ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Preserve Cloud Data Using Multi-Keyword Ranked Search over Encrypted Technique

Varshini R[1], Dr B G Geetha[2]

B. E Final Year, Department of Computer Science and Engineering, K. S. Rangasamy College of Technology, Tiruchengode, Namakkal, India[1]

Head of the Department, Department of Computer Science and Engineering, K. S. Rangasamy College of Technology, Tiruchengode, Namakkal, India[2]

ABSTRACT: The group of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics elect the efficient similarity measure of coordinate matching many matches possible relevance of knowledge documents. The search query to use inner product similarity to quantitatively evaluate such similarity measure first propose a basic idea for the MRSE supported a secure inner product computation give the significantly improved MRSE schemes to understand various stringent privacy requirements in two different threat models enhance search experience of the search service extend the two schemes to support more search semantics The analysis investigating privacy and efficiency guarantees of proposed schemes is given Experiments on the real-world data set indeed introduce low overhead on computation and communication.

I. INTRODUCTION

Cloud computing could even be a computing paradigm where an outsized pool of systems is connected privately or public networks, to provide dynamically scalable infrastructure for application data and file storage. With the arrival of this technology, the value of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing may be a practical approach to experience direct cost benefits and it's the potential to rework a knowledge center from a capital-intensive found out to a variable priced environment.

The idea of cloud computing is predicated on a really fundamental principal of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of grid computing distributed computing utility computing autonomic computing is to broaden horizons across organizational boundaries are used in the various of the system software are applied.

II. CLOUD COMPUTING MODELS

Cloud Providers offer services which will be grouped into three categories. Software as a Service (SaaS) during this model, an entire application is obtainable to the customer, as a service on demand. one instance of the service runs on the cloud & multiple end users are serviced. On the customer side there is no need for upfront investment in servers or software license for the provider the costs are lowered since just one application must be hosted & maintained. Today SaaS is obtainable by companies like Google, sales department Microsoft, Zoho, etc. The layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are

DOI: 10.15680/IJIRCCE.2020. 0803033

pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, etc.

III. PUBLIC AND PRIVATE CLOUDS

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

Externally hosted Private Cloud

This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources. Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

IV. EXISTING SYSTEM

Considering a cloud data hosting service involving three different entities, the data owner, the data user, and the cloud server. The data owner has a collection of data documents $\mathcal{F}$ to be outsourced to the cloud server in the encrypted form *C*. To enable the searching capability over *C* for effective data utilization, the data owner, before outsourcing, will first build an encrypted searchable index *I* from $\mathcal{F}$, and then outsource both the index *I* and the encrypted document collection *C* to the cloud server. To search the document collection for *t* given keywords, an authorized user acquires a corresponding trapdoor *T* through search control mechanisms, for example, broadcast encryption. Upon receiving *T* from a data user, the cloud server is responsible to search the index *I* and return the corresponding set of encrypted documents. To improve the document retrieval accuracy, the search result should be ranked by the cloud server according to some ranking criteria (e.g., coordinate matching, as will be introduced shortly). Moreover, to reduce the communication cost, the data user may send an optional number k along with the trapdoor *T* so that the cloud server only sends back *top-k* documents that are most relevant to the search query. Finally, the access control mechanism is employed to manage decryption capabilities given to users and the data collection can be updated in terms of inserting new documents, updating existing documents, and deleting existing documents.

Threat Model

The cloud server is considered as "honest-but-curious" in our model, which is consistent with related works on cloud security. Specifically, the cloud server acts in an "honest" fashion and correctly follows the designated protocol specification. However, it is "curious" to infer and analyze data (including index) in its storage and message flows received during the protocol so as to learn additional information. In this model, the cloud server is supposed to only know encrypted data set C and searchable index *I*, both of which are outsourced from the data owned this stronger model, the cloud server is supposed to possess more knowledge than what can be accessed in the known ciphertext model. Such information may include the correlation relationship of given search requests (trapdoors), as well as the data set related statistical information. As an instance of possible attacks in this case, the cloud server could use the known trapdoor information combined with document/keyword frequency to deduce/identify certain keywords in the query.

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.

V. PROPOSED SYSTEM

The challenging problem of privacy-preserving multi-keyword ranked keyword mapping and search over encrypted cloud data (MRSE) and establish a gaggle of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, the elect the efficient principle of coordinate matching proposes the matter of Secured Multi keyword search (SMS) over encrypted cloud data (ECD) and construct a gaggle of privacy policies for such a secure cloud data utilization system. From number of multi-keyword semantics and select the highly efficient rule of coordinate matching to identify the similarity between search query and data and for further matching use inner data correspondence to the quantitatively formalize principle for similarity measurement and first propose a basic Secured multi keyword ranked keyword mapping and search scheme using secure scalar product computation then improve it to satisfy different privacy requirements. The Ranked result provides top k retrieval results to propose an alert system which can generate alerts when un-authorized user tries to access the information from cloud the alert will generate within the sort of mail and message was first propose a basic MRSE scheme using secure scalar product computation significantly improve it to satisfy different privacy requirements in two levels of threat models.

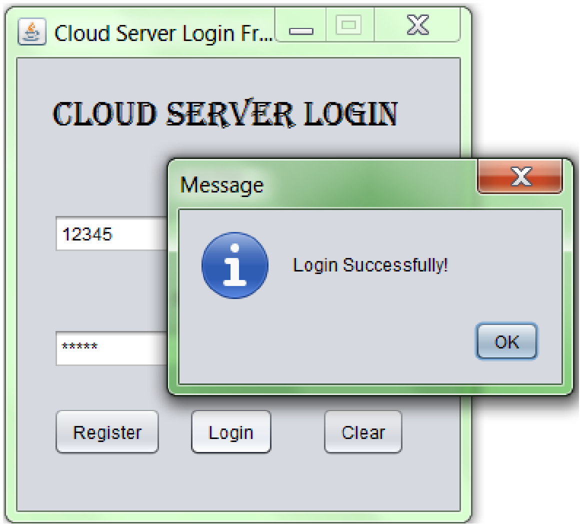
ADVANTAGES

Multi-keyword ranked ontology keyword mapping and search over encrypted cloud data (MRSE) Coordinate matching by scalar product similarity.
Secured Multi keyword ranked ontology keyword mapping and search to style search schemes which enable multi-keyword query and supply result similarity ranking for valuable data retrieval rather than returning undifferentiated results. Privacy to stop cloud server from learning additional information from dataset and index and to satisfy privacy requirements. Effectiveness with high performance functionality and privacy should be achieved with low communication and computation overhead of the Data privacy the data owner can resort to the normal symmetric key cryptography.

VI. MODULES

INDEX KEYWORD MAPPING

The ranked Index keyword mapping and look for operative use of outsourced cloud data of the model of our system that make a design for an instantaneously achieve security and performance assurances Multi keyword ranked keyword mapping and search to style search schemes which permit multi-keyword query and supply result similarity ranking for effective data retrieval, rather than returning undifferentiated results.



12345

*****

Message

Login Successfully!

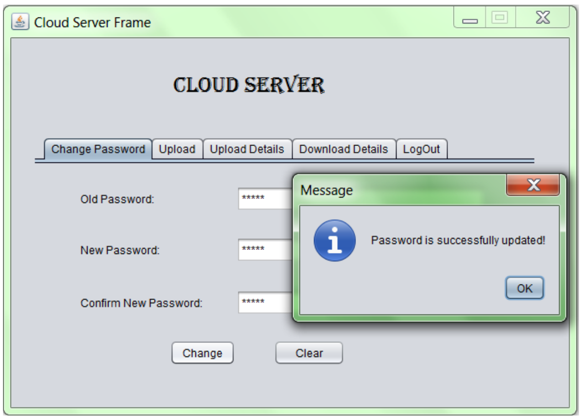
Privacy-Preserving to stop the cloud server from learning additional information from the dataset and the index and to satisfy privacy. Efficiency goals on functionality and privacy should be achieved with low communication and computation over head.

The document to quantify the relevance of that document and to the query users identify the dataset to be regained Boolean queries achieve well with the precise search necessity stated by the used is more elastic for users to spot an inventory of keywords indicating their concern and regain the foremost relevant documents with a order Data privacy the data owner can resort to the normal symmetric key cryptography to encrypt Index privacy the cloud server infers any association between keywords and encrypted documents from an various of thee index the searchable index should be built to stop and the cloud server from the acting quite association attack.

Keyword Privacy as users generally wish to possess their search from existence showing to others just like the cloud server the foremost vital concern is to cover what they're searching the keywords specified by the corresponding trapdoor the trapdoor is often generated during a cryptographic thanks to protect the query keywords.

Encrypt Module

The RSA Algorithm to convert the encrypted document to the Zip file from the activation code then activation code sends to the user for download.



Old Password: *****

New Password: *****

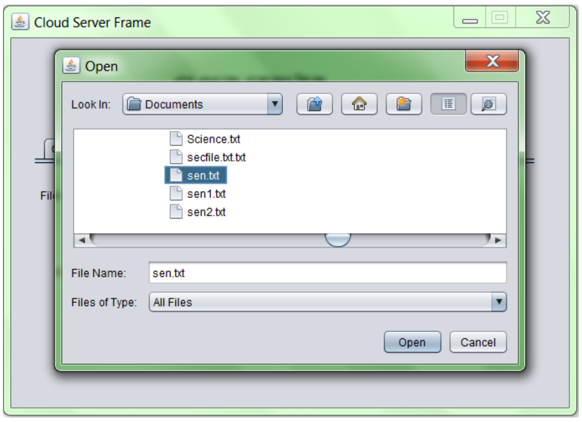
Confirm New Password: *****

Message

Password is successfully updated!

Client Module

This module is employed to assist the client to look the file using the multiple key words concept and the accurate result list supported the used query. The user goes to pick the specified file and register then user details and obtain activation code in mail from the email before enter the activation code now user can download the file

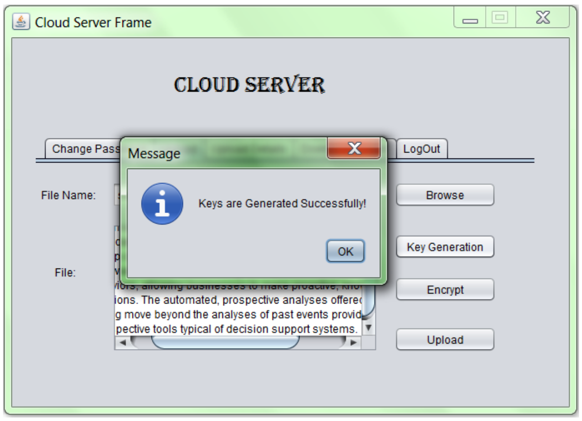


File Name: sen.txt

Files of Type: All Files

Multi-keyword mapping Module

This module is employed to assist the user to urge the accurate result supported the multiple keyword concepts. The users can enter the multiple words query the server goes to separate that question into one word after search that word enter our database display the matched glossary from the database and therefore the user gets the file from that list privacy breaches propose a basic SMS scheme using secure inner product computation which is ready-made from a secure k-nearest neighbor (kNN) technique then improve it step by step to realize various privacy requirements in two levels of threat models.



Keys are Generated Successfully!

tions, allowing businesses to make proactive, kno
ions. The automated, prospective analyses offere
g move beyond the analyses of past events provid
pective tools typical of decision support systems.

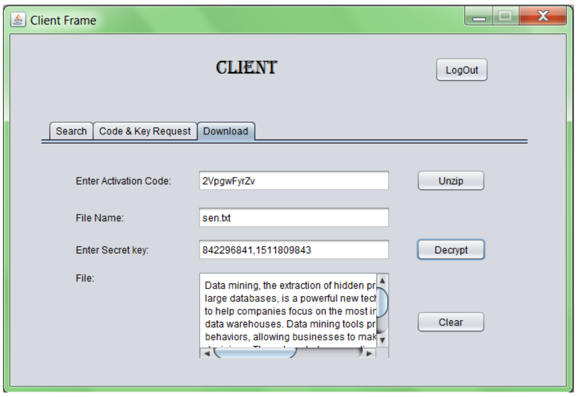
- Showing the problem of Secured Multi-keyword search over encrypted cloud data
- coordinate matching and inner product similarity.

Admin Module

This module is employed to assist the server to look at details and upload files with the safety. 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 consider the user downloading details and therefore the counting of file request details on flowchart.

File upload Module

This module is employed to assist the server to look at details and upload files with the safety Admin uses the log key to the login time Before the admin logout change the log key now admin can change the password after the login and consider the user downloading details of the counting of file request details on flowchart Then admin can upload the file after the formation of the conversion of the Zip file format When any User request for the then Ranking is completed on requested data using k-nearest neighbor algorithm are also using the Ranking matching‖ principle is used After ranking user gets the expected results of the query.



Enter Activation Code: 2VpgwFyrZv

File Name: sen.txt

Enter Secret key: 842296841,1511809843

File:

Data mining, the extraction of hidden pr
large databases, is a powerful new tech
to help companies focus on the most in
data warehouses. Data mining tools pr
behaviors, allowing businesses to mak

VII. CONCLUSION

Multi-keyword ranked search over encrypted cloud data and establish a spread of privacy requirements are used in various multi-keyword semantics elect the efficient measure of coordinate matching to effectively capture the relevance of outsourced documents to the query keywords and use scalar product to quantitatively evaluate such similarity measure For as the various of the search meeting the challenge of supporting multi-keyword semantic without privacy breaches of propose a basic idea of MRSE using secure inner product computation give two improved MRSE schemes to understand various stringent privacy requirements in two different threat models also are investigate some further enhancements of our ranked search mechanism including supporting more search semantics TF IDF and dynamic data operations. The analysis is using within the various investigating privacy and efficiency guarantees of proposed schemes is given for the new experiments on the real-world data set.

REFERENCES

1. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption," Proc. 29th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '10), 2010.
2. A. Singhal, "Modern Information Retrieval: A Brief Overview," IEEE Data Eng. Bull., vol. 24, no. 4, pp. 35-43, Mar. 2001.
3. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data," Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS '10), 2010.
4. C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467- 1479, Aug. 2012.
5. D. Boneh and B. Waters, "Conjunctive, Subset, and Range Queries on Encrypted Data," Proc. Fourth Conf. Theory Cryptography (TCC), pp. 535-554, 2007.
6. D. Boneh, E. Kushilevitz, R. Ostrovsky, and W.E.S. III, "Public Key Encryption That Allows PIR Queries," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '07), 2007.
7. D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2004.
8. D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.
9. E. Shen, E. Shi, and B. Waters, "Predicate Privacy in Encryption Systems," Proc. Sixth Theory of Cryptography Conf. Theory of Cryptography (TCC), 2009.
10. E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216. 2003.

11. I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.
12. J. Katz, A. Sahai, and B. Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products," Proc. 27th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2008.
13. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.
14. L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACMSIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50-55, 2009.
15. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous Ibe, and Extensions," J. Cryptology, vol. 21, no. 3, pp. 350- 391, 2008.
16. M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and Efficiently Searchable Encryption," Proc. 27th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '07), 2007.
17. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '10), pp. 383- 392, June 2011.
18. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, Apr, 2011.
19. N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.
20. P. Golle, J. Staddon, and B. Waters, "Secure Conjunctive Keyword Search over Encrypted Data," Proc. Applied Cryptography and Network Security, pp. 31-45, 2004.
21. R. Brinkman, "Searching in Encrypted Data," PhD thesis, Univ. Of Twente, 2007.
22. R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.
23. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan. 2010.
24. W.K. Wong, D.W. Cheung, B. Kao, and N. Mamoulis, "Secure kNN Computation on Encrypted Databases," Proc. 35th ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), pp. 139-152, 2009.
25. Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.