ISSN:2348-2079

Volume-8 Issue-4

International Journal of Intellectual Advancements and Research in Engineering Computations

Fine-grained request approval with truth form over encrypted spatial data in cloud storage

Dr.S.Sadesh[1], G.Ashish[2]

[1]Professor, Computer Science and Engineering, Velalar College of Engineering and Technology, Erode 12, Tamil Nadu, India.

[2]M.E Student, Dept. Computer Science and Engineering, Velalar College of Engineering and Technology, Erode 12, Tamil Nadu, India.

ABSTRACT

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 scheme, each data item is given its own access control policy. 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 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.

Keywords: Key Coordinate Matching, MKS-Tree, Fine-grained inquiry, Spatial Data, Tokens, LBS supplier, Sub tree.

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 [1-5]. TSpace 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 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 [6-10].

Author for correspondence:
Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Erode 12, Tamil Nadu, India.

LITERATURE SURVEY

Facilitating secure and efficient spatial query processing on the cloud

Database redistributing is a typical distributed computing worldview that permits information proprietors to exploit its on-request capacity and computational assets. Existing methodologies either bargain classification of the information or experience the ill effects of high correspondence cost between the worker and 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 [11-18]. 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. In addition, we contrast and existing methodologies on enormous datasets and show that this methodology lessens the normal question correspondence cost between the approved client and specialist co-op, as just a solitary round of correspondence is required by the proposed approach. We characterize a few assault models and show that our plan gives solid protection from them. This permits a harmony between the security of information and quick reaction time as the inquiries are handled on encoded information at the cloud worker. Along these lines, the double change strategy protects the information as well as empowers the validated clients to recover spatial range question reactions effectively.

Fastgeo: efficient geometric range queries on encrypted spatial data

The rising interest of re-appropriating information is moving huge scope datasets, including enormous scope spatial datasets, to open mists. In this paper, we formalize the idea of Geometrically Searchable Encryption, and propose an effective plan, named FastGeo, to ensure the security of customers' spatial datasets put away and questioned at an open worker. FastGeo underpins subjective mathematical zones, accomplishes sub linear search time, and empowers dynamic refreshes over scrambled spatial datasets. We propose FastGeo, an effective two-level hunt plot that can work mathematical ranges over encoded spatial datasets. Our test results over a real-world dataset exhibit its viability by and by. Additionally, our correlation with past arrangements shows that the overall thought of two-level inquiry can be utilized as a significant technique to help search time and empower profoundly productive updates over scrambled information when complex activities, for example, process then compare activities, are engaged with search.

Enabling efficient and geometric range query with access control over encrypted spatial data

A basic query function, range query has been exploited in many scenarios such as Sql retrieves, location-based services, and computational geometry. A long-standing problem is that the user's data may be completely revealed to the cloud server because it has full data access right. We propose an Efficient and Geometric Range Query scheme (EGRQ) supporting searching and data access control over encrypted spatial data. We employ secure KNN computation, polynomial fitting technique and order-preserving encryption to achieve secure, efficient and accurate geometric range query over cloud data. To improve the efficiency, R-tree is adopted to reduce the searching space and matching times in whole search process. Finally, we theoretically prove the security of our proposed scheme in terms of confidentiality of spatial data, privacy protection of index and trapdoor, and the unlink ability of trapdoors. EGRQ can achieve both arbitrary geometric range query and data access control with one round of communication. Benefited from R-tree adopted to reduce the searching space and matching times in whole querying process, it is also not vulgar that the performance of computing overhead in our EGRQ. Security analysis also demonstrates the high security of our proposed scheme in terms of confidentiality of spatial data, privacy protection ofindex and trapdoor, and the unlink ability of trapdoor.

Light weight and privacy-preserving delegable proofs of storage with data dynamics in cloud storage

Distributed storage has been in across the board use these days, which lightens clients' weight of neighbour hood information. Stockpiling. Capacity

(POS) is the primary procedure acquainted with address this issue. POS permitting a third gathering to confirm the information trustworthiness in the interest of the information proprietor altogether improves the versatility of cloud administration. we propose another variation plan called "Delegatable Proofs of Storage (DPOS)". Accelerate the label age process by at any rate a few multiple times, without giving up productivity in some other angle. Our plan is sound and protection saving against evaluator in the standard model. The proposed plot is as productive as private key POS plot, particularly very productive in validation label age. Certain POS plots, our own improves the verification label age speed by multiple times. Our conspire likewise forestalls information spillage to the reviewer during the examining procedure.

Secure range search over encrypted uncertainiot outsourced data

The operation of IOT needs a strong data handling capacity, where most of the data is sensor data. Limitations associated with measurement, delays in data updating, and or the need to preserve the privacy of data can result in the sensor data being uncertain. Searchable encryption (SE) scheme is a promising technique that allows the searching over encrypted (uncertain) data stored offshore. Use homo morphic and order-preservin gencryption (OPE) to encrypt data published by the data owners. Design is to ensure the privacy of the dataset, without affecting the efficiency of keyword search on the (encrypted) dataset. The diversity and range of IoT devices will grow as they are deployed in a broader range of applications, ranging from civilian to military and battle field and so on. The security of uncertain IoT data, particularly those outsourced to the cloud or the edge, we developed an effective indexing technique to support range searches on multidimensional encrypted data. Using the KD-tree to organize the objects to improve the retrieval efficiency. OPE and homomorphic encryption scheme to encrypt the dataset.

Identity-based data outsourcing with comprehensive auditing in clouds

Cloud storage system provides facilitative file storage and sharing services for distributed clients. Identity-based data outsourcing (IBDO) scheme equipped with desirable features advantageous over existing proposals in securing outsourced data. The proxies are identified and authorized with their recognizable identities, which eliminates complicated certificate management in usual secure distributed computing systems. Security analysis and experimental evaluation indicate that our IBDO scheme provides strong security with desirable efficiency. Introduced the notion of identity based data outsourcing and proposed a secure IBDO scheme. The identity-based feature and the comprehensive auditing feature make our scheme advantageous over existing PDP/PoR schemes. Security analyses and experimental results show that the proposed scheme is secure and has comparable performance as the SW scheme.

Verifiable social data outsourcing

Social data outsourcing is an emerging paradigm for effective and efficient access to the social data. A third-party Social Data Provider (SDP) purchases complete social datasets from Online Social Network (OSN) operators and then resells them to data consumers who can be any individuals or entities desiring the complete social data satisfying some criteria. Initiate the study on verifiable social data outsourcing whereby a data consumer can verify the trustworthiness of the social data returned by the SDP. The OSN provider to generate some cryptographic auxiliary information, based on which the SDP can construct a verification object for the data consumer to verify the query-result trustworthiness. Extensive experiments based on a real Twitter dataset confirm the high efficacy and efficiency of our schemes. In this paper, we initiated the study of verifiable social data outsourcing to allow a data consumer to verify the trustworthiness of the social data returned by the SDP. The data consumer to verify the social-graph correctness, social-graph completeness, and content authenticity of any query result returned by an untrusted SDP.

System analysis

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 method

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 keyword 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

1. Multi-keyword ranked ontology keyword mapping and search over encrypted cloud data **MKS-Tree (Multidimensional keyword Search).**
2. "Coordinate matching" by inner product similarity.
3. 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.
4. 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.

Module description

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 keyword 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**.

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

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.

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

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.

Ontology keyword mapping

Cloud data under the aforesaid model, our system design should instantaneously achieve security and performance by **(MROS).**

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 over head.

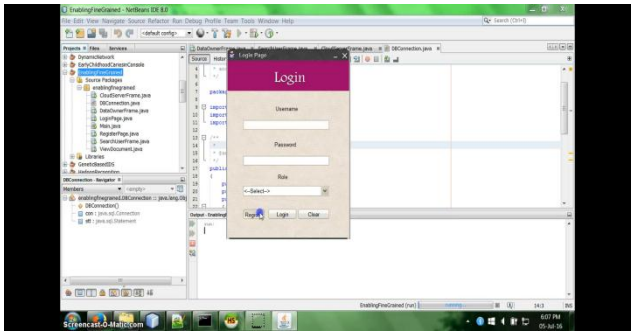
Coordinate matching

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. 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.

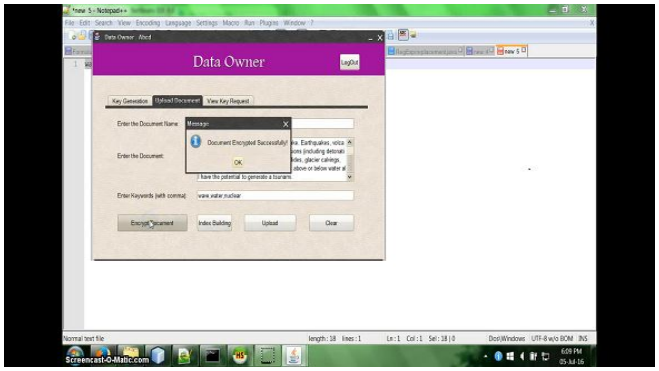
- Data privacy
- Index privacy
- Keyword Privacy.
- The trapdoor can be generated in a cryptographic way to protect the query keywords.

RESULT AND IMPLEMENTATION

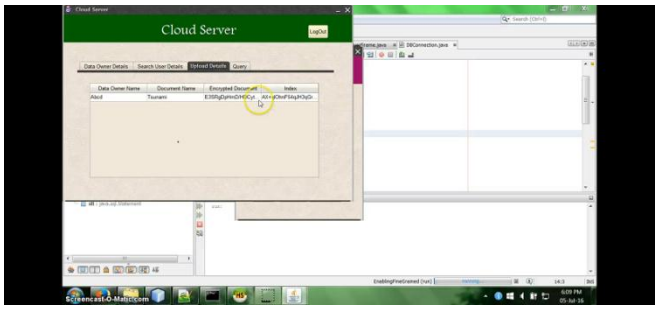
Login page

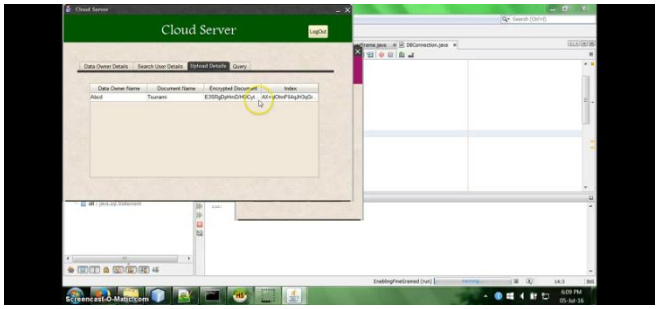


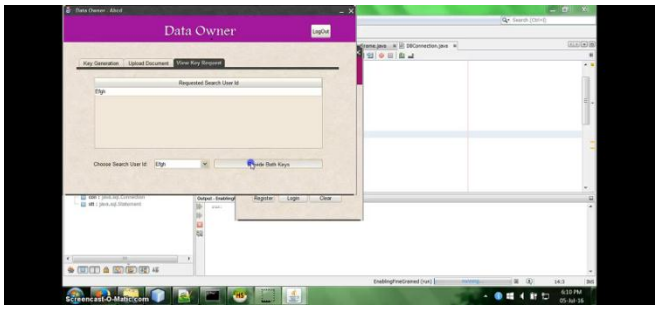
Data owner page



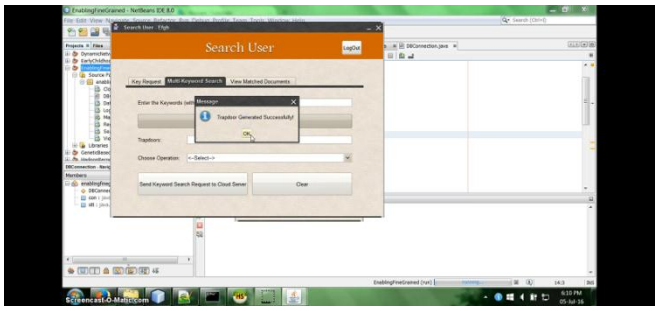
Cloud server



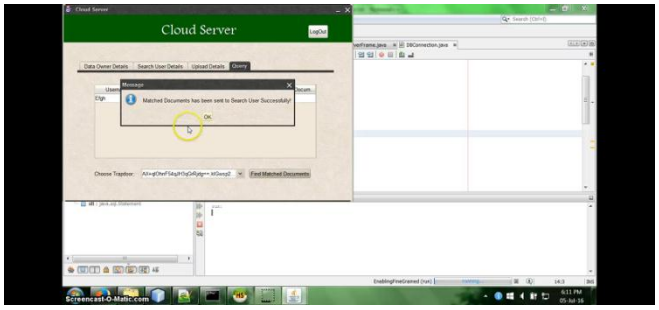


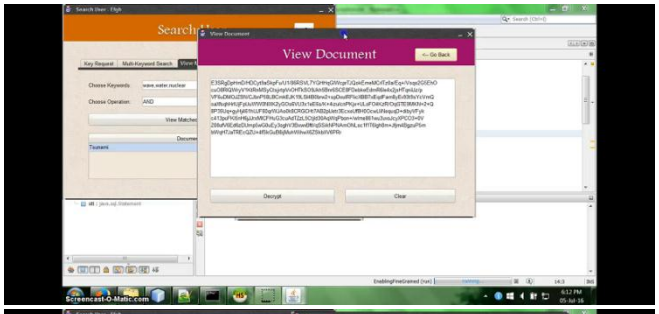


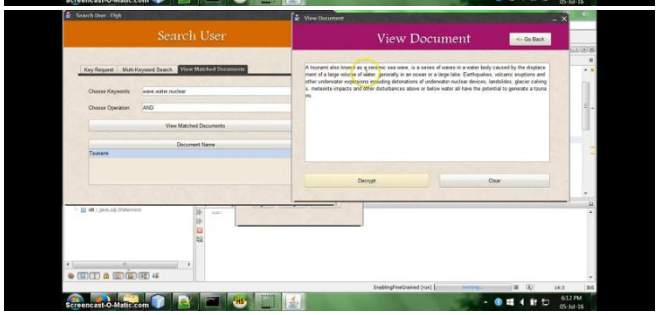
Search User page



View document page







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 fine-grained 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]. Feng Tian, Zhenqiang Wu, Xiaolin Gui,Jianbing Ni, ”Fine grained query authorization with integrity veritification over encrypted spatial data in cloud storage”, IEEE Transctions on Cloud Computing, 2020,DOI:10.1109/TCC.2020.3010915

[2]. 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.

[3]. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, “Lightweight fine-grained search over encrypted data in fog computing,” IEEE Transactions on Services Computing, 12(5), 2019, 772–785,.

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

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, “Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval,” IEEE Transactions on Vehicular Technology, 67(7), 2018, 6504–6517.

[11]. W. Zhang, Y. Lin, and Q. Gu, “Catch you if you misbehave: Ranked keyword search results verification in cloud computing,” IEEETransactions on Cloud Computing, 6(1), 2018, 74–86.

[12]. C. Guo, R. Zhuang, Y. Jie, K. Choo, and X. Tang, “Secure range search over encrypted uncertain iot outsourced data,” IEEE Internet of Things Journal, 6(2), 2018, 1520–1529.

[13]. Y. Wang, Q. Wu, B. Qin, W. Shi, R. Deng, and J. Hu, “Identity based data outsourcing with comprehensive auditing in clouds,” IEEE Transactions on Information Forensics and Security, 12(4), 2017, 940–952.

[14]. X. Yao, R. Zhang, Y. Zhang, and Y. Lin, “Verifiable social data outsourcing,” in Proc. of IEEE Conference on Computer Communications, Atlanta, USA, 2017, 1-9

[15]. Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from in distinguishability obfuscation," IEEE Transactions on Information Forensics and Security, 12(3), 2017, 676–688.

[16]. K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen, "An efficient and fine-grained big data access control scheme with privacy preserving policy," IEEE Internet of Things Journal, 4(2), 2017, 563–571.

[17]. J. Li, R. Ma, and H. Guan, "Tees: An efficient search scheme over encrypted data on mobile cloud," IEEE Transactions on CloudComputing, 5(1), 2017, 126–139.

[18]. H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, 10(5), 2017, 701–714.