JOURNAL OF BASIC SCIENCE AND ENGINEERING

SECURE DATA MANAGEMENT SYSTEM WITH ENHANCED AUTHENTICATION AND ACCESS CONTROL

Ms.D.RAJAPRIYA M.E.,(Ph.D.)

Department of Computer Science and Engineering Karpagam College Of Engineering
Othakkalmandapam, Coimbatore-641032
rajapriya.d@kce.ac.in

JAYAVARSHINI.K

Department of Computer Science and Engineering Karpagam College Of Engineering
Othakkalmandapam, Coimbatore-641032
jayavarshinikannan@gmail.com

RAGAVI.K.C

Department of Computer Science and Engineering Karpagam College Of Engineering
Othakkalmandapam, Coimbatore-641032
ragavikc@gmail.com

MATHUSREE.P.S

Department of Computer Science and Engineering Karpagam College Of Engineering
Othakkalmandapam, Coimbatore-641032
nklmathu35@gmail.com

Abstract**—**The emergence of cloud computing, data owners are being driven to move their intricate data management systems from on-site locations to private cloud providers in order to take advantage of increased flexibility and cost savings. However, sensitive data must be encrypted before being outsourced in order to safeguard data privacy. This renders outdated the conventional method of using data, which relies on plaintext keyword searches. It is therefore crucial to activate an encrypted cloud data search service. In order to satisfy the effective data retrieval demand, search services must support multi-keyword queries and offer result similarity rating, given the volume of data users and documents stored in cloud storage. Similar efforts on searchable encryption seldom distinguish between search results and concentrate on single keyword or Boolean keyword search. In this paper, we formulate and solve the difficult problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM) for the first time. We also define a stringent set of privacy requirements that must be met in order to realize such a secure cloud data utilization system. The effective principle of "Enhanced Association Rule Mining coordinate matching," or capturing as many matches as possible, is our choice among multiple-keyword semantics for measuring similarity between search queries and data documents. We then use "inner product similarity" to quantitatively formalize this principle for similarity measurement.

Keywords—Cloud Computing, Security, Encryption, Efficiency Analysis, keyword mapping, cyber-attack.

INTRODUCTION

In the vast landscape of contemporary computing, cloud computing emerges as a transformation force, delivering a spectrum of services via the internet. This paradigm shift enables businesses and individuals to seamlessly access a great number of IT resources, ranging from servers, storage, and databases to software, analytic, and intelligence, all on a flexible, as-needed basis through renowned cloud providers such as Microsoft Azure, G oogle CloudPlatform and Amazon Web Services. The three types of cloud computing services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) - constitutes the foundational elements of this digital revolution. The merits of cloud computing are manifold, encompassing agility, facilitating rapid scalability, cost savings through pay-as-you- go models, and heightened security, as cloud providers invest in cutting-edge technologies to safeguard customer data. Diving into the realm of data security within the cloud, Symmetric Searchable Encryption (SSE) takes center stage, offering a ground breaking approach to preserving privacy while out sourcing data to the cloud. SSE, leveraging symmetric encryption algorithms, allows users to search encrypted data without the need for decryption. By generating encrypted searchable indexes and employing trapdoor for search queries, users can interact seamlessly with encrypted data stored on cloud servers, ensuring protection against keyword search, pattern search, and content leakage attacks. Privacy-preserving cloud data search, a pivotal technique, empowers data owners to leverage the cloud's scalability while maintaining control over data privacy. This is achieved through the encryption of data before outsourcing and the use of cryptographic techniques, such as searchable encryption and homo morphic encryption, enabling cloud providers to search encrypted data without decrypting it. This becomes especially critical for businesses handling sensitive datalike customer information or financial records, offering a robust shield against potential compromises. The importance of encrypted cloud data amplifies in the digital age, where businesses and organizations increasingly rely on cloud storage. Encrypted cloud data, whether implemented through server-side encryption performed transparently by the cloud provider or client-side encryption executed by users prior to uploading data, serves as a potent defense against security threats. It guards against data breaches, thwarting unauthorized access even in the event of a compromised cloud provider. It also addresses insider threats by restricting decryption without the requisite encryption key, and shields against government surveillance by ensuring encrypted data remains in decipherable without the corresponding encryption key. As more entities transition their data to the cloud, thread option of encrypted cloud data becomes paramount for safeguarding privacy and security, presenting a straight forward yet effective strategy against diverse security threats inherent in the digital landscape.

I. ENCRYPTEDCLOUDDATA

The process of using encryption methods to protect sensitive data kept in cloud settings is known as "encrypted cloud data," which helps to improve privacy and security. With the growing number of people and business depending on cloud services for storage and data processing, it is critical to safeguard private information from possible breaches and unwanted access. Encrypted cloud data is essentially protected from unauthorized parties, including service providers themselves, by encoding the data in way that rendersitunint eligible without the necessary decryption keys. This method addresses issues with data privacy and regulatory compliance by adding an extra degree of protection. In the constantly changing world of cloud computing, users may reduce the dangers of data exposure by using encrypted cloud data practices, guarantee eingamore reliable and safe storage option.

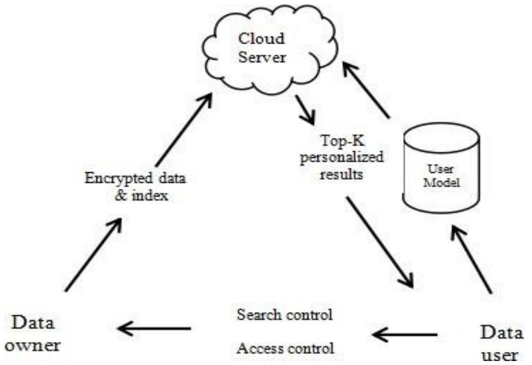

Figure1.Encryptedcloud data

CLOUDSTORAGE

The way data is stored, accessed, and managed is being completely transformed by the revolutionary technology known as cloud storage. Essentially, it entails saving data on distant servers that users can access online, giving them scalable and practical options for storing and retrieving data. With this revolutionary method, real gear and on-premises infrastructure are no longer required, providing a more adaptable and affordable option. The smooth uploading, downloading, and sharing of data by users promotes accessibility and cooperation across geographic borders. Prominent suppliers of cloud storage include prominent entities such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, who provide an array of services customize dto meet thevarying requirements of their clientele. Despite the many advantages of cloud storage, worries about privacy and data security have prompted the creation of authentication and encryption protocols to guarantee the integrity and confidentiality of stored data. Cloud storage, which provides scalable and effective solutions for both consumers and organizations, is becoming more important in creating the digital world.

RELATEDWORK

The notion of exchanging personal health data via cloud storage in a healthcare-cyber physical system has gained popularity in recently ears in ceitenhances access quality. The privacy of health data can only be protected by encrypting it, but this reduces usefulness and flexibility in terms of effective search. Attribute-based searchable encryption (ABSE) has demonstrated its use by enabling fine-grained searching in shared cloud storage. This technique, however, is impractical for devices with limited capabilities and storage space since a typical ABSE requires significant calculations. In a healthcare cloud- based cyber-physical system(CCPS),data is frequently gathered by resource-constrained devices; hence, ABSE techniques cannot be applied directly here. The proposed method manages the inherent computational cost of the ABSE scheme by performing the computationally heavy operations of a typical ABSE scheme on the block chain network. Thus, the suggested approach is appropriate for online storage and retrieval of personal health data in a conventional CCPS. The suggested system provides two major benefits by utilizing block chain technology.

MODULEDESCRIPTION

To create a cloud data usage system more secure, we must first describe and solve the difficult problem of search over encrypted cloud data (EARM) and privacy- preserving multi-ke word ranked ontology keyword mapping. We also construct a tight set of privacy constraints. Among many multi-keyword semantics, we select the effective "coordinate matching" concept. We formulate a set of privacy principles for such a safe cloud data usage system and present the problem of Secured Multi keyword search (SMS) over encrypted cloud data (ECD). We choose the most effective coordinate matching rule as many matches as possible from the number of multi-keyword semantics to determine the degree of similarity between the search query and the data. To further refine the matching process, we employ inner data correspondence to quantitatively formalize this similarity measurement principle. Using secure inner product computing, we first present a basic Secured multi keyword ranking ontology keyword mapping and search strategy, which we subsequently refine to satisfy various privacy criteria.

A. CLOUDSETUP

Instead of delivering results that are not distinguishable, this module improves the schemes that support multi-keyword queries and offer result similarity rating for efficient data retrieval. Privacy-Preserving: To protect privacy and stop the cloud server from getting further information from the dataset and index. Efficiency: Minimal communication and processing overhead should be required to meet the aforementioned functionality and privacy criteria.

B. EARMCOORDINATEMATCHING

An intermediary similarity metric called coordinate matching" counts the amount of query keywords that exist in the content in order to determine how relevant the document is to the query. Boolean searches perform effectively when users pinpoint the precise subset of the dataset that has to be recovered and meet

their specified search criteria. Users may more easily find the most pertinent publications in a rank order by selecting a list of keywords that express their concerns. In order to protect data privacy, the data owner can use conventional symmetric key cryptography to encrypt the data before outsourcing, so preventing the cloud server from accessing the data that has been outsourced. If the cloud server determines that there is a connection between encrypted documents and keywords, it may compromise index privacy. As a result, a searchable index has to be created to stop association attacks like this one from occurring on the cloud server.

C. PREFILTERINGANDSECURITYMANAGEMENT

This module is designed to assist the user in obtaining precise results by using several keyword ideas. Users can input a query with several words; the server will combine those words into a single term after searching our database for that word. Ultimately, the user obtains the file from the pre-filtered list of matching words in the database. Another way to define the search query is as a binary vector association rule, where each bit indicates if the matching phrase exists in the request. The query vector and data vector's inner product might be used to precisely assess the similarity.

Encrypt Module

This module helps the server to encrypt the document using DES Algorithm, convert them to a Zip file with an activation code, and sends the code to the user for download.

Client Module

With the aid of this module, the client may search the file with various key phrases and receive an exact list of results depending on their query. Before entering the activation code, the user must choose the necessary file, register their information, and get an activation code in the mail from the "customerservice404" email. The user may then download and extract the Zip

file.

Multi-keyword Module

This module is designed to assist the user in obtaining precise results by using several keyword ideas. Users can input a query with several words; the server will combine those words into a single term after searching our database for that word. Lastly, show the user the database's matched word list so they may select the file from it. The similarity may be precisely calculated by taking the inner product of the query vector and data vector. The search query is furthermore represented as a binary vector, where each bit indicates whether the matching term exists in this request for information. Direct outsourcing of data vectors or query vectors, however, will infringe upon search or index privacy.

Admin Module

The server may examine details and upload files with security thanks to this module. The log key to the login time is used by the admin. Modify the log key prior to the admin logging out. After logging in, the administrator may check the user's downloading history and the specifics of each file request counted on a flowchart, as well as modify the password. Once the Zip file format has been converted, the administrator can upload the file.

Ranking Result

Whenever any of the user request for the file(data)then Ranking will happen on requested file(data) using kNN algorithm. After the process the results of the query is given to the user.

SYSTEMFLOWDIAGRAM

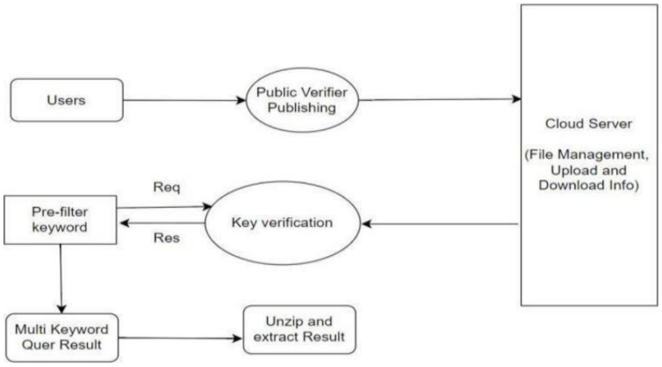
Users
Public Verifier Publishing
Cloud Server
(File Management, Upload and Download Info)
Req
Pre-filter keyword
Key verification
Res
Multi Keyword Quer Result
Unzip and extract Result

Figure6: SystemflowDiagram

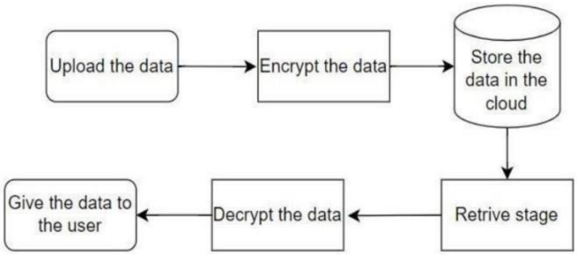

Figure6: FlowArchitecture

SYSTEMTESTINGAND IMPLEMENTATION

The system testing for the proposed EARM (Encrypted and Attribute-Based Retrieval Model) scheme aims to ensure that it fulfills essential requirements. Privacy is apar amount concern, necessitating the protection of both data and keywordsfrom any potential compromise, even when stored on the cloud server. The accuracy of the scheme is crucial, demanding that search results be ranked based on their relevance to the search query. Additionally, efficiency and scalability are vital aspects, requiring the scheme to perform effectively across varying workloads. Security is a fundamental requirement,necessitating robust measures against unauthorized access and potential attacks. In terms of system implementation, the EARM scheme can be realized through various technologies and platforms. The process involves the user encrypting data using a secure encryption scheme, followed by uploading the encrypted data to the cloud. Subsequently, the user submits a search query to the system, which then utilizes privacy parameters to generate a secure token. This secure token is then transmitted to the cloud server, completing the retrieval process. By adhering to these steps, the EARM scheme ensures a secure, accurate, and efficient encrypted data retrieval process while maintaining user privacy and safeguarding against potential security threats.

ALGORITHMDETAILS

Establishing a secure cloud data utilization system involves tackling the difficult problem of search over encrypted cloud data (EARM) and privacy-preserving multi- keyword ranking ontology keyword mapping and. This study proposes a formal way for addressing this issue and presents a comprehensive set of privacy restrictions. From several multi- keyword semantics, the "coordinate matching" notion emerges as the most successful, and it will guide our approach.

Function Secured Multi Keyword Search(encrypted Cloud Data, encrypted Query): initialize privacy constraints and principles for each keyword in encrypted Query:

Encrypted Ontology Terms retrieve Encrypted Ontology Terms(keyword, encrypted Cloud Data) similarity Scores compute Similarity Scores(encrypted Query, encrypted Ontology

```
 Terms) selected Ontology Terms select Top Matches(similarity Scores) fortermin selected
 Ontology Terms:
  Inner Data Similarity compute Inner Data Similarity(term, encrypted Query) inner
   Product
Secure Inner Product(term, encrypted Query) rank And Refine(term, inner Data
Similarity, inner Product) Return ranked Encrypted Cloud Data
```

RESULTANALYSIS

In this section, the focus is on the methodology and results of a recommendation system. This system involves the user encrypting data using a secure encryption scheme. The cloud admin provides the secret key to the user. With the help of these key user will upload the data. The uploaded data is in encrypted for meven the cloud admin can't able to see what the data is. While downloading the uploaded data the decryption process is carried out with the help of the secrete key provided by the admin to the user. The process begins with the step of key providence followed by uploading of the data. The uploaded data is in encrypted form. This data is stored in the server/cloud. While downloading the data decryption will takes place to get the original data. A comparison of the accuracy levels of a suggested algorithm with an existing algorithm is shown in the accompanying table. Within the dataset, the current approach attains an accuracy rate of 70%, whereas the suggested technique shows a significant enhancement with an accuracy rate of 80%. The performance difference between the two algorithms is summarized in this table, which shows that the suggested method performs better in terms of accuracy than the current one. The 10% improvement in accuracy indicates that, in comparison to the established approach, the suggested algorithm provides outcomes with improved precision or dependability. For academics, practitioners, and stakeholders in the area, this data is in valuable since it offer saclear picture of the improvements in accuracy performance brought about by the suggested method.

algorithm	accuracy
existing	70
proposed	80

Table1.Comparisontable

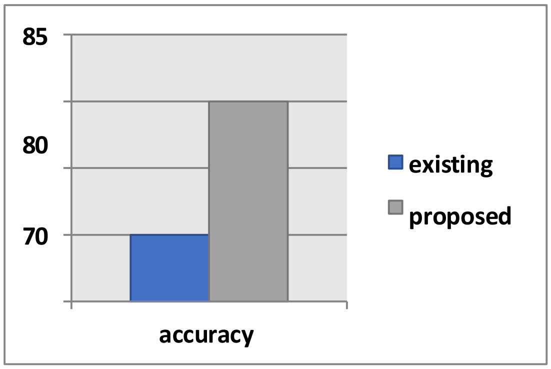

Figure1.Comparisongraph

CONCLUSION

To sum up, our Enhanced Association Rule Mining (EARM) technology is a major step forward in data mining and information retrieval techniques. Our approach strikes an equilibrium between privacy protection and efficiency by deftly combining the concepts of secure inner product computation and coordinate matching. The system's flexibility to adjust to multiple threat models guarantee esitsapplicability in a range of situations and meets varying degrees of privacy needs Extensive testing, encompassing privacy resilience, accuracy validation and performance evaluation, confirms our EARM system’s dependability. Its practicality is further supported by the low processing and communication overhead seen in real-world studies. Our EARM system’s dependability. Its practicality is further supported by the low process in gand communication overhead seen in real-world studies. Our EARM system, as a comprehensive solution, is ready to contribute significantly to the area by offering a strong framework for similarity assessment and respecting strict privacy guidelines.

II. REFERENCES

[1] Zulifqar, Anayat, Kharal, (2021) “A Review of Data Security Challenges and their Solutions in Cloud Computing.” International Journal of Information Engineering & Electronic Business, 13(3): 32-41.

[2] Sun.(2019)“Privacy protection and data security in cloud computing: a survey, challenges, and solutions.” IEEE Access, 7: 147420-147452.

[3] Ilakiya, Vijithra, Kuppusamy, and Mahalakshmi. (2019) “Impact of Asymmetric Encryption in Cloud Computing: A Study.” International Journal of Computer Sciences and Engineering, 7(3): 32-43.

[4] Malhotra and Singh. (2019) “An Optimized Solution for Ranking Based On Data Complexity.” International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(11): 41-49.

[5] Islam, Chaudhury, and Islam. (2019) “A simple and secured cryptography system of cloud computing.” In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), IEEE:1-3.

[6] Suneetha, Kishore, Singh, (2019) “A Security Model Using Artificial Neural Networks and Database Fragmentation in Cl Environment”, International Journal of Recent Technology and Engineering(IJRTE)8(2):34- 43.

[7] Tyagi. (2021) “Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional- Neural Networks (CNN).” International Journal of Computer Networks and Applications, 8(4): 288- 299

[8] Sana, Li, Javaid, Liaqat, and Ali. (2021) “Enhanced Security in Cloud Computing Using Neural Network and Encryption.” IEEE Access, 9: 145785-
145799.

[9] Pulido-Gaytan, Tchernykh, Cortés-Mendoza, Babenko, Radchenko, Avetisyan, and Drozdov. (2021) “Privacy- preserving neural networks with Homomorphic encryption: Challenges and opportunities.” Peer- to-Peer Networking and Applications, 14(3): 1666-1691 38

[10] Zhang, Qiuyu,MinruiFu,YiboHuang, and ZhenyuZhao (2022) "Encrypted Speech Retrieval Scheme Based on Multiuser Searchable Encryption in Cloud Storage." Security and Communication Networks