OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

KEYWORD SEARCH SCHEME OVER ENCRYPTED DATA ON MOBILE CLOUD

KHAN SHIBA NAZ JAMEEL AHMAD[1], ASST.PROF. V. S. KARWANDE[2]

ME Student, Department of Computer Science & Engineering, EESGOI , India[1]

HOD, Assistant Professor, Department of Computer Science and Engineering, EESGOI, India. [2]

Abstract*: Cloud storage offers users easy, large, and scalable storage at a low cost, but data protection is a major concern that prevents users from trusting the cloud with their content. Encrypting files before uploading them to the cloud and decrypting them after accessing them is one way to enhance privacy from the viewpoint of the data owner. Data encryption, on the other hand, is a significant overhead for mobile devices, and data retrieval necessitates a convoluted communication mechanism between the data user and the cloud. With restricted network capacity and battery life, these problems usually result in considerable overhead in computing and communication, as well as increased power usage for mobile device users, making encrypted search over mobile cloud extremely difficult. We suggest TEES (Traffic and Energy Saving Encrypted Search) as bandwidth and energy efficient encrypted search architecture for the mobile cloud in the proposed framework. The proposed architecture offloads computation from mobile devices to the cloud, and the communication between mobile clients and the cloud is further optimized. It has been shown that when performance enhancing techniques are used, data protection does not suffer. Our tests show that TEES speeds up file retrieval and saves resources, while also reducing network traffic.

Keywords: *TEES (Traffic and Energy Saving Encrypted Search); Mobile Cloud Storage (MCS); symmetric encryption (SSE); order-preserving symmetric encryption (OPSE);. TF (Term Frequency); Order Preserving Encryption (OPE).*

----------∴∴∴----------

I INTRODUCTION

The Cloud storage is a service model in which data is maintained, controlled, and backed up remotely on the cloud side while remaining accessible to users via a network. Mobile Cloud Storage (MCS) refers to a group of growingly popular online services that serve as the primary file storage for mobile devices. MCS allows users of mobile devices to store and retrieve files or data on the cloud through wireless communication, improving data availability and facilitating file sharing without depleting the mobile device's local resources.

Since the problem of data protection is so important in cloud storage systems, confidential data is encrypted by the owner before being sent to the cloud, and data users retrieve the data they're searching for using an encrypted search scheme. However, because of the restricted processing and battery capacities of mobile devices, as well as data sharing and accessing approaches by wireless communication, mobile cloud storage systems face new challenges compared to conventional encrypted search schemes. As a result, MCS needs a suitable and effective encrypted search scheme.

Cloud computing, which can host and distribute services from remote servers, has become increasingly popular on the Internet recently. Cloud computing has the ability to manipulate large amounts of data and resources due to its simplicity and cost savings. Cloud storage is a popular cloud application that can be accessed from anywhere at any time. Individuals and businesses alike have flocked to the cloud for the ease of storing their data. When cloud storage becomes more commonly used, new problems emerge, such as data protection and privacy, which have been identified as the most significant barriers to people outsourcing their data to the cloud. Encrypting data before outsourcing it is an easy way to reduce the risk of confidential information being leaked to third-party service providers. However, since one

cannot explicitly search over the encrypted ciphertext, it makes data use more difficult. While some current techniques include searchable encryption, the creation of search indexes is based on the documents' pre-selected keywords. To boost search efficiency, an effective approximate keyword rank search scheme over encrypted cloud data is proposed. First, the relationships between keywords and documents are investigated. The length of record indexes can be decreased by removing the most important information from the initial indexes, according to the findings of the study.

The length of the record indexes that are retained trades computation time for search precision. Users' queries are often designed in a similar manner. Finally, to avoid the leakage of information found in documents and user requests, the validity of a user query and the document indexes is evaluated in encrypted form. The proposed scheme's efficiency is compared to that of the current scheme in. The proposed scheme effectively increases the search efficiency in terms of computation time and space, according to simulation results. This paper's contributions can be summarized as follows: For keyword rank search, a searchable encryption scheme with a shorter index length is suggested. The document index and question vector are built using latent semantic analysis. A real-world dataset is used to test the proposed system. The results show that while search precision can be preserved, search efficiency can be improved.

II LITERATURE SURVEY

Searchable Encryption is a new cryptographic technique that allows users to search encrypted data stored in the cloud. A novel searchable encryption scheme for the client-server architecture is introduced in this paper. The scheme uses the modular inverse's properties to create a probabilistic trapdoor that makes searching the stable inverted index table easier. We suggest indistinguishability by the use of a probabilistic trapdoor property. We build a proof-of-concept prototype and put it to the test with a real dataset of files. We equate the efficiency of our scheme to our argument that it is light in weight. In comparison to other current systems, our system provides a higher degree of protection, according to the security review[1].

Cloud storage has become one of the most commonly used forms of cloud computing as network bandwidth and Internet popularity have grown. Since the consumer may have a wide range of terminals, including PCs, notebook computers, and tablets PCs and smart phones can access data from a variety of locations and on multiple terminals, cloud storage is the most convenient. To share data between these devices, you'll need a suitable solution. Many customers are suspicious of the service for a variety of reasons. cloud storage protection, fearing that their data would be compromised will be misplaced or stolen As a consequence, cloud computing is difficult to implement. Large-scale storage. We attempt to develop a safety model in this paper.

for a new cloud storage security policy, and Examine the model's protection as well. Finally, we suggest some additional ideas. We have a number of technological issues to address [2].

Sensitive data is increasingly being consolidated into the cloud as Cloud Computing becomes more mainstream. Sensitive data must be encrypted before being outsourced to protect data privacy, making successful data use a difficult job. Traditional searchable encryption schemes allow users to safely search over encrypted data using keywords, but these techniques only support Boolean searches, which ignore data file relevance. When used specifically in the sense of Cloud Computing, this method has two significant flaws. On the one hand, users who do not have prior knowledge of the encrypted cloud data must post process each retrieved file in order to find the ones that most closely fit their interests; on the other hand, retrieving all files containing the queried keyword inevitably creates excessive network traffic, which is absolutely undesirable in today's pay-as-you-go cloud paradigm. We identify and solve the problem of efficient yet stable ranked keyword search over encrypted cloud data for the first time in this paper. Ranked search improves device efficiency by returning matching files in a ranked order based on certain relevance parameters (e.g., keyword frequency), bringing privacy-preserving data hosting services closer to realistic implementation in Cloud Computing. We show the inefficiency of the state-of-the-art searchable symmetric encryption (SSE) security concept by first giving a simple yet ideal construction of ranked keyword search. We then propose a specification for ranked searchable symmetric encryption and provide an efficient design by properly using the current cryptographic primitive, order-preserving symmetric encryption, to achieve better practical efficiency (OPSE). Our proposed solution, when compared to previous SSE schemes, has a “as-strong-as-possible” security guarantee while correctly realizing the target of ranked keyword search, according to a detailed review. Extensive experimental results show that the proposed solution is efficient [3].

Most data owners are outsourcing their corpus data from local sites to the commercial public cloud due to the advent of cloud computing, which provides greater flexibility and cost savings. However, sensitive data must be encrypted before being outsourced in order to protect data privacy, and encrypted data often provides efficient data utilization services, which is a difficult job. Traditional searchable encryption techniques, on the other hand, use Boolean search to search data using keywords, but this technique does not

meet the needs of multi-user data and retrieving huge data files from the cloud. The solution to this problem is to use ranked keyword search over encrypted cloud data, which increases device usability and file retrieval accuracy. Furthermore, one-to-many order-preserving mapping techniques have been developed and explored the relevance score, from information retrieval to the development of a safe searchable index, in order to protect the score information. In addition, the idea of score dynamics is being studied for use in upgrading encrypted cloud files. We proposed a framework in this paper to increase efficiency and protection by adding a physical layer security feature, which will make the system more stable and less vulnerable to attacks[4].

Cloud computing is commonly used by individuals and businesses to take advantage of a variety of cloud-based services. Users are persuaded to outsource their knowledge and records to an untrustworthy Cloud Service Provider through large databases in the cloud (CSP). However, there are some privacy and security issues with cloud storage that should be considered as major disadvantages to expanding it among users. Encrypting data before sending it to the cloud is one of the methods for maintaining data security in cloud storage. This ensures data security and increases users' confidence in the CSP. This, however, prohibits users from directly searching outsourced documents. Standard encryption algorithms, such as AES, RC4, and DES, have a searching restriction in that the entire ciphertext must be retrieved and then decrypted before the search procedure can begin. Users' search features have recently been the focus of a lot of research. In most cases, a keyword-based search strategy is employed. Users may use this method to retrieve only the documents that contain specific keywords. Searchable encryption algorithms, on the other hand, have privacy and security issues. The Secure Searchable Based Asymmetric Encryption (SSAE) algorithm is proposed in this paper, which provides indistinguishability under the Adaptive-Chosen Ciphertext Attack. The proposed searchable encryption algorithm has been mathematically proven to be stable, and it can search encrypted data without decrypting it[5].

Individuals and corporate customers can eliminate high capital outlays in the procurement and management of both software and hardware, as well as the operating overhead that comes with it, thanks to cloud computing. Despite the numerous advantages, outsourcing data storage to the commercial public cloud deprives consumers of full control over the systems that handle their data, making protection and privacy the most significant barriers to cloud adoption. Although data encryption protects data confidentiality, it also renders the conventional data utilization service based on plaintext keyword search obsolete. As a result, providing an encrypted cloud data search service with privacy assurance is critical. With such a large number of data users and a large number of outsourced data files in the cloud, this problem is especially difficult to solve, as it is extremely difficult to satisfy the realistic requirements of accuracy, device usability, and high-level user searching experiences. This paper examines these issues and defines the problem of fuzzy keyword search over encrypted cloud data, which should be examined for efficient cloud data use. For suitable device usability and overall user searching experience, fuzzy keyword search aims to accommodate various styles and representation inconsistencies in different user searching input while preserving keyword privacy. We also investigate how the concept of fuzzy search naturally supports similarity search, a fundamental and efficient method commonly used in information retrieval, in order to broaden the range of secure cloud data usage services. We explore the issues that current searchable encryption methods have yet to address, as well as research directions and technological approaches that might help these new search functionalities become a reality. The proposed research could be the cornerstone for cloud service providers to deliver value from cloud technology to their enterprise and individual customers in a safe and productive manner, thus facilitating widespread adoption of cloud computing[6].

III. SYSTEMS ARCHITECTURE

We use updated routines and new algorithms to implement the modules in our system in order to improve protection while also increasing energy and traffic performance. There will be three parts of our system's presentation.The Data Owner, to offload the measurement and ranking load of the relevance scores to the cloud, the data owner generates a TF (Term Frequency) table as an index and encrypts it using Order Preserving Encryption (OPE). We introduce our one-to-many OPE in the data owner module to monitor the statistics information leak.The Data User,to help manage the keywords-files connection leak, we wrap the keywords to be checked by adding some noise in the data user module. We use a ranking feature to measure the relevant score on the cloud in order to get the top-k relevant files.

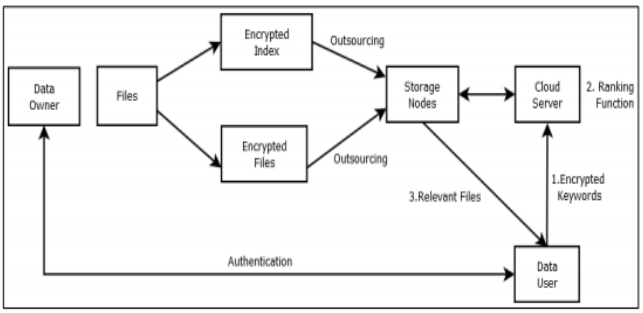

Figure No 3.1: System Architecture

The cloud server is in charge of calculating the relevance scores for the data user to get the top-k related files given a keyword in ORS (One Round Trip Search). As a result, both the unwrap and rank functions are implemented in the cloud server module.

IV EXPERIMENTAL RESULTS

In this Fig.4.1 show the make-series operator is used to partition and convert the original telemetry table into a collection of time series for analysis. Using a variety of functions This graph depicts a time analysis graph of file vs. uploading time (ms).

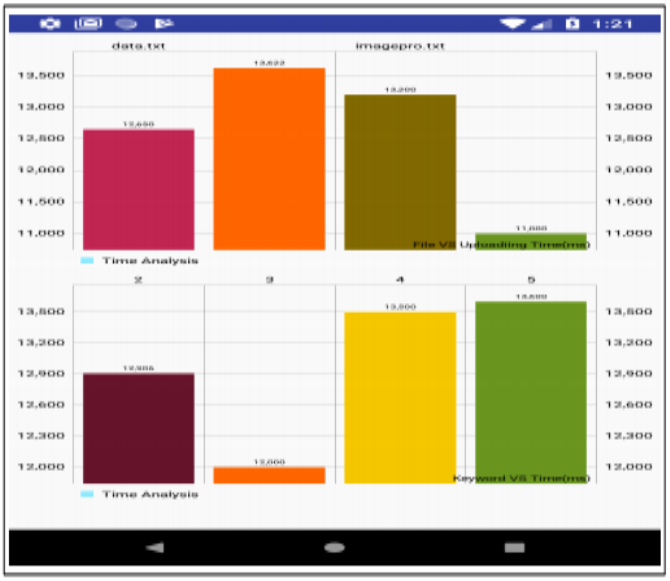

Figure No 4.1: Experimental Results

In the existing system required time for search file is more but in the proposed system required less time for search files as shown in figure 4.2:

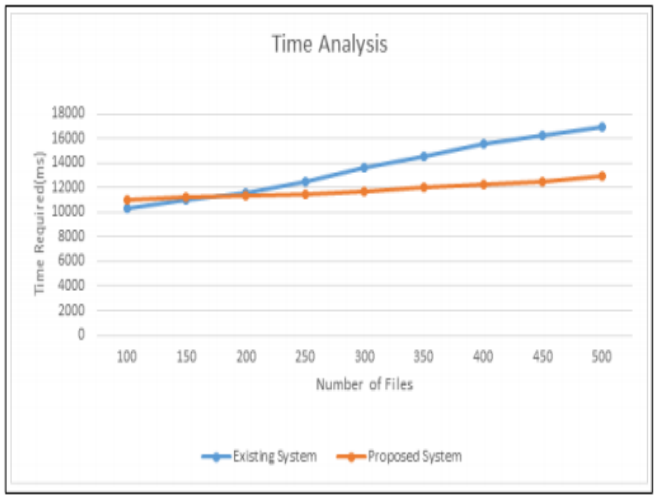

Figure No 4.2: Existing System Vs. Proposed System

V CONCLUSION

In this paper we developed an efficient implementation to achieve encrypted search in a mobile cloud. The proposed system's security analysis revealed that it is safe enough for mobile cloud computing, and a series of tests demonstrated its effectiveness. When compared to conventional methods with equivalent levels of protection, it saves a lot of resources. This work can be expanded to include more innovative applications based on the proposed scheme. To make encrypted data search effective, we proposed a single keyword search scheme.

REFERENCES

[1]. Shahzaib Tahir, Sushmita Ruj, Yogachandran Rahulamathavan, Muttukrishnan Rajarajan, Cornelius Glackin, "A New Secure and Lightweight Searchable Encryption Scheme over Encrypted Cloud Data," IEEE Transactions on Emerging Topics in Computing, 2168-6750 2017.

[2] Zhang Jing, Wang Jinsu, Zheng Zhuangfeng, Zhao Chongan, "Cloud Storage Encryption Security Analysis," IEEE International Conference on Cloud Computing and Big Data Analysis., 978-,20 16.

[3] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," International Conference on Distributed Computing Systems, 2010.

[4] Payal V. Kale, Prof. Rashmi Welekar, "A Survey on Different Techniques for Encrypted Cloud Data," International Conference on Intelligent Computing and Control Systems, 2017.

[5] Majid Bakhtiari, Majid Nateghizad, Anazida Zainal, "Secure Search Over Encrypted Data in Cloud Computing," International Conference on Advanced Computer Science Applications and Technologies, 2013.

[6] Cong Wang, Qian Wang, and Kui Ren, "Towards Secure and Effective Utilization over Encrypted Cloud Data," International Conference on Distributed Computing Systems Workshops, 2011.

[7] Haoran Yuan, Xiaofeng Chen, "Secure Cloud Data Deduplication with Efficient Re-encryption," IEEE Transactions on Services Computing, 2019.

[8] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong TMACS: A robust and verifiable threshold multi-authority access control system in public cloud stor age 2015 IEEE.

[9] Yingjie Xue, Jianan Hong, Wei Li and Kaiping Xue, LABAC: A location-aware attribute-based access control scheme for cloud storage 2016 IEEE.

[10] Jianan Hong, Kaiping Xue TAFC: Time and attribute factors combined access control on time sensitive data in public cloud 2015 IEEE.

[11] Kaiping Xue, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, David S.L. Wei, "Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage," IEEE Transactions on Information Forensics and Security, 2016.

[12] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi honest-but-curious cloud servers", in Communications (ICC), 2012 IEEE In ternational Conference on. IEEE, 2012.

[13] J. Zhang, B. Deng, and X. Li, "Additive order preserving encryption based encrypted documents ranking in secure cloud storage", Advances in Swarm Intelligence, pp. 5865, 2012.

[14] N. Cao,C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi keyword ranked search over encrypted cloud data", in INFOCOM, 2011 Pro ceedings IEEE. IEEE, 20