www.ijiarec.com

ISSN:2348-2079

Volume-9 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

A novel multilevel ranking technique for cloud computing services based on quality and usability

Mrs. B. Ananthi., M.E., Ms. Priyadharshini. S.V, M.E

[1]Assistant Professor, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Elayampalayam – 637205.

[2]Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Elayampalayam – 637205.

ABSTRACT

In this paper, a fine-grained question approval plot with respectability check is proposed over scrambled spatial information for area based administrations (LBS). The fine-grained inquiry approval is empowered dependent on a circulation of the spatial information by utilizing a non-uniform segment in the spatial area to produce a thickness based space filling bend (DSC), which can be utilized to create list esteems for questioning and change keys. The change keys can be utilized to produce question tokens for a protected spatial inquiry just as develop a change key tree whose sub tree can be conveyed by the LBS supplier to an approved client as change key for question tokens age. Fine-grained access control schemes are commonly used in cloud computing. In this type of schemes, each data item is given its own access control policy. The entity that wants to access the data item needs to provide its credentials to a policy enforcer. In a cloud environment, normally, the policy enforcer is not the owner of the data. The access control policies and the credentials might reveal some information that the policy enforcer is not entitled to know. This paper proposes a fine-grained access control scheme. It prevents the policy enforcers from comprehending the access control policies and the entities credentials by using cryptographic techniques. Compared with the existing schemes, the proposed scheme provides higher level privacy. Besides, the proposed conspire builds a Binary Key Coordinate Matching with MKS-Tree(Multidimensional keyword Search) to help honesty check by totaling a summary of the spatial information dependent on the DSC and utilizing the MKS-tree as a confirmation structure. The LBS supplier can share a sub tree of the MKS-tree to approved client as his confirmation structure, which relates to the change key of the approved client. Along these lines, the approved client can just create the substantial question tokens and check the inquiry brings about his approved district. The security properties of the proposed plot is talked about, and broad test results exhibit the high productivity of confirmation structure age and check tasks.

INTRODUCTION

Searchable Encryption supports the query capabilities over the encrypted data at the cloud without decryption. Nevertheless, most of the SE schemes focus on SQL queries, and cannot be directly employed to spatial data because of the completely different relationship among the data. To enable query services on encrypted spatial data, space filling curves have been widely used to transform the original locations of POIs to one-dimensional index values. Space filling curve passes through every partition of a closed space, and has no intersection with itself. In this way, each point in multi-dimensional space will be mapped as a value to one-dimensional space. Standard Hilbert curve (SHC) as a form of space filling curve is applied as a building block in many schemes for spatial data transformation, which can protect the confidentiality of outsourced spatial

Author for correspondence:
Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women

data and make effective spatial queries. With the transformation key and the original spatial query, users can generate the query tokens to search over the encrypted spatial data. Thus, the fine-grained verification capability authorization is supported, which means only the users with the verification structure corresponding to the authorized region can verify the integrity of the query result. The proposed scheme is suitable for the application where the LBS provider (data owner), such as Foursquare, provides POI data to the third party companies and developers [1-5].

LITERATURE REVIEW

Facilitating secure and efficient spatial query processing on the cloud

Ayesha M. Talha has proposed in this paper database redistributing is a typical distributed computing worldview that permits information proprietors to exploit its on-request capacity and computational assets. The primary test is keeping up information classification concerning untrusted parties i.e., cloud specialist organization, just as giving applicable question brings about ongoing to confirmed clients. Existing methodologies either bargain classification of the information or experience the ill effects of high correspondence cost between the worker and the client. To beat this issue, we propose a double change and encryption conspire for spatial information, where encoded inquiries are executed completely at the administration supplier on the encoded database and scrambled outcomes are come back to the client. The client issues scrambled spatial range questions to the specialist organization and afterward utilize the encryption key to unscramble the inquiry reaction returned. This permits a harmony between the security of information and productive inquiry reaction as the inquiries are handled on encoded information at the cloud worker.

Lightweight fine-grained search over encrypted data in fog computing

Yinbin Miao has proposed in this paper fog computing, as an extension of cloud computing, outsources the encrypted sensitive data to multiple fog nodes on the edge of Internet of Things (IoT) to decrease latency and network congestion. However, the existing cipher text retrieval schemes rarely focus on the fog computing environment and most of them still impose high computational and storage overhead on resource-limited end users. In this paper, we first present a Lightweight Fine-Grained cipher texts Search (LFGS) system in fog computing by extending Cipher text-Policy Attribute-Based Encryption (CP-ABE) and Searchable Encryption (SE) technologies, which can achieve fine-grained access control and keyword search simultaneously. The LFGS can shift partial computational and storage overhead from end users to chosen fog nodes. Furthermore, the basic LFGS system is improved to support conjunctive keyword search and attribute update to avoid returning irrelevant search results and illegal accesses.

Fastgeo: Efficient geometric range queries on encrypted spatial data

Boyang Wang has proposed in this paper spatial information have wide applications, e.g., area based administrations, and mathematical range inquiries (i.e., discovering focuses inside mathematical territories, e.g., circles or polygons) are one of the major hunt capacities over spatial information. The rising interest of re-appropriating information is moving huge scope datasets, including enormous scope spatial datasets, to open mists. In the meantime, because of the worry of insider assailants and programmers on open mists, the security of spatial datasets ought to be mindfully protected while questioning them at the worker side, particularly for area based and clinical utilization.

EXISTING SYSTEM

The large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. The searchable encryption focuses on single keyword search or Boolean keyword search, and rarely differentiates the search results.

DISADVANTAGES

- Single-keyword search without ranking is not possible
- Identity based keyword extraction is not available
- Less security.
- Poor reliability.
- Boolean- keyword search without ranking
- Single-keyword search with ranking

PROPOSED SYSTEM

We define and solve the challenging problem of privacy-preserving multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (MROS), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching". We propose the problem of Secured Multi key word search (SMS) over encrypted cloud data (ECD), BKCM with MKS-Tree (Multidimensional keyword Search and construct a group of privacy policies for such a secure cloud data utilization system. From number of multi-keyword semantics, we select the highly efficient rule of coordinate matching, i.e., as many matches as possible, to identify the similarity between search query and data , and for further matching we use inner data correspondence to quantitatively formalize such principle for similarity measurement.

We first propose a basic Secured multi keyword ranked ontology keyword mapping and search scheme using secure inner product computation, and then improve it to meet different privacy requirements. The Ranked result provides top k retrieval results. Also we propose an alert system which will generate alerts when un-authorized user tries to access the data from cloud, the alert will generate in the form of mail and message.

ADVANTAGES OF PROPOSED SYSTEM

- Multi-keyword ranked ontology keyword mapping and search over encrypted cloud data MKS-Tree (Multidimensional keyword Search).
- "Coordinate matching" by inner product similarity.
- Secured Multi keyword ranked ontology keyword mapping and search : To design search schemes which allow multi-keyword query and provide result similarity ranking for valuable data retrieval, instead of returning undifferentiated results.
- Privacy: To prevent cloud server from learning additional information from dataset and index, and to meet privacy requirements. Effectiveness with high performance: Above goals on functionality and privacy should be achieved with low communication and computation overhead.

SOFTWARE REQUIREMENTS

- Operating System : Windows XP Professional
- Front end : JDK 1.7/Net Beans 8.2
- Coding Language: Java
- Backend: SQL SERVER

PROPOSED METHODOLOGY

Secure Privacy Preserving Keyword Search (SPKS) grants cloud service provider to decrypt the data and return file containing keywords. This technique overcomes the computation and communication overhead, provides query and data privacy for the users. It figures out six algorithms for efficient searching on encrypted data. The flow of Secure multi keyword search (SMS) with co-ordinate matching is illustrated. First, TRIPLE DES Algorithm for Key Generation used to generate a public/private key pair. Second, the encrypts all the content in the file and keywords are encrypted respectively which then stored in the server. Third, To compute used on the retrieving phase where user generates a trapdoor and pass it to CSP (cloud service provider). Fourth, TRIPLE

DES with MROS checks whether the keyword contains in the encrypted data. Fifth, Decrypt mainly for CSP to decrypt the intermediate result partly and sends the cipher text and the partial decrypted content .Sixth, Recovery runs by the user to decrypt the plain text. Therefore it provides semantic security in plain text attack.

The following steps are required while searching takes place in encrypted data using multi-Ranking keyword search.

- Multi-dimensional query are converted to its sms secure multikeyword search coordinate matching .
- Attributes are defined in a hierarchical way. i.e., attribute hierarchy.
- Indexes and capabilities are generated by MROS Index and Classified Average Precision algorithm respectively.

It is a multi-round protocol between server and user on single keyword .It uses per index file where each document contains a keyword. The keyword index is encrypted using pseudorandom bits using heuristic pseudorandom functions.

On the setup phase user chooses a random secret key to encrypt the file. Then the user submits index and file content to server .On the retrieval phase, when the user wants to search or retrieve file from the server, user retrieves the index file and then computes keyword with the secret key .The computed key is sent to server, where server matches the file and then sent to the user .The per-index file scheme using pseudorandom functions is the better than using bloom filters. This scheme fails when multiple keywords are used.

MODULE DESCRIPTION
ONTOLOGY KEYWORD MAPPING

To allow ranked ontology keyword mapping and search for operative use of outsourced cloud data under the aforesaid model, our system design should instantaneously achieve security and performance assurances as follows Multi keyword ranked ontology keyword mapping and search : To design search schemes which allow multi-keyword query and provide result similarity ranking for effective data retrieval, instead of returning undifferentiated results.

Privacy-Preserving: To prevent the cloud server from learning additional information from the dataset and the index, and to meet privacy. Efficiency: Above goals on functionality and privacy should be achieved with low communication and computation overhead [6-8].

COORDINATE MATCHING

“Coordinate matching” is an intermediate similarity measure which uses the number of query keywords appearing in the document to quantify the relevance of that document to the query. When users identify the exact subset of the dataset to be regained, Boolean queries achieve well with the exact search necessity stated by the user. It is more elastic for users to identify a list of keywords indicating their concern and regain the most relevant documents with a rank order.

Data privacy, the data owner can resort to the traditional symmetric key cryptography to encrypt the data before outsourcing, and effectively prevent the cloud server into the outsourced data.

Index privacy, if the cloud server infers any association between keywords and encrypted documents from index. Therefore, the searchable index should be built to prevent the cloud server from acting such kind of association attack.

Keyword Privacy, as users generally wish to have their search from existence showing to others like the cloud server, the most vital concern is to hide what they are searching, i.e., the keywords specified by the corresponding trapdoor. The trapdoor can be generated in a cryptographic way to protect the query keywords.

ENCRYPT MODULE

This module is used to help the server to encrypt the document using TRIPLE DES Algorithm and to convert the encrypted document to the Zip file with activation code and then activation code send to the user for download.

CLIENT MODULE

This module is used to help the client to search the file using the multiple key words concept and get the accurate result list based on the user query.

The user is going to select the required file and register the user details and get activation code in mail from the "customerservice404" email before enter the activation code. After user can download the Zip file and extract that file.

MULTI-KEYWORD ONTOLOGY MAPPING MODULE

This module is used to help the user to get the accurate result based on the multiple keyword concepts. The users can enter the multiple words query, the server is going to split that query into a single word after search that word file in our database. Finally, display the matched word list from the database and the user gets the file from that list. The search query is also described as a binary vector where each bit means whether corresponding keyword appears in this search request, so the similarity could be exactly measured by inner product of query vector with data vector. However, directly outsourcing data vector or query vector will violate index privacy or search privacy. To meet the challenge of supporting such multi-keyword semantic without privacy breaches, we propose a basic SMS scheme using secure inner product computation, which is adapted from a secure k-nearest neighbor (kNN) technique, and then improve it step by step to achieve various privacy requirements in two levels of threat models.

- Showing the problem of Secured Multi-keyword search over encrypted cloud data
- Propose two schemes following the principle of coordinate matching and inner product similarity.

ADMIN MODULE

This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart. The admin can upload the file after the conversion of the Zip file format.

FILE UPLOAD MODULE

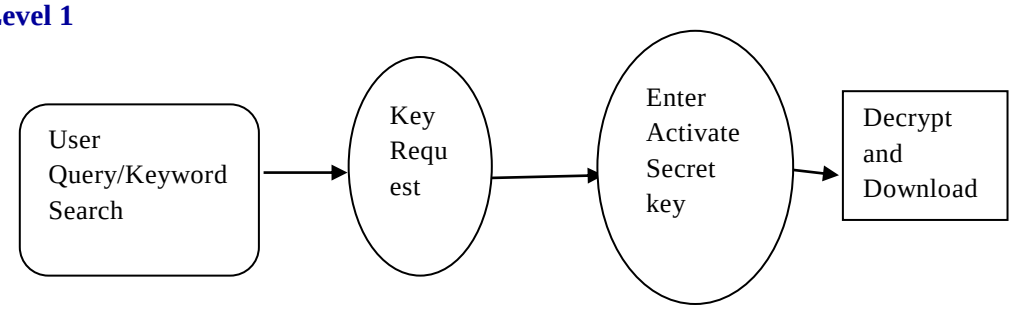
This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart. The admin can upload the file after the conversion of the Zip file format.

RANKING RESULT

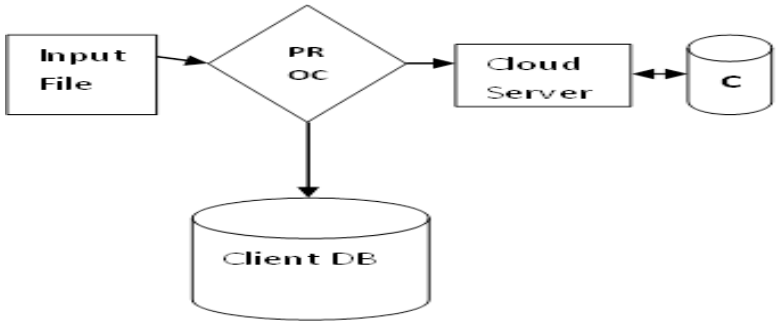
When any User request for the data then Ranking is done on requested data using k-nearest neighbor algorithm. For ranking ―co-ordinate matching‖ principle is used. After ranking user gets the expected results of the query.

SYSTEM FLOW DIAGRAM

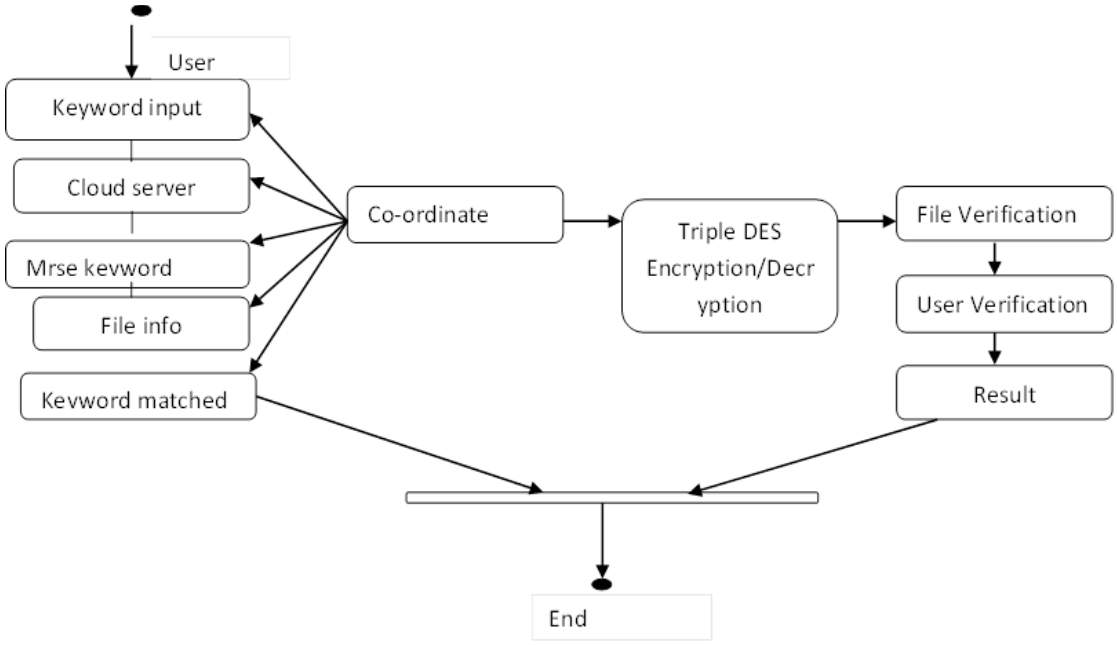
Level 1



Level 2



PROCESS FLOW DIAGRAM



EXPERIMENTAL SETUP AND RESULT

Multiple users are created at a centralized location for the data owners and data users. We can see that either of the users can access the system once they login.

The exchange of communication between data owners and data users is strictly through Data frames system which enables the system to be secured. Since the contents are encrypted and kept in the cloud, public viewing of these files is impossible.

The files or contents can be viewed only after the consent of the data owners, after getting the secret key.

Data Encryption and decryption Result When Triple DES algorithm is applied on the data then we get encrypted data. And that encrypted data is store on the cloud. User can access the data after downloading and decrypting file. For encryption and decryption keys are provided.

Ranking Result When any User request for the data then Ranking is done on requested data to co-ordinate matching‖ principle is used. After ranking user gets the expected results of the query.

SYSTEM IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and

effective. implementation of a modified application to be replaced as an existing one. This type of conve Triple DES tion is relatively easy to handle, provided there are no major changes in the system. .

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

CLOUD SETUP

In this module we have setup data owner and cloud server. So the data owner is going push the data into the cloud sever. When users outsource their private data onto the cloud, the cloud service providers are able to control and monitor the data and the communication between users and the cloud will be secured Cryptography cloud Storage In this module while the data is uploaded into data may contain sensitive information, the cloud servers cannot be fully entrusted in protecting data. For this reason, outsourced files must be encrypted. Any kind of information leakage that would affect data privacy are regarded as unacceptable In this model we used a series of searchable symmetric encryption schemes have been enable search on cipher text. In the former, files are ranked only by the number of retrieved keywords, which impairs search accuracy Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to all users and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system.

Thus we proposed the problem of multiple-keyword ranked search over encrypted cloud data, and construct a variety of security requirements. From various multikeyword concepts, we choose the efficient principle of coordinate matching. We first propose secure inner data computation. Also we achieve effective ranking result using k-nearest neighbour technique.

This system is currently work on single cloud, In future is will extended up to sky computing & Provide better security in multi-user systems.

CONCLUSION

In this paper, a fine-grained inquiry approval plot with honesty confirmation is proposed over the encrypted spatial information for area based administrations. Considering the conveyance of the spatial information, a thickness based space filling bend is intended to create the inquiry records of the encoded spatial information, and question token age and result confirmation approaches are acquainted with ensure finegrained and evident spatial inquiry. The proposed plot empowers the information proprietor to accomplish fine-grained spatial area approval in both the question token age and question result check.

Trial results illustrate that the computational expense of the record and confirmation structure age approaches is not as much as that of BKCM with MKS Tree Mapping based approaches, and the computational and capacity costs of the uprightness confirmation approach are not as much as that of SPR. Also, the honesty confirmation plot doesn't present bogus negative in the outcomes confirmation. In the future work, the time factor will be considered in the fine-grained undeniable inquiry approval, which empowers client to produce inquiry tokens and check the question results as it were in his approved area and time run.

REFERENCES

[1]. M. Talha, I. Kamel, and Z. A. Aghbari, “Facilitating secure and efficient spatial query processing on the cloud,” IEEE Transactions on Cloud Computing, 7(4), 2019.

[2]. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, “Lightweight fine-grained search over encrypted data in fog

computing," IEEETransactions on Services Computing, 12(5), 772–785, 2019.

[3]. Wang, M. Li, and L. Xiong, "Fastgeo: Efficient geometric range queries on encrypted spatial data," IEEE Transactions on Dependableand Secure Computing, 16(2), 2019, 245–258.

[4]. G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Transactions on Information Forensics and Security, 14(4), 2019, 870–885.

[5]. Y. Ji, C. Xu, J. Xu, and H. Hu, "vabs: Towards verifiable attribute based search over shared cloud data," in Proc. of the 35th International Conference on Data Engineering, Macao, China, 2019, 2028–2031.

[6]. J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Providing task allocation and secure deduplication for mobile crowd sensing via fog computing," IEEE Transactions on Dependable and Secure Computing, 17(3), 2018, 581–594.

[7]. M. U. Arshad, A. Kundu, E. Bertino, A. Ghafoor, and C. Kundu, "Efficient and scalable integrity verification of data and query results for graph databases," IEEE Transactions on Knowledge and Data Engineering, 30(5), 2018, 866–879.

[8]. Yang, J. Xu, J. Weng, J. Zhou, and D. S. Wong, "Lightweight and privacy-preserving delegatable proofs of storage with data dynamics in cloud storage," IEEE Transactions on Cloud Computing, 2018, DOI: 10.1109/TCC.2018.2851256.