

EFFECTIVELY SECURED DUAL SERVER NUMERIC-RELATED SQL RANGE QUERIES IN CLOUD DATA STORES

Mohd Anamullah Shareef¹, Dr. Md Ateeq ur Rahman²

Research Scholar, Dept. of Computer Science & Engineering, SCET, Hyderabad¹

Professor, HOD, Dept. of Computer Science & Engineering, SCET, Hyderabad²

Abstract: - Cloud computing is one of the most used technologies these days due to the numerous benefits that it offers. It is very easy for small-scale enterprises and individuals to store their data on the cloud and operate from the cloud rather than investing in infrastructure, software, and hardware. The cloud offers flexible, cost-effective services and applications for any type of user. The cloud environment is scalable from the storage requirements of an individual to a large-scale enterprise. Hence it can be used by anyone and everyone is charged as per the usage of the cloud resources. One can maintain their organizational data in the databases over the cloud. Some schemes to secure the database content on the cloud are in place but they do not offer complete privacy protection and data confidentiality and there is still some scope for data leakage from the cloud and it was a serious security threat. The main reason for the privacy issues of the cloud is that the data is not in the control of the data owner and he must completely rely on the services provided by the cloud administrator. The existing schemes do not provide sufficient privacy preservation and can pose security threats when the SQL queries run on the cloud databases. There is a scope for pattern identification of access with the increasing number of queries that hit the cloud database. In this project, we come up with a novel mechanism to secure the data on the database using a Two-cloud approach with a set of connection procedures to provide confidentiality and prevent the data leakage of numeric queries that hit the cloud database. security analysis and simulation of the above-mentioned technique has yielded better results when compared to its existing counterparts.

Keywords: - *privacy preserving, range query, database, cloud computing*

I INTRODUCTION

The cloud industry is growing at a rapid rate due to the various benefits that it offers to its users like low maintenance costs, zero investment in infrastructure, pay as per usage, resource scalability, etc. Hence many and many users and enterprises are showing interest in outsourcing their data to the cloud.[1] However, having sensitive information on the cloud is not recommendable as the data is not in the control of the data owner, and the cloud service provider might be honest but curious do to which there is a scope for privacy loss and data leakage [2]. Hence it is necessary to encrypt the data before subcontracting the data to the cloud-like database system. A common situation of outsourcing a database to the cloud is shown in the figure below [3]:

A cloud consumer such as an IT company would want to maintain a database on the cloud for easy access and collaboration and the database could contain sensitive information such as transaction information, financial information, account information, [4] etc. and the cloud service provider may be honest but curious to know the information that's stored in the database and can use his privileges to access the database content [5].

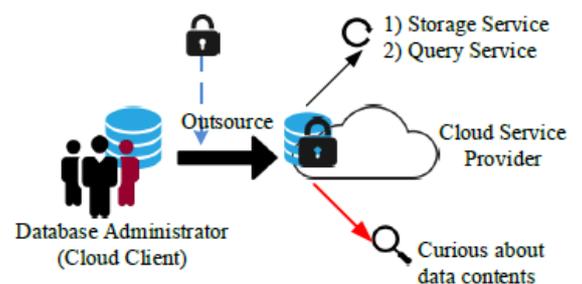


Fig. 1. Outsourced database, service and the privacy risk

He might also gain access to this information and sell it to his competitors which is a big operational risk for the IT company [6]. We have a twofold responsibility to protect the database is on the cloud [7].

1. The data in the database should not be revealed to the cloud server.
2. The queries that run on the database reveal information about the data that is present on the cloud database. Hence the queries should be protected from the cloud service provider.

Some of the existing systems that offer a solution to the above-mentioned problems are in place like “crypt DB” but privacy loss has not been eliminated thoroughly [8].

Hence, we come up with a two cloud approach or architecture where the data is encrypted and stored in one cloud [9] While the keys for decrypting the data are stored on another cloud. To protect the query patterns, they are split up into two parts and stored on each cloud [10]. We assume that the two clouds do not interact with each other and hence there is no chance of any collusive behavior from the cloud administrators. We also come up with some connection procedures on how to access both the clouds and query the encrypted cloud database. The performance of the proposed system is satisfactory mutation and can be scaled up for more complex database queries to be implemented in real-time systems.

II LITERATURE SURVEY

“A survey on multi-keyword ranked search manipulations over encrypted cloud data”

Based on the present-day advancements in cloud computing there is a necessity to load a variety of data owner's information onto the public cloud servers. Show the data stored by data owner may contain their private sensitive information as well as their job-related data which needs to get privacy protected with the high-security standards. Considering this data may get outsourced to some other organizations so we may need to emphasize increasing the trustability and effectiveness in utilization of services contributed by the corresponding server. Primary data owner's sensitive data needs to get privacy protected by converting its form to cipher-text form by using an appropriate encryption mechanism after that it may need to get redirected to the corresponding server. In certain circumstances, this data will be in huge volumes and data user may need to search for the desired data using appropriate multi keywords based search so that the desired data will get retrieved into the Data user end most effectively and efficiently.

“Efficient and Expressive Keyword Search over Encrypted Medical Data in Hybrid Cloud”

These days in cloud computing domains client-based services can be effectively and efficiently delivered in the aspect of data than as a service. What if we have a closer look at the information that resides in the server sometimes carries some potential content so that privacy preservation becomes a crucial factor that has to be considered. In this proposed framework, the keyword-oriented search process is driven effectively on private sensitive encrypted data and enables authorized users to utilize it. Along with that data confidentiality over access control methodologies, the entire process is been monitored in a fine-grained approach show that the entire approach will increase the privacy preservation standards effectively.

“Practical Techniques for Searches on Encrypted Data”

In the environments of data storage service or mailing service server the data that got stored needs to get encrypted so that we can achieve privacy-preserving towards the desired store data, when we much emphasize on security sometimes there is a chance to lose or sacrifice operational functions performance. About that in certain circumstances when a client attempts to retrieve the serviced documents which carry certain verbal words that need to get evaluated the process of handling search mechanism empower the data stored in the server so that the processing of the query over the desired data needs to be driven effectively and efficiently without violating the standards of security and emphasize on increasing the data confidentiality at most. As we attempted to increase the security standards we need to adapt cryptographic and encryption methodologies that converts the plain text data into the cipher-text form so that the converted data will be stored in the server and even it should effectively facilitate the retrieval process so that the searching mechanism will be driven over the encrypted data that got stored in the data server. When the methodologies of encryption is been isolated from the un-authorized server so that any unauthorized or unreliable server calls cannot handle the searching process with a secure keyword not letting the server know about that so that user-level authorization is been driven at the data server and encryption and decryption are been carried out within the authorized secure confined users only.

III SYSTEM ANALYSIS

Existing System:

In the existing cloud environments where a user wants to outsource his database, it is not secure as the data in the cloud is not in the purview of the data owner. the data in the cloud database could be encrypted but it is difficult to run queries and retrieve it with the existing mechanisms. Moreover, the queries that run on the cloud database are exposed to the cloud service administrator and they reveal the underlying patterns of the data in the database. The cloud service administrator can misuse the data, and this poses a serious operational threat. Hence we have to come up with a solution to protect the data and the queries that are associated with the cloud database.

Drawbacks:

1. The existing system is not secure
2. It poses operational threats

Proposed System:

We come up with a two cloud approach or architecture where the data is encrypted and stored in one cloud While the keys for decrypting the data are stored on another cloud. To protect the query patterns, they are split up into two parts and stored on each cloud. We assume that the two clouds do not interact with each other and hence there is no chance of any collusive

behavior from the cloud administrators. We also come up with some connection procedures on how to access both the clouds and query the encrypted cloud database.

Benefits:

1. Security of data is achieved
2. Security of queries is achieved

IV IMPLEMENTATION

The total project is been modular is in the following subsections to achieve the functional requirements of the desired targets.

1. Cloud server:

In this cloud server module facilities like cloud client organization comer data user authorization come list of all uploaded files along with the registered patient details and all file transactions are been listed effectively.

2. Data administrator:

In this client module, account registration and authorisation from the server for the approval of the registered accounts, authentication check in order to to avail the services from the server, searchable range queries, searches in geometric approach, search is over special data and calculation of Geographic distances carbon facilitated effectively.

3. Dual server:

In this year's server module all file download requests and their corresponding information it is been administered effectively.

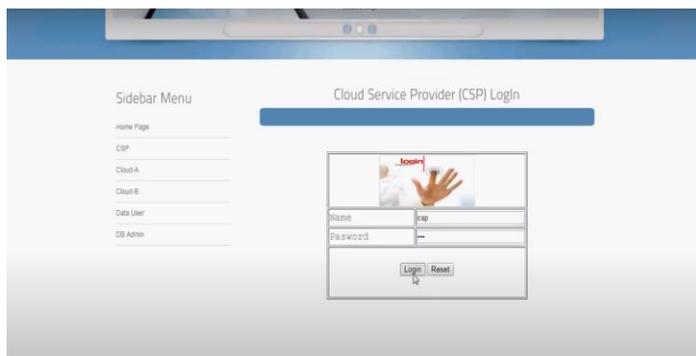
4. Data user:

This data user module new data user can be registered, their profile view, multi-keyword search process, request initiation for a specific file to the corresponding cloud and view response related to that and list of all permitted files is displayed effectively.

V PROJECT EXECUTION AND TESTING

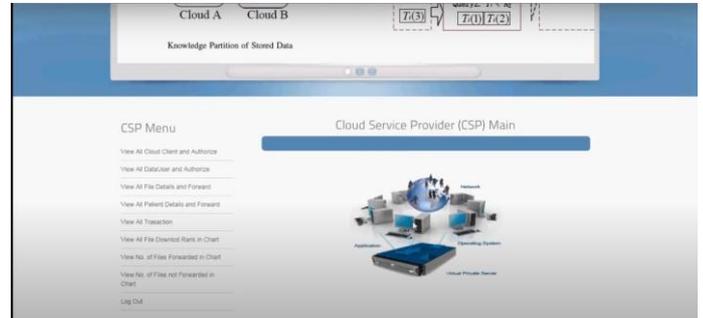
Cloud Service Provider login page:

Credentials of cloud server service provider are entered in this login page so that if the evolution process succeeds to control will get directed to cloud Service Provider home page for failure will lead to a warning page.



Cloud Service Provider home page:

This is a welcome page after successful entry of Cloud Service Provider credentials at its login page. Clear all CSP functional requirements are listed.



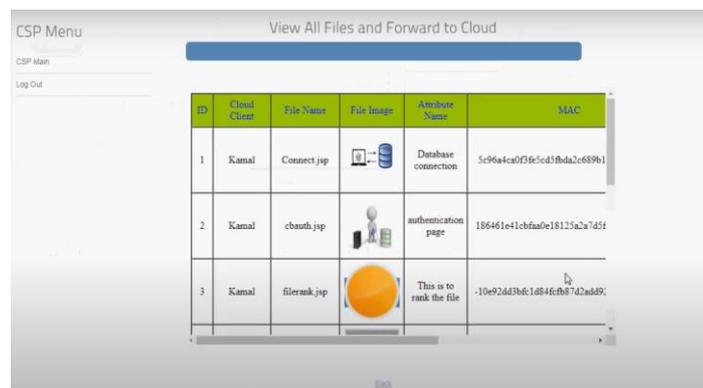
View all cloud client and other is the page:

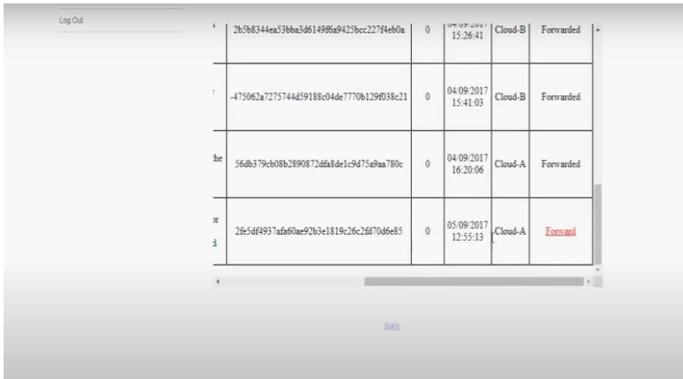
On this page, all cloud data clients can be authorized by CSP, so that their corresponding services can be availed.



View all files and forward to cloud page:

In this View, all files and forward to the cloud page all uploaded files are been listed and their corresponding forward operation status is reported.

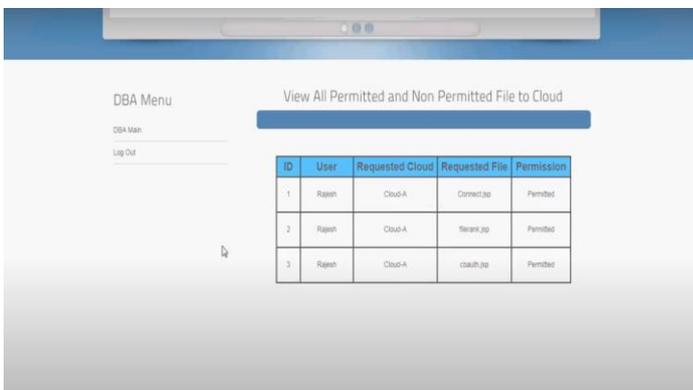




ID	User	Requested Cloud	Requested File	Permission
1	Rajesh	Cloud-A	connect.jsp	Permitted
2	Rajesh	Cloud-A	server.jsp	Permitted
3	Rajesh	Cloud-A	cloud.jsp	Permitted

File permission page:

In this file permission page, all the users with their corresponding requested file to a specific server is granted or not will be acknowledged here.



Search Data and Send Download Request

Query Type: LIMIT | Table Name: clouds_files | Cloud: Cloud-A | Enter Query: 2

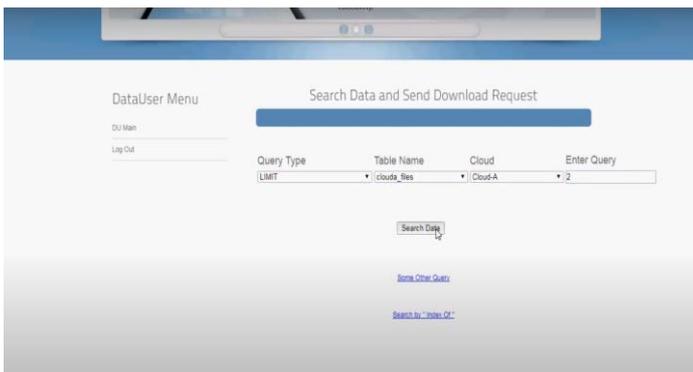
[Search Data](#)

[Some Other Query](#)

[Search by "Index Of"](#)

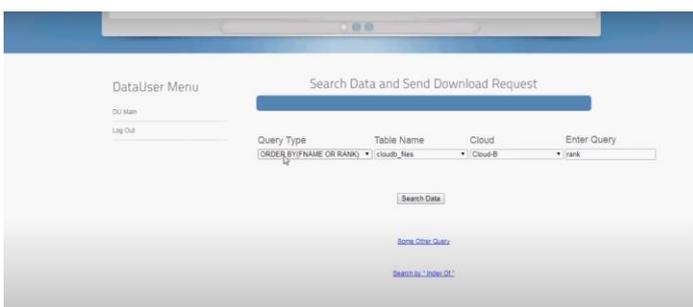
Query search page:

In this query, search page attributes like query type table name, specific cloud, and query are been taken as inputs to filter or retrieve the specific data is being entered here.



View Data and Send Download Request

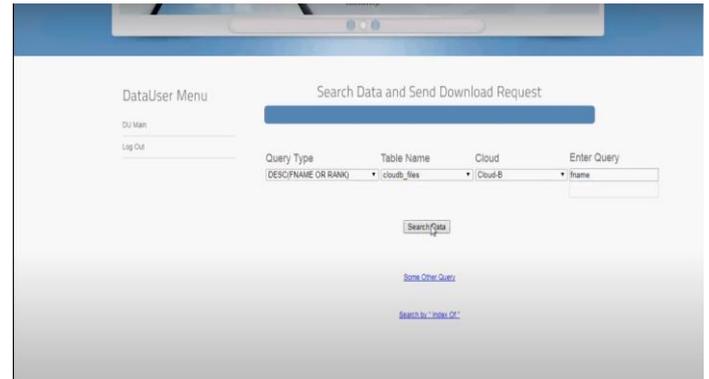
File Image	Attribute Name	MAC	Rank	Date	Download Request
	Database connection	5c96a4ca0f565c45f8da7c68961e488490647	2	04-09-2017 15:08:57	Send or View
	authentication page	186461e41c6fa0c18125a7a45f1353469545f	1	04-09-2017 15:13:23	Send or View



DBA Menu

View All Permitted and Non Permitted File to Cloud

ID	User	Requested Cloud	Requested File	Permission
1	Rajesh	Cloud-A	connect.jsp	Permitted
2	Rajesh	Cloud-A	server.jsp	Permitted
3	Rajesh	Cloud-A	cloud.jsp	Permitted



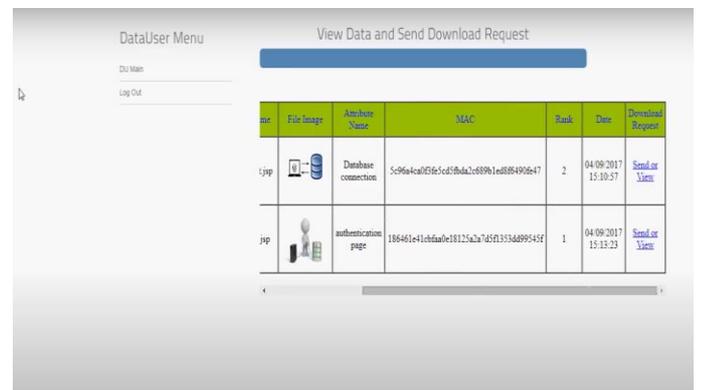
DBA Menu

View All Permitted and Non Permitted File to Cloud

ID	User	Requested Cloud	Requested File	Permission
1	Rajesh	Cloud-A	connect.jsp	Permitted
2	Rajesh	Cloud-A	server.jsp	Permitted
3	Rajesh	Cloud-A	cloud.jsp	Permitted

Query result page:

In this query result page, multi-keyword process results are listed in the form of a table is displayed as well the download request is also facilitated here.



DBA Menu

View All Permitted and Non Permitted File to Cloud

ID	User	Requested Cloud	Requested File	Permission
1	Rajesh	Cloud-A	connect.jsp	Permitted
2	Rajesh	Cloud-A	server.jsp	Permitted
3	Rajesh	Cloud-A	cloud.jsp	Permitted

VI CONCLUSION

In this project, we have recommended a two-cloud approach along with a set of connection procedures to secure the database on the cloud and prevent any numeric queries from exposing the underlying patterns to the cloud administrators. We observed that using range queries this static data is protected and is also scalable for larger systems. The simulation of the existing system has provided good security and the results are satisfactory. Hence, we can successfully achieve data confidentiality while accessing the database is on the cloud and it proves that the proposed access mechanism is efficient and practical enough to apply it to larger systems.

Future Enhancement:

We would like to further improve this system to be scalable and perform faster while running queries on encrypted databases. We would also like to extend our new mechanism to use more complex and aggregated queries that utilize Sum and average etc.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

- [2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.
- [3] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 459–470, 2014.
- [4] J. W. Rittinghouse and J. F. Ransome, *Cloud computing: implementation, management, and security*. CRC press, 2016.
- [5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.
- [6] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587–1611, 2013.
- [7] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in *Proceedings of the 23rd ACM Symposium on Operating Systems Principles*. ACM, 2011, pp. 85–100.
- [8] C. Curino, E. P. Jones, R. A. Popa, N. Malviya et al., "Relational cloud: A database-as-a-service for the cloud," 2011, <http://hdl.handle.net/1721.1/62241>.
- [9] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, "Hosting services on an untrusted cloud," in *Advances in Cryptology-EUROCRYPT 2015*. Springer, 2015, pp. 404–436.
- [10] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 3184–3195, 2016.