International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 13; Issue: 7; July- 2024

ENCRYPTED KEYWORDS SEARCH PROTECTION USING CLOUD COMPUTING

KAVYA NAYAK
PG student
Department of Master of Computer Application
The Oxford College of Engineering
Bommanahalli Bengaluru-560068
kavyanayak02@gmail.com

ASHOK B P
Assistant Professor
Department of Master of Computer Application
The Oxford College of Engineering
Bommanahalli Bengaluru-560068
ashokbp.mca @gmail.com

ABSTRACT

The work actually aims at giving proper and attribute wise justification related to high level security provisions of a huge amount of sensitive information in a cloud environment it also aims to ensure that the search requirements are properly maintained. The current methods of data encryption methods fail literally on both ends security and usability due to todays fast and rapidly increasing data breaches and unauthorized access. this is a project that the employed state of the art cryptographic technique in whichever the basic data and search queries are kept encrypted.no meaningful information will leak out in a search. A homomorphic encryption scheme and searchable encryption schemes enable a user to conduct a search on encrypted data without the necessity of decryption at the user side, hence maintaining confidentially and integrity. The solution needs to be scalable cloud computing resources in large data with complex searches entail very little performance overhead. This approach minimizes the risk of showing of data in transit and at rest, offering strong protection from potential attackers.

Keywords: Encryption, Decryption, File Processing

INTRODUCTION

Protection against leakage of sensitive information has emerged as a prime issue for the interest of every individual and organization in the rapidly changing digital world. This project entitled “Encrypted Keyword Search Protection Using Cloud Computing “addresses this critical issue by integrating advanced cryptographic techniques with the expansive capabilities of cloud technology. essentially, the project allows safe and efficient searching of encrypted data stored on cloud platforms without compromising user privacy at the cost of search speed and accuracy. If data is encrypted using traditional methods, search functionality becomes rather impractical because if defeats the purpose of encryption by decrypting the data every time a query is

made. However, these modern, advanced algorithms used in this innovative approach make it possible to search for keywords directly in their encrypted form. This implies that through this searching process, sensitive information will remain unknown to everybody also from the cloud service provider but protected within their encrypted form.it scales and flexes cloud computing to deliver support to large scale data management but provides a robust framework that can be adapted into very different applications: health and finance, among others and personal data storage. The project is focused on user centric design to assure the encryption and search mechanisms are user friendly and seamlessly integrated into existing workflows. With the growing concern for data breaches and cyber threats

II. LITERATURE SURVEY

The "Encrypted Keyword Search Protection Using Cloud Computing" project emphasizes the most critical issue related to data privacy and security in a cloud environment. The more the world turns digital, the greater the dependence on cloud computing becomes for storing and managing data because it is flexible, scalable and cost effective. However, this very convenience brings increased concerns about data breaches and unauthorized access. Traditional schemes of encryption do an excellent job of keeping the data both at rest and in transit very secure, but they are quite disappointing in terms of search over encrypted data excluding breaking the security. This is where searchable encryption can conduct searches encrypted data without decrypting it and thus offers confidentiality to the saved records.

The literature on this topic surveys quite a good number of approaches and algorithms designed to enable efficient and secure keyword examinations of encrypted data. Pioneering work by song, Wagner and Perring presented the concept of searchable symmetric encryption that empowers keyword searches concerning encrypted data. Subsequent research built upon this foundation and went ahead to develop public key encryption schemes, including the presented by boneh, crescenzo, Ostrovsky, and persiano of public key encryption along with keyword search.it is such seminal works that have inspired a spate of innovations tuned to trade off between security, search efficiency, and system performance.

Recent research has been conducted in enhancing practically and scalability of such schemes in real world cloud environments. The latest techniques, such as dynamic searchable encryption, have

been proposed to uphold the dynamic nature of cloud data with update, delete and insert operations without the need for complete re-encryption.

This 'Encrypted Keyword Search Protection Using Cloud Computing' project converges cryptographic research and practical application in safeguarding data privacy within the cloud. With improved encryption techniques and innovative algorithms in search, this research tends to give a secure and efficient solution for management and querying of encrypted data, answering the increasing call for secure cloud computing solutions within different sectors such as health, finance and government.

III.EXISTING SYSTEM

The security framework of the encrypted keyword search protection system in cloud computing typically includes data owners encrypting data before uploading it to the cloud, so that cloud service contributor untouchable the plaintext data; the user generates encrypted keywords through a secure encryption scheme and submits these until cloud for execution of search operations. The cloud server, with the aid of searchable encryption algorithms, matches the encrypted keywords against the encrypted data to retrieve the relevant documents. During this process, neither the data nor the keywords are decrypted. While this approach adds some layer of security to the system, it has several limitations. First, it often uses symmetric key encryption.to this end secure key management and distribution need to be enforced; otherwise, it could be pretty cumbersome and may be breached if not handled properly.

Second it might make the search procedure ineffective because of the large part of current techniques being linear scans on ciphertexts, which brings in high computational overhead and latency, especially on large datasets. third while data itself is encrypted, accessed might be revealed and lead to possible inference attacks. Hence their applications remain limited in practice. Last but not least, the perpetual trust required in cloud service distributor is a questionable concern, for any breach at the providers end may let out the encrypted data to threats.

IV.PROPOSED SYSTEM

With the exponential growth of data in today's world, along with exponential cloud adoption, such options must offer high levels of data privacy and security while efficient search techniques.in this paper, we propose the secure encrypted keyword search framework, which works with the power of cloud computing, maintaining robust security measures over

sensitive information.it gives rise to an interesting concept where data encrypted before uploading it to the cloud and the search queries are processed in encrypted form as well. Our framework integrates advanced cryptographic techniques the homomorphic and searchable encryption to allow keyword inspection on encrypted data without revealing the plaintext of the content cloud provider. Proposed system essentially comprises three modules a data security module, a mechanism for generating secure indexes and an encrypted search algorithm.

Firstly, the data encryption module makes sure that all data is first encrypted by a strong symmetric encryption algorithm before sending to cloud thus guaranteeing the inaccessibility of the underlying data to cloud provider. Meanwhile a secure index is created from encrypted data using cryptographic hashing and homomorphic encryption.

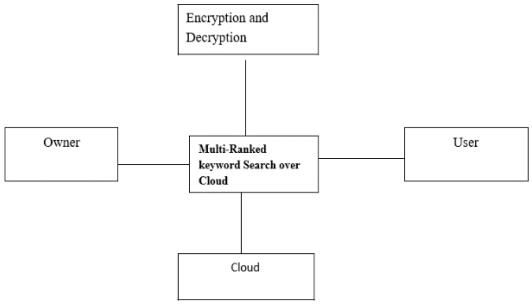

Fig: Context Diagram

At the time of searching the keyword of the user is similarly encrypted into a ciphertext using the same methodology as that applied during data encryption.it is then matched with the secure table in the cloud, which helps retrieve relevant encrypted data. Again, note that all this is done in the cloud server without decrypting anything ends to end security is preserved. The results are sent back to user for decryption locally using his private key.

V.MODULE DESCRIPTION IMPLEMENTATION

Carrying out module description for 'Encrypted Keyword Search Protection Using Cloud Computing'.

This project targets blueprint and appliance of the mechanism for safe and efficient keyword find over the encrypted data keep in the cloud. The computing cloud is leveraged to provide the required computational power and scalability for process.

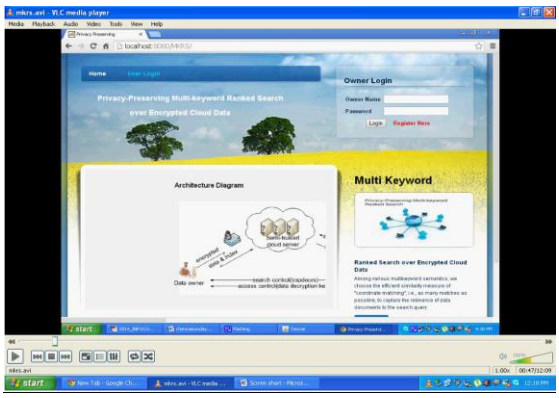

Fig: Home Page

Encryption Module

This module helps the owner to encrypt documents using RSA encryption. This module also encodes the search list sends it to the cloud. This module provides facilities for online file encryption by cloud services for a big number of users.

Client Module

This module helps the client to search documents with specific keywords and obtains the result. The client selects the required document, enters their details and obtain an activation code through an email from "mailfromchennaisunday" now the client has to enter the authorization code and then download the document.

Multi-keyword module

This module helps the client to get the proper result on the basis of different keyword queries. Here the client inputs various keywords. The server processes these keywords into a single term that is then used to search the matching result available in the database from where the client can download his required document.

Owner module

this tier enables the server to recognize hidden tools for account security management. The administrator uses a log key at login and updates it before he or she logs out. He is allowed to change the password after login managing client download permissions and handle manual request through the flowchart. Moreover, an administrator may update accounts after modifying the percentage of manual administrator tasks in a consistent manner.

VI. Result

it is the implementation of a multi-layered encryption scheme that greatly improves both security and efficiency. Specifically, it combines state-of-the-art cryptographic techniques of homomorphic and searchable encryption thus users can securely search for their encrypted data stored in the cloud without exposing the actual keywords or data itself to the cloud provider. What is innovative here is to piece together these encryption schemes in order to this security dwells not only in detail of information storage and transmission but also includes search queries. To this effect, this approach reduces the potential risks due to data breaches and unauthorized access, an important issue in cloud computing environments.

The project also solves more practical problems in deployment, creating a seamless framework that allows the integration of any current cloud storage service without major changes in the underlying infrastructure. This greatly enables adaptability and scalability, whereby it may be adopted by various organizations to improve their security

measures related to data without incurring high costs or huge operational disruptions.

Sl no.	Test Case	Expected Result	Actual Result	Status
1	Login form	Page displayed	Page displayed and given info	Pass
2	Incorrect info	Error	Error displayed	Pass
3	Application settings	Links and application to be managed	Links generated and options displayed	Pass
4	Login settings	Different login settings to be displayed	Selected from different options	Pass
5	Page design	Entered and updated in accordance	Results as according to the mode	Pass
6	Fields management	All options checked	Result as according to the mode	Pass

Fig: Test Case

CONCLUSION

The tradition proposed in this venture is toward supporting efficient ranked keyword searches for the effective utilization of remotely stored data in encrypted cloud computing. To do this appropriately for security, we turn into the newly developed primitive OPSE and derive an efficient many-to-many order-preserving mapping function to help in the construction of an effective Ranked Searchable Symmetric Encryption scheme. We present extensive experimental results to show the effectiveness of our solution. As a follow-up to existing studies, we point out some possible directions for future work on ranked keyword searches over encrypted cloud data. Since the IDF factor has to be involved for score computation, new approaches should be designed to perfectly preserve the order when generalizing scores for each of the provided keywords.

REFERENCE

[1] Curtmola, R., Garay, J.A., Kamara, S., & Ostrovsky, R. (2006). “Searchable symmetric encryption: improved definitions and efficient construction.” Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS). this paper presents foundational work on searchable symmetric encryption (SSE), which is crucial for understanding the basis of encrypted keyword search.

[2] Boneh, D., Crescenzo, G.D., Ostrovsky, R., & Persiano, G. (2004). “Public key encryption with keyword search.” Advances in Cryptology-EUROCYPY 2004.This work introduces the concept of public key encryption with keyword search (PEKS), laying the ground work for further developments in encrypted search.

[3] Goh, E. J. (2003) “Secure indexes.” IACR Cryptology ePrint Archive, Report 2003/216.Goh’s report discusses secure indexing methods, which are vital for creating efficient and secure searchable encrypted data.