E-ISSN 2250-0944
ISSN 2250-1150
doi: 10.31838/ijprt/14.01.07

Research Article

An Efficacy Analysis of Data Encryption Architecture For Cloud Platform

P. DINESHKUMAR[1], K. GEETHA[2], V. JEEVA[3], P.J. ARUN[4], C. NITHIESH[5]
[1]Assistant Professor, Department of Information Technology, K.S.Rangasamy College of Technology, Tiruchengode - 637 215.
[2]Professor, Department of Computer science and Engineering, Excel Engineering college, Komarapalayam – 638 183.
[3,4,5]UG Students, Department of Information Technology, K.S.Rangasamy College of Technology Tiruchengode - 637 215

Received: 17.09.23, Revised: 25.10.23, Accepted: 09.11.23

ABSTRACT

With the rise of cloud computing, many data owners are opting to outsource their complex data management systems to commercial public clouds for greater flexibility and cost savings. However, to ensure data privacy, sensitive data must be encrypted before outsourcing, which renders traditional plaintext keyword search obsolete. Therefore, it is crucial to enable an encrypted cloud data search service that allows for multi-keyword queries and provides result similarity ranking to meet the needs of effective data retrieval. While previous works on searchable encryption have focused on single keyword search or Boolean keyword search, they have rarely differentiated the search results. In this paper, we address the challenging problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM) for the first time. We establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality, given the large number of data users and documents in the cloud.

Keywords: Cloud Computing , Symmetric Searchable Encryption , Privacy-Preserving Cloud Data Search, Encrypted Cloud Data.

1. INTRODUCTION

1.1 Cloud Computing

Distributed computing is the conveyance of processing administrations over the web ("the cloud"). With distributed computing, organizations and people can get to an expansive scope of IT assets, like servers, stockpiling, data sets, organizing, programming, examination, and insight, dependent upon the situation from a cloud supplier like Amazon Web Administrations (AWS), Microsoft Sky blue, or Google Cloud Stage (GCP).

1.2 Symmetric Searchable Encryption

Symmetric accessible encryption (SSE) is a sort of encryption that permits clients to look through over encoded information without decoding it. This is helpful for re-appropriating information to a cloud server while as yet having the option to look through done with everything. SSE works by first scrambling the information utilizing a symmetric encryption calculation. The client then produces an accessible file of the encoded information, which is likewise scrambled. The file is then shipped off the cloud server, alongside the encoded information. At the point when the client needs to look through over the information, they send a secret entryway for the pursuit catchphrase to the cloud server. The cloud server utilizes the secret entryway to look through the scrambled file and returns a rundown of encoded reports that match the pursuit rules. The client can then decode the encoded records to see the outcomes.

1.3 Privacy-Preserving Cloud Data Search

Security safeguarding cloud information search is a strategy that permits information proprietors to re-appropriate their information to the cloud while as yet keeping up with command over their protection. This is accomplished by encoding the information prior to re-appropriating it, and afterward utilizing cryptographic procedures to permit the cloud supplier to look through the scrambled information without having the option to decode it. Protection saving cloud information search is significant on the grounds that it permits information proprietors to exploit the adaptability and adaptability of the cloud without agonizing over their information being compromised. This is particularly significant for organizations and associations that store touchy information, like client data or monetary information. There are various ways of carrying out protection saving cloud information search.

1.4 Encrypted Cloud Data

Scrambled cloud information is information that has been encoded prior to being put away in the cloud. This is finished to shield the information from unapproved access, regardless of whether the cloud supplier is compromised. There are various ways of scrambling cloud information. One normal methodology is to utilize a procedure called server-side encryption. Server-side encryption is finished by the cloud supplier, and it is straightforward to the client. This implies that the client doesn't need to do anything unique to scramble their information. One more way to deal with encoding cloud information is to utilize a procedure called client-side encryption. Client-side encryption is finished by the client before the information is transferred to the cloud. This implies that the cloud supplier never approaches the decoded information. Encoded cloud information is turning out to be progressively significant as an ever increasing number of organizations and associations are moving their information to the cloud**.**

2. LITERATURE REVIEW

2.1 A Survey Of Information Security Difficulties And Their Answers In Distributed Computing

Isma Zulifqar et.al. Has proposed in this paper, Distributed computing is the freshest electronic processing network that offers the clients with advantageous and adaptable assets to access or work with various cloud applications. Distributed computing is the accessibility of the PC network administrations, essentially putting away information and computational power, without unequivocal client dynamic control. The information in distributed computing is put away and gotten to on a far off server by utilizing cloud specialist co-op' applications. Giving insurance is a main pressing concern since data is moved to the far off server through a medium. It is critical to handle the security issues of distributed computing prior to executing it in an association. In this paper, we point out the information related security issues and answer for be tended to in the distributed computing organization. To shield our information from noxious clients we can carry out encryption. We enjoy examined the benefits of distributed computing in our paper.

2.2 Security Assurance And Information Security In Distributed Computing: An Overview, Difficulties, And Arrangements

Dish Jun Sun et.al. Has proposed in this paper Protection and security are the main issues to the ubiquity of distributed computing administration. Lately, there are many exploration plans of distributed computing security assurance in light of access control, quality based encryption (ABE), trust and notoriety, however they are dispersed and need brought together rationale. In this paper, we deliberately survey and dissect applicable examination accomplishments. To start with, we examine the design, ideas and a few deficiencies of distributed computing, and propose a structure of security insurance; second, we talk about and break down fundamental ABE, KP-ABE (key arrangement characteristic based encryption), CP-ABE (figure text strategy trait based encryption), access structure, disavowal system, multiauthority, fine-grained, follow component, intermediary re-encryption(PRE), progressive encryption, accessible encryption(SE), trust, notoriety, expansion of custom access control and various leveled key; third, we propose the examination challenge and future bearing of the security assurance in the distributed computing; at long last, we direct out comparing security insurance regulations toward compensate for the specialized lacks.

2.3 Effect Of Uneven Encryption In Distributed Computing: A Review

M. Ilakiya et.al. Has proposed in this framework, distributed computing" a type of On-request processing utilized by business people groups, associations and organizations on pay - as-your premise. The Distributed computing worldview enjoy many benefits like accessibility, adaptability, robotized refreshes on programming, improved coordinated effort and effectively reasonable, that makes it as a proficient mechanism for use. Security danger to its information put away in shared medium is a central issue. To guarantee the verification of the information numerous components were being used. Over past many years Cryptography is one most broadly involved method for hiding information from outsider. Symmetric key cryptography involves the comparable key for both the encryption and decoding of messages. All things considered, Uneven key cryptography utilizes two distinct kinds of keys. This paper examined about the concise outline of calculations and components done by the analysts in regards to validation and approval issues in the hilter kilter key situation. Distributed computing is a worldview for conveyance of registering administrations over the web, on-request, as pay as your administration.

2.4 An Upgraded Answer For Positioning In View Of Information Intricacy

Sheenam Malhotra et.al. Has proposed in this framework; Distributed computing is an arising field with part of opportunities for the support at the Framework Layer and Programming Layer. A capacity design is related with two cycles specifically the capacity and the recovery interaction. The capacity design assumes an imperative part in how rapidly the information is recovered. The recovered information is introduced according to the heaviness of the recovered information. This paper presents an original secure stockpiling and the positioning system for the reports for cloud. As no past reference for any information is kept at the server, the information is encoded in light of the co-connection between the information documents determined by Cosine closeness. The positioning of the recovered information is finished through Managed AI system. The assessment of the boundaries is finished on the foundation of calculation time and all out number of genuine recoveries on multi-watchword search. Different dataset from Kaggle are utilized to perform and cross approve the proposed calculation. Distributed computing gives a suitable and solid administrations to the clients as far as putting away and protecting the information by partaking in the excellent administrations. The more prominent adaptability and financial reserve funds are the spurring factors for the organizations and ventures to deal with the complicated neighbourhood information in the cloud.

2.5 A Basic And Got Cryptography Arrangement Of Distributed Computing

SM Jahidul Islam et.al. Has proposed in this framework; Distributed computing is a tremendous developing innovation in the IT enterprises. Cloud Specialist organizations (CSP) are offering different reasonable and adaptable administrations to the clients. Clients of distributed computing are filling in an equivalent rhyme. As distributed computing is turning into a fundamental piece of human existence, clients and CSP are seeing for appropriate security feathers. Numerous analysts are working in the security parts of distributed computing. In this paper, we present a reasonable cryptography and secure confirmation framework for distributed computing. This methodology incorporates auto encryption and KEYs changing cycle in the cloud end. New produced KEYs won't be shipped off clients at first. Clients will be actually looked at in three stages for verification. CSP can set off encryption process whenever physically or it will be performed consequently after logged out by the clients. This technique will guarantee additional security for information/documents as well as keep programmers from getting unique records/information even they got legitimate qualification.

3. EXISTING SYSTEM

In recent times, cloud computing is widely used for storage and information sharing purposes in various established commercial segments, particularly in online businesses like Google and Amazon. Cloud systems offer several benefits to users, including easy operations, low implementation costs, and reduced maintenance expenses. However, there are significant risks associated with data security procedures in cloud systems. Despite ongoing analysis and reforms in this area, concerns about cloud data protection and user reliability remain uncertain due to the increasing prevalence of cyber-attack schemes and errors in cloud storage systems. To address this risk and contribute to the effort of providing optimal data security solutions in cloud data storage and retrieval systems, this paper proposes a cloud data encryption and retrieval model influenced by Symmetric Searchable Encryption and Machine Learning. The proposed model enhances data security and incorporates an effective keyword ranking approach using an Artificial Neural Network.

4. PROPOSED SYSTEM

We present a novel approach to address the complex issue of maintaining privacy while conducting multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (EARM). In order to make this secure cloud data utilization system a reality, we establish a comprehensive set of stringent privacy requirements. Among the various multi-keyword semantics available, we have chosen the efficient principle of "coordinate matching" as the basis for our proposed Secured Multi keyword search (SMS) over encrypted cloud data (ECD). To ensure the security of this system, we have developed a series of privacy policies. To determine the similarity between a search query and the encrypted data, we employ the highly efficient rule of coordinate matching, which aims to maximize the number of matches. Additionally, we utilize inner data correspondence to quantitatively formalize this principle for similarity measurement. Our initial proposal involves a basic Secured multi keyword ranked ontology keyword mapping and search scheme that utilizes secure inner product computation. Subsequently, we have made improvements to meet various privacy requirements. The ranked results obtained from this system provide the top k retrieval results. Furthermore, we have introduced an alert system that generates alerts in the form of emails and messages whenever an unauthorized user attempts to access the data stored in the cloud.

4.1 Cloud Setup

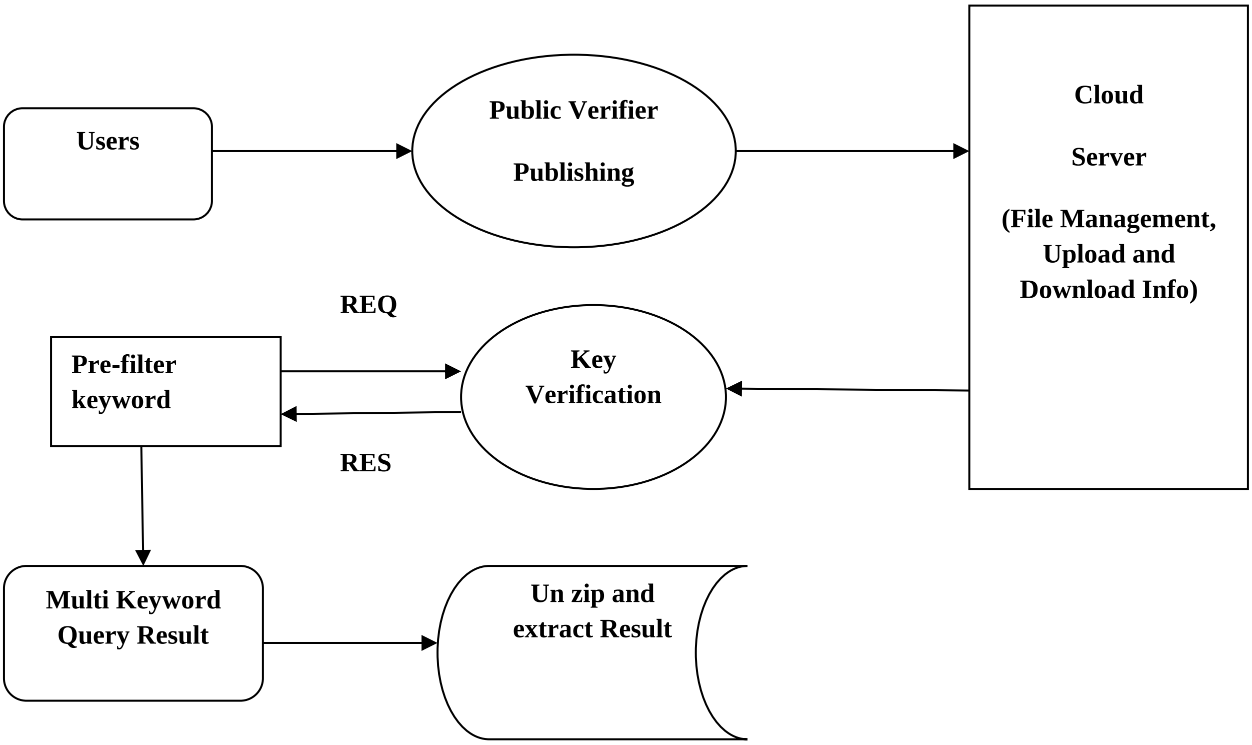
This module improves the existing schemes by enabling multi-keyword queries and providing a ranking of results based on their similarity to enhance the effectiveness of data retrieval. It ensures privacy by preventing the cloud server from gaining any additional information from the dataset and index, while also meeting privacy requirements. The module aims to achieve these goals with minimal communication and computation overhead.

4.2 Earm Coordinate Matching

"Coordinate matching" is an intermediate measure of similarity that quantifies the relevance of a document to a query based on the number of query keywords it contains. Boolean queries work well when users know the exact subset of the dataset they want to retrieve. However, this module offers more flexibility by allowing users to specify a list of keywords that indicate their areas of interest, and then retrieves the most relevant documents in a ranked order.

4.3 Prefiltering And Security Management

This module assists users in obtaining accurate results based on multiple keyword concepts. Users can enter a query with multiple words, which the server will then split into individual words and search for corresponding files in the database. The module then prefilters the matched word list from the database, allowing the user to retrieve the desired file. The search query is represented as a binary vector association rule, where each bit indicates whether a corresponding keyword appears in the search request. The similarity between the query vector and data vector can be precisely measured using the inner product.


Users
Public Verifier
Publishing
Cloud
Server
(File Management, Upload and Download Info)
REQ
Pre-filter keyword
Key Verification
RES
Multi Keyword Query Result
Un zip and extract Result

Encrypt Module

The Encrypt Module is utilized by the server to encrypt documents using the TRIPLE DES Algorithm. It also converts the encrypted document into a Zip file, which includes an activation code. This activation code is then sent to the user for download.

Client Module

The Client Module assists the client in searching for files using the concept of multiple keywords. It provides an accurate result list based on the user's query. The user can select the desired file, register them details, and receive an activation code via email from the "customerservice404" email address. The activation code must be entered before the user can download and extract the Zip file.

Multi-keyword Module

The Multi-Keyword Module aids the user in obtaining accurate results based on multiple keyword concepts. Users can enter a query consisting of multiple words. The server will split the query into individual words and search for corresponding files in the database. The module then displays a list of matched words from the database, allowing the user to retrieve the desired file. The search query is represented as a binary vector, where each bit indicates whether a corresponding keyword appears in the search request. The similarity between the query vector and data vector is measured by the inner product. However, directly outsourcing the data vector or query vector would compromise index privacy or search privacy.

Admin Module

This module facilitates secure viewing of details and file uploads by the server. The administrator utilizes a log key to record login times and is advised to change it before logging out. After logging in, the administrator can modify their password and access flowcharts displaying user download and file request details. Additionally, the administrator can upload files in Zip format.

File upload Module

This module facilitates the server in securely viewing details and uploading files. The administrator utilizes the log key to record the login time. Prior to logging out, the administrator is required to modify the log key. After logging in, the administrator has the ability to modify the password and access the flowchart displaying user downloading details and file request counts. Additionally, the administrator can upload files after converting them to the Zip file format.

Ranking Result

The requested data undergoes a ranking process utilizing the k-nearest neighbor algorithm when a user makes a data request. The ranking process employs the co-ordinate matching principle. Once the ranking is complete, the user receives the anticipated query results.

5. CONCLUSION

The proposed EARM scheme represents a significant advancement in the realm of privacy-preserving cloud data search. This comprehensive and sophisticated solution effectively tackles all major challenges associated with this issue, ensuring security, efficiency, and scalability. The EARM scheme has the potential to revolutionize the way we store and search for data in the cloud, enabling users to search for encrypted data without compromising their privacy. This innovative solution can be applied to a range of applications, including secure cloud storage, privacy-preserving data sharing, and secure search for sensitive data. Although still under development, the EARM scheme promises to safeguard the privacy of our data and online activities.

6. FUTURE WORK

The privacy of the EARM scheme can be enhanced by employing advanced encryption and obfuscation techniques. For instance, the utilization of homomorphic encryption enables search functionality on encrypted data without the need for decryption. Additionally, the EARM scheme can be expanded to accommodate more intricate queries, including Boolean and range queries. To further enhance the performance and scalability of the EARM scheme, the implementation of more efficient algorithms and data structures is recommended. Distributed algorithms can be employed to effectively handle substantial workloads.

REFERENCES

1. Zulifqar, Anayat, Kharal, (2021) "A Survey of Information Security Difficulties and their Answers in Distributed computing." Worldwide Diary of Data Designing and Electronic Business, 13(3): 32-41.
2. Sun. (2019) "Security assurance and information security in distributed computing: a study, difficulties, and arrangements." IEEE Access, 7: 147420-147452

3. Ilakiya, Vijithra, Kuppusamy, and Mahalakshmi. (2019) "Effect of Hilter kilter Encryption in Distributed computing: A Review." Global Diary of PC Sciences and Designing, 7(3): 32-43.
4. Malhotra and Singh. (2019) "An Advanced Answer for Positioning In light of Information Intricacy." Worldwide Diary of Creative Innovation and Investigating Engineering(IJITEE), 8(11): 41-49.
5. Islam, Chaudhury, and Islam. (2019) "A straightforward and got cryptography arrangement of distributed computing." In 2019 IEEE Canadian Gathering of Electrical and PC Designing (CCECE), IEEE: 1-3.