only users whose validation structure matches the allowed area can validate the query results. Cloud storage is a computer data storage system that stores digital data in a logical pool called the "cloud.". Physical storage is often distributed across multiple servers (sometimes in different locations), and the physical environment is typically owned and managed by the hosting company. Enterprises only have to pay for the storage they use.

This usually corresponds to the average monthly usage. I'm not saying that cloud storage is cheaper. Rather, it costs an ongoing cost rather than an initial cost. Spatial databases are used to store and query data that represents objects specified in geometric space. Most spatial databases support the representation of simple geometric objects such as points, lines, and polygons. Resists unilateral access inside and outside the cloud. Sensitive data such as email, personal health records, photo albums, and tax records may need to be encrypted by the data owner before being offloaded to the commercial public cloud. However, with traditional plaintext keyword search-based data usage services, only users whose validation structure matches the allowed area need to validate the query results. Cloud storage is a computer data storage system that stores digital data in a logical pool called the "cloud." Physical storage is often distributed across multiple servers (sometimes in different locations), and the physical environment is typically owned and managed by the hosting company. Enterprises only

have to pay for the storage they use. This usually corresponds to the average monthly usage. I'm not saying that cloud storage is cheaper.

Rather, it costs an ongoing cost rather than an initial cost. Spatial databases are used to store and query data that represents objects specified in geometric space. Most spatial databases support the representation of simple geometric objects such as points, lines, and polygons. To counter unilateral access to sensitive data inside and outside the cloud. Emails, personal health records, photo albums, tax documents, etc. may need to be encrypted by the data owner before being offloaded to the commercial public cloud. However, this removes the traditional data usage service based on plaintext keyword search.

Service models

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The Software-as-a-Service model provides pre-built applications with the required software, operating system, hardware, and network. PaaS provides operating systems, hardware, and networks, and customers install or develop their own software and applications. The IaaS model provides only hardware and networks. Customers install or develop their own operating systems, software, and applications.

Deployment of cloud services:

Cloud services are typically delivered via a private cloud, community cloud, public cloud, or hybrid cloud. Services provided by the public cloud are generally provided over the Internet and are owned and operated by cloud providers. Examples include public services such as online photo storage services, email services, and social networking sites. However, enterprise services can also be provided in the public cloud.

In a private cloud, the cloud infrastructure is dedicated to a particular organization and is managed by the organization or a third party. In the community cloud, services are shared by multiple organizations and are only available to those groups. Infrastructure may be owned and operated by your organization or cloud service provider. Hybrid clouds are a combination of different methods of resource pooling (for example, a combination of public and community clouds).

Cloud services are popular

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Cloud users don't have to invest in IT infrastructure or buy hardware or software licenses, reducing upfront costs, improving return on investment, rapid deployment, customization, flexible use, and new innovations. The solutions you can take advantage of new innovations.

In addition, cloud providers that specialize in specific areas (such as email) can offer advanced services that may not be available or developed by a single organization. Other benefits for users are scalability, reliability, and efficiency.

Scalability means that cloud computing offers unlimited processing power and storage capacity. The cloud is reliable in that you can access your applications and documents from anywhere in the world over the Internet. Cloud computing is often seen as efficient because it allows enterprises to free up resources and focus on innovation and product development.

Another potential advantage is that your personal information can be better protected in the cloud. In particular, cloud computing can incorporate privacy protection into technology from the beginning and improve efforts to use better security mechanisms. Cloud computing enables more flexible IT procurement and expansion, and may be able to adjust steps based on data confidentiality. Widespread use of the cloud can also promote open standards for cloud computing that specify basic data security characteristics common to different services and providers. Cloud computing can also enable a better audit trail. Moreover, the information in the cloud is not easily lost.

2 BACKGROUND STUDY

C. Guo, R. Zhuang, Y. Jie, K. Choo, and X. Tang [1] Secure range search of encrypted data from IoT devices. In particular, use homomorphic, order-maintaining encryption (OPE) to encrypt data published by the data owner. Then create a data index using a k-d tree (KDtree). These schemes are designed to ensure the privacy of the dataset without sacrificing the efficiency of

keyword searches on the (encrypted) dataset. Demonstrate that our scheme can preserve both data and query privacy and evaluate its performance to demonstrate this.

Y. Wang, Q. Wu, B. Qin, W. Shi, R. Deng, and J. Hu [2] Cloud storage systems provide distributed clients with simplified file storage and sharing services. To address integrity, controllable outsourcing, and origin auditing concerns on X. Yao, R. Zhang, Y. Zhang, and Y.Lin

[3] Social data outsourcing is a new paradigm for effective and efficient access to social data. In such systems, a third-party social data provider (SDP) purchases the complete social dataset from an online social network (OSN) operator and resells it to data consumers. A data consumer is an individual or organization that needs complete social data. Meets certain criteria. SDP is not completely reliable and returns false query results to data consumers by adding fake data or deleting / modifying true data in favor of companies wishing to pay. This white paper begins an investigation into the outsourcing of verifiable social data. This study allows data users to verify the authenticity of the social data returned by the outsourced files, they propose an identity-based data outsourcing (IBDO) scheme equipped with SDP.

Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, desirable features advantageous over existing proposals in securing outsourced data. First, the IBDO scheme allows users to allow a dedicated proxy to upload data to a cloud storage server on their behalf. For example, a company can allow some employees to upload files to their cloud account in a controlled way.

and X. Zhang [4] Cloud storage services allow users to offload data to cloud servers and save on local data storage costs. However, unlike using local storage devices, users do not physically manage the data stored on cloud servers. Therefore, the data integrity of the offloaded data is an issue. Many public validation schemes have been proposed to allow third-party auditors to verify the integrity of a user's data. These schemes make the unrealistic assumption that the verifier has sufficient computational power to support the verifier's expensive verification costs, communications, and computational efficiency.

K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen [5] Controlling access to large amounts of big data can be a daunting task, especially if big data is stored in the cloud. Ciphertext policy attribute-based encryption (CPABE) allows end users to encrypt data based on the access policy defined for some attributes of the data consumer, and only data consumers whose attributes meet the access policy encrypt the data. It is a promising encryption technology that enables you to make it. Decode. CPABE adds the access policy to the ciphertext in clear text format. This may reveal personal information about the end user. The existing method only partially hides the attribute value in the access policy, but the attribute name is not yet protected.

J. Li, R. Ma, and H. Guan [6] Cloud storage provides convenient, large-scale, and scalable storage at a low cost, but privacy is a major concern that prevents users from trusting and storing files in the cloud. One way to improve privacy from the data owner's point of view is to encrypt the file before it is offloaded to the cloud and decrypt it after it is downloaded. However, data encryption is a significant overhead for mobile devices, and the data acquisition process requires complex communication between the data consumer and the cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging.

H. Tian, Y. Chen, C.-C. Chang, H. Jiang,

Y. Huang, Y. Chen, and J. Liu [7] Cloud storage is an increasingly popular application of cloud computing that can provide on-demand data outsourcing services to both organizations and individuals. However, users may not completely trust their cloud service provider (CSP) because it is difficult to determine if the CSP meets their legal expectations for data securityTherefore, it is very important to develop efficient verification methods to increase the trust of data owners in cloud storage. This white paper introduces a new public audit scheme for secure cloud storage based on dynamic hash tables (DHT). This is a new 2D data structure that resides in the Third Parity Auditor (TPA) to map data property information records. In contrast to existing work, the proposed scheme migrates allowed information from CSP to TPA, thereby significantly reducing computational costs and communication overhead.

Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li

[8] Searching with encrypted data is a very important technique in cloud computing, and pre- outsourcing encryption is the basic solution for protecting user data in untrusted cloud server environments. Many secure search schemes have a single

contributor scenario where a paging record or a secure searchable index of records is encrypted and is usually managed by a single owner based on symmetric encryption. I'm in focus. In this paper, they attention on a distinctive but extra difficult situation in which the outsourced dataset may be contributed from a couple of proprietors and are searchable with the aid of using a couple of users, i.e., multi- consumer multi-contributor case. Inspired by attribute-based encryption (ABE), the first attribute-based keyword search scheme with efficient user revocation (ABKSUR) that enables scalable, fine-grained (ie, file-level) search authentication. Introduce. Our scheme allows multiple owners to independently encrypt data and offload it to a cloud server.

M. Talha, I. Kamel, and Z. A. Aghbari [9] Database outsourcing is a not unusualplace cloud computing paradigm that permits facts proprietors to take benefit of its on-call for garage and computational resources. The main challenge is to maintain the confidentiality of the data to untrusted parties. B. Cloud service provider. Provides real-time query results related to authenticated users. Existing approaches have the problem of compromising data confidentiality or increasing the cost of communication between the server and the user. To solve this problem, they have dual spatial data conversion and encryption where the encrypted query is fully executed by the service provider of the encrypted database and the encrypted result is returned to the user. We propose a cryptographic scheme.

Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li [10] Fog computing is an extension of cloud computing that offloads sensitive encrypted data to multiple fog nodes at the edge of the Internet of Things (IoT) to reduce latency and network congestion. However, existing ciphertext recovery schemes rarely focus on fog computing environments, and most of them still impose heavy computational and memory overhead on resource-constrained end users. This paper first introduces the Lightweight FineGrained Ciphertexts Search (LFGS) system to fog computing by extending CiphertextPolicy AttributeBased Encryption (CPABE) and Searchable Encryption (SE) technologies. This makes it possible to achieve fine-tuned access control and keyword search at the same time. LFGS can offload some of the computational and storage overhead to end-user-selected fog nodes. In addition, the basic LFGS system has been improved to support conjunction keyword searches and attribute updates to prevent irrelevant search results and unauthorized access. Formal security analysis shows that the LFGS system can withstand ChosenKeyword Attack (CKA) and ChosenPlaintext Attack (CPA), and simulations using real-world datasets make the LFGS system really efficient and feasible. It shows that.

3. PROPOSED METHODOLOGY

Multi-Keyword Ontology A set of rigorous privacy requirements to define and solve the difficult problem of protecting privacy with keyword mapping and encrypted cloud data (MROS) searches, and to achieve such a secure cloud data sharing system. To develop. Choose an efficient concept of coordinate matching from multiple multi-keyword semantics. We present the Secured Multikeyword Search (SMS) problem over encrypted cloud data (ECD) and build a set of privacy standards for such a safe cloud data utilization system.

We first propose a basic Secured multi keyword ranking ontology keyword mapping and search technique based on safe inner product computation, which we subsequently develop to fulfill various privacy needs. Ranking results show the first k search results. In addition, we propose an alert system that generates alerts when unauthorized users try to access data from the cloud. Notifications are generated in the form of emails and messages.

- Cloud Setup
- Cryptography Cloud Storage
- Vector Model

a) CLOUD SETUP

Cloud Setup This module sets up the data owner and cloud server. Therefore, the data owner transfers the data to the cloud server. When users offload private data to the cloud, cloud service providers can control and monitor the data, protecting communication between users and the cloud. **CRYPTOGRAPHY CLOUD STORAGE**

Encrypted cloud storage In this module, data is uploaded to storage and search services. You cannot fully trust the cloud server to protect your data because the data may contain sensitive information. For this reason, outsourced files must be

encrypted. located on premise (i.e., in the customers region of control). Specifically, this means that access to customer data is under its control and is only granted to trusted parties.

b) VECTOR MODEL

Vector model This model uses a set of searchable symmetric encryption schemes that allow the search for ciphertext. In the former case, the files are sorted by the number of keywords found, which affects the accuracy of the search. A vector space model, or conceptual vector model, is an algebraic model for representing a text document (and generally any object) as a vector of identifiers (such as the concept of an index). It is used for information filtering, information retrieval, indexing, and relevance ranking

4 RESULT &DISCUSSION

Fig 1. HOME MAPPING

Home Mapping is the process of using the Internet to view, analyze, or share a visual representation of geospatial data in a map format. Improve service by identifying the root cause of IT infrastructure problems and changes.

Service mapping uses traffic-based actions to create service maps for a more integrated infrastructure.

Fig 2. SEARCHING

Web Search is a dedicated computer server that searches for information on the Web. User query search results are often returned as a list. These hits consist of web pages, images, and other file types.

5 CONCULSION

Searchable encryption is a mechanism that enables secure retrieval of encrypted data on remote servers. This task is the first to discover and solve the problem of searching encrypted cloud data in one term, providing a set of privacy constraints. To better capture the similarities between search terms and outsourced documents, we have determined an efficient principle of "coordinated coordination". i.e As many matches as possible between different multi-keyword semantics. Addresses the difficulty of multi-meaning words without losing confidentiality. First, it provides a basic strategy for secure multi- keyword search based on secure dot product computing. This has been significantly enhanced to meet the privacy requirements of the two threat models. Compare DES, RSA, and planned Triple DES. The proposed approach shows that there is a significant difference in the time required for the encryption and decryption process. A thorough investigation and hands-on testing of the various methods of guaranteeing privacy and efficiency will be provided.

9 REFERENCES

[1] C. Guo, R. Zhuang, Y. Jie, K. Choo, and X. Tang, "Secure rangesearch over encrypted uncertain iot outsourced data," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1520–1529, 2018.

[2] Y. Wang, Q. Wu, B. Qin, W. Shi, R. Deng, and J. Hu, "Identitybased data outsourcing with comprehensive auditing in clouds," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 940–952, 2017.

[3] X. Yao, R. Zhang, Y. Zhang, and Y. Lin, "Verifiable social data outsourcing," in Proc. of IEEE Conference on Computer Communications, Atlanta, USA, May 2017, pp. 1-9.

[4] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from in distinguishability obfuscation," IEEE Transactions on InformationForensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[5] K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, "An efficient and fine- grained big data access control scheme with privacy preserving policy," IEEE Internet of Things Journal, vol. 4, no. 2,pp. 563–571,2017.

[6] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic- hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 701–714, 2017.

[7] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Verifiable attribute- based keyword search with fine-grained owner- enforced search authorization in the cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187–1198, 2016.

[8] B.Ananthi, S.V.Priyadharshini, and M.Ramesh "Security Multikeyword Search over encrypted cloud data based on quality and usability," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1520–1529, 2018.