SECURE CLOUD STORAGE USING A ROBUST ENCRYPTION SCHEME

Huidrom Bikram Singh

Dept. of M.C.A
Dr. Ambedkar Institute of Technology
Bangalore, India

Shobha Rani. B.R

Dept. of M.C.A
Dr. Ambedkar Institute of Technology
Bangalore, India

Abstract

Cloud storage paradigm has become one of the most important and useful technology in the present trends. Cloud storage focuses on improving the effectiveness of data storage and access from the cloud. Cloud resources are not only meant to share by multiple users, it is also usually used for dynamically relocating the data as per demand. In cloud many heterogeneous devices like laptop, smart-phone, and tablet are connected

using again diverse network like LAN, WAN, 3G/4G wireless network etc. Because of this diversity of technology and unsecure network unfortunately make cloud storage suffer lack of data confidentiality. To make sure the data are confidential we encrypt the data, this encryption generates problem to query the desire data among the encrypted data, which result in fetching unwanted data or redundant data. To overcome the problems we propose a system which encrypts the data in a very robust way so that it will work fine in dynamic SQL environment. This system directly connect data owner with user who seeks the data so that data can be access only with the consent of the data owner. Also the end user are directly connect with the administrator which provide a security key to the user after validating the information provided by the user which reduces the chances of having fake user. The propose system also enable the data owner to set price for the data which he/she uploaded. The data owner can also view the performance of file which he/she uploaded.

Keywords: Encryption Scheme,Metadata, Encrypted database management, Cost model

I. Introduction

The “Secure cloud database storage with a robust encryption scheme” is a internet base application which enable us to store data on cloud database and access securely by other users who wants the data. This cloud database storage enables us to share the resources to multiple remote users to any part of the world instantly.

This application is a very simple and user friendly applications which can be easily understand and use by the users of it. This system mostly focuses on the data confidentiality of user and accesses those data only with the consent of owner. It provides extreme level of data confidentiality by using a encryption scheme which is so robust that it will work definitely well in the dynamic environment. Upon with encryption this system will allow access to the owner’s data only with the consent of the owner, he/she will provide a secure master key to the user who want the particular data after that only a user can download a file. So chances of loosing data or misuse are really less. If in case any data has been lost then there is back up system from which you can retain your data back.

It also reduces the cost and maintenance charges instead of keeping our own database which would be far more expensive. We can scale up or scale down the uses of cloud database according to our need. This application is almost similar to electric bill payment, were we are required to pay according to what we used. The cost of using cloud resources are so clearly specified according to the period of usage so that the tenant or client can estimate how much it will cost to use for some period of time. Since the pricing is so clear the client of this system

II. Literature Survey

The cloud computing is one of the most successfully converging as very important paradigm where we store data or execute program as the server for company program without maintaining the resources required personally or in company, but this positive trend is getting some limitation. Some of the issues usually face in cloud storage were discussed in the survey. In [1] explains that ,data confidentiality is the main issue in the cloud storage, user data can be access and misuse by unwanted users. To safeguard data they used to encrypt, but this encryption causes difficulty to track the actual file which they want from cloud and causes to get irrelevant or redundant file. Encryption schemes usually allow the execution of SQL query but mostly suffer

from performance or they need the choice of which encryption scheme should be used for each column and SQL Queries. Service charges of using cloud resources are unclear often.In [2] it is discussed that, in the cloud mode physical security is lost because of sharing computing resources with many other people. No users have knowledge or control of where the resources run. If user want to shift data from one cloud to another, it may be incompatible due to service provide by each vendor may be different. In [3],explains that Guaranteeing the integrity of the data (storing, retrieval, and recovery) truly implies that it changes just in light of approved transactions. A regular standard to guarantee data integrity does not yet exist. Availability of the cloud cannot be always sure; the system may break down because of any issue.

III. PROPOSED SYSTEM

The proposed system overcomes the issues of what we have found in the existing system. The issues overcome are, it guarantees the best level of data confidentiality for any databases workload, even when there is a change in the set of SQL queries dynamically in the heterogeneous environment of device and various network connections. The proposed system gives the clear precise price of cloud services we used. This system is very compatible that is we can transfer data from one cloud to another which uses different vendor equipment. Data owner control master key of the data so without his permission data cannot be accessed. Data owner can view the performance of the data which he/she uploaded.

A. Architecture

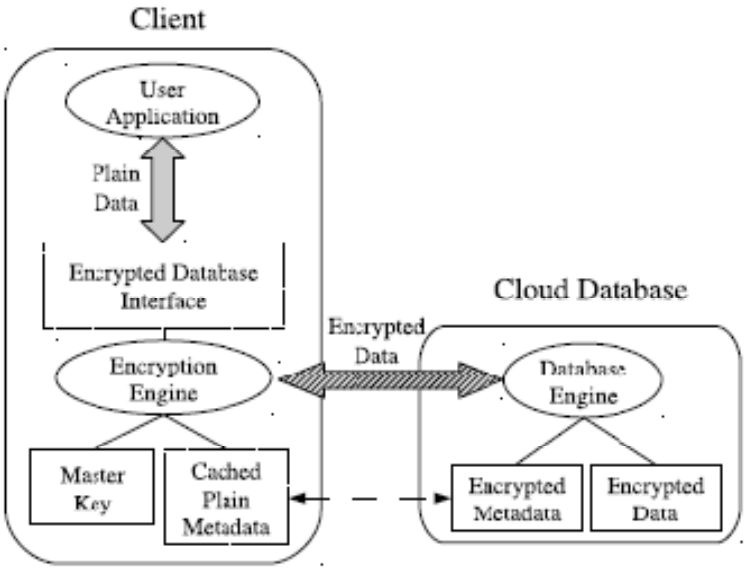

Figure II. Architecture

From the figure shown above explains the architecture of cloud databases.

The client uses this application and put the plain data on the Encrypted Database interface. This encrypted database interface will link to the data encryption engine where data is going to encrypt and generate a master key. The encrypted data and the encrypted metadata will store in the cloud database. The legitimate client can download the file by using this secure master key.

B. Encryption Schemes: We have to consider the SQL aware encryption algorithms that can guarantee data confidentiality and execute sql operation by concurrent users in the encrypted data.

The following encryption schemes are in use:

- Random (Rand)*:* This is the most secure encryption scheme then all we used here because it does not reveal the data at any point. But this algorithm does not support any SQL operation.
- *Deterministic (Det):*This scheme encrypt data in a deterministic way, so that it can maintain the equality of data is preserved. This scheme support the equality operator of SQL.
- *Order preserving encryption (Ope):*This scheme preserve a numerical value in the encrypted data as in the order of original data. This scheme support the comparison operators: =,<,<=,>,>=.
- *Homomorphic Sum (Sum):*Here homomorphic means with respect to sum operation, in this scheme the multiplication of the encrypted integers should be equal to the sum of original data integer. This encryption support sum operator of Sql query.
- *Search (search):*This scheme support quality check on the string of any length. This scheme support "LIKE" operator to search any string or substrings.

- *Plain:*It does not actually encrypt the data this scheme is useful only when we want to make all Sql query work.

  We make use of all these encryptions scheme to support all Sql query operators. We place each encryption technique in each layer so if one layer does not support the operator it will check the other consecutive layers.

C. Meta Data

This is the extra information that help legitimate client who knows master key to run SQL queries over the encrypted data, this metadata help to retrieve the exact data, which we want and also allows executing concurrent SQL query. The metadata are store in a table called “metadata table” which are correspond to the “plain table”.

D. Encrypted database management

- *Database Creation:* When a new database table has to be created a master key for that table has to be set by the owner’s, which is given to the legitimate client. On each new table creation a new row into the metadata table is inserted i.e. ‘name’, ‘data type’ and ‘confidential parameter’.
- *SQL commands execution* : When a users want to execute Sql command on the cloud, the encryption engine analyst the sql query to identify table, column and operator involve (example ==, <, >). The customer issues a solicitation for the table metadata for each included table, and decrypts the metadata with the master key. At that point, the customer figures out if the real layers of the onions connected with the included columns uphold the SQL operators.
- *Adaptive layer removal:* When sql command has been issues the encryption engine will analyst the query for the operator that involve in the query. If the outer layer of the does not support the operator then the outer layer should be remove to check whether inner layer does support the operator like wise the layers will be remove until we get a compatible layer.

E. Cost model:

The costs of cloud database storage service are base on the function of following parameters:

Cost=f (time, price, usage)

Where,

- *Time:* It is the time period for which the tenant require the service.
- *Price:* This is the price of cloud resources provider for using there resources and service.
- *Usage:* This is the total amount of usage of cloud resources.

IV. IMPLEMENTATION

A simple GUI is designed to implement the above methodology which is shown in following figures.This application is developed using Java and J2EE on Eclipse with MySQL as Database at the backend.

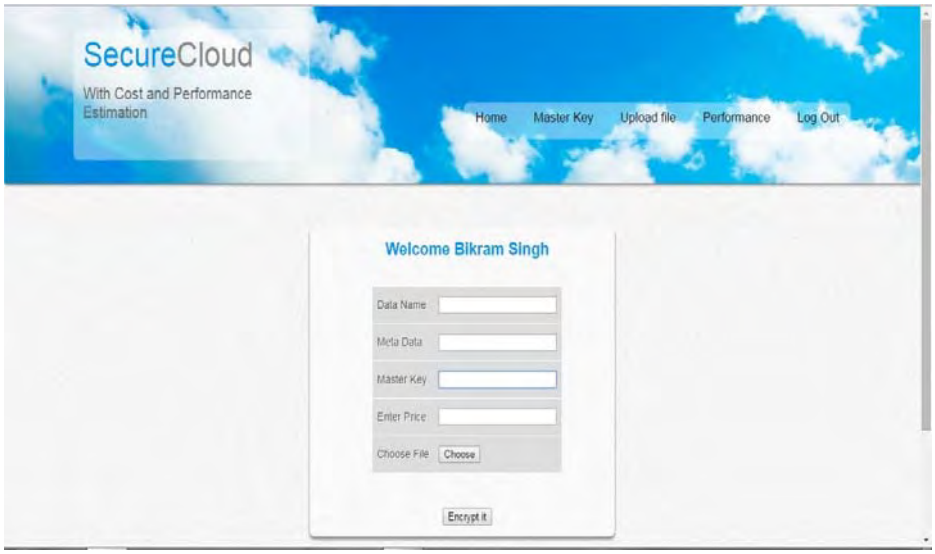

Figure 1.Upload

Figure 2. Encrypted Data

Fig 1.shows the brief encrypted form of user data which users is about to upload in the cloud database, and Fig 2 shows the page where data owners name the details of the file which he/she is about to upload in the cloud database.

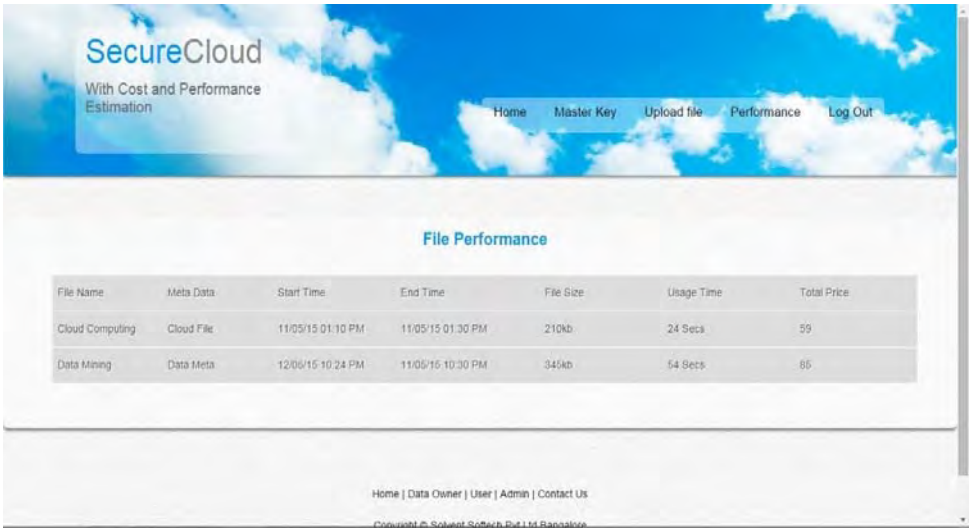

Figure 3. View File

Figure 4. File Performance

Fig.3 displays the all the files with its details, which are uploaded by a particular data owner, and Fig 4 shows the performance of the file uploaded by a particular data owner. The chart shows the file name and the level of usage by other users. The highest chart means the highest uses of the file and lowest chart means the lease uses of the file.

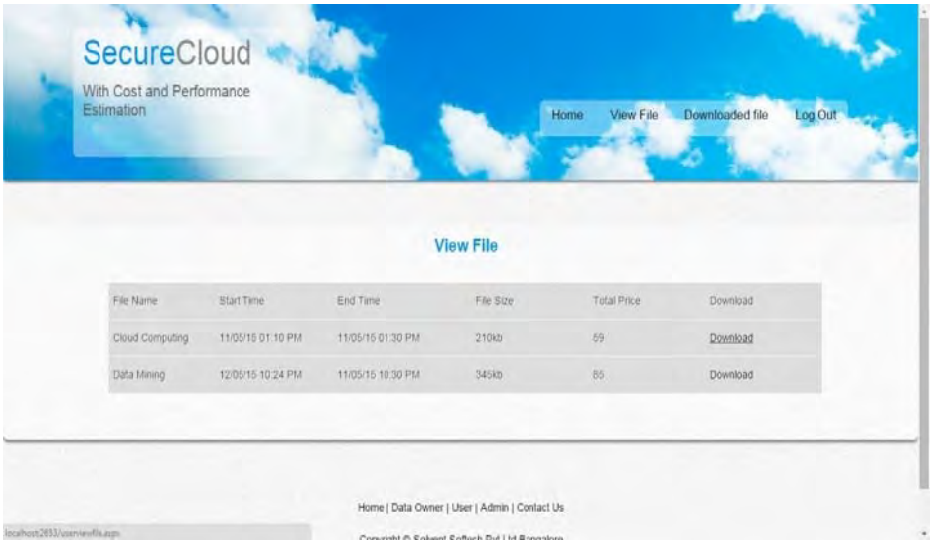

Figure 5. View File by End Users to Download

The legitimate end users can view the file which are on the cloud database after they successfully login into the system. If the end users want any file to download then he/she can click on the download link, which will sent a request to the data owner for master key. If data owner thinks you are a person to trust then he/she will provide the master key.

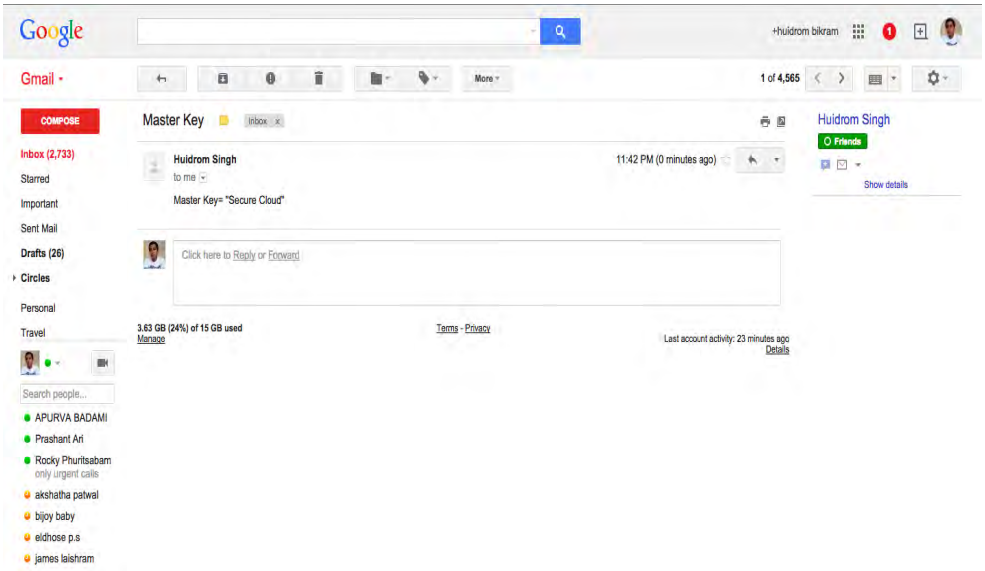

Figure 6. Master key

Above figure showss that when an end user want a certain file to download, they will request the file owner to provide the master key. If the owner wants him/her to access the file then owner will provide master key.

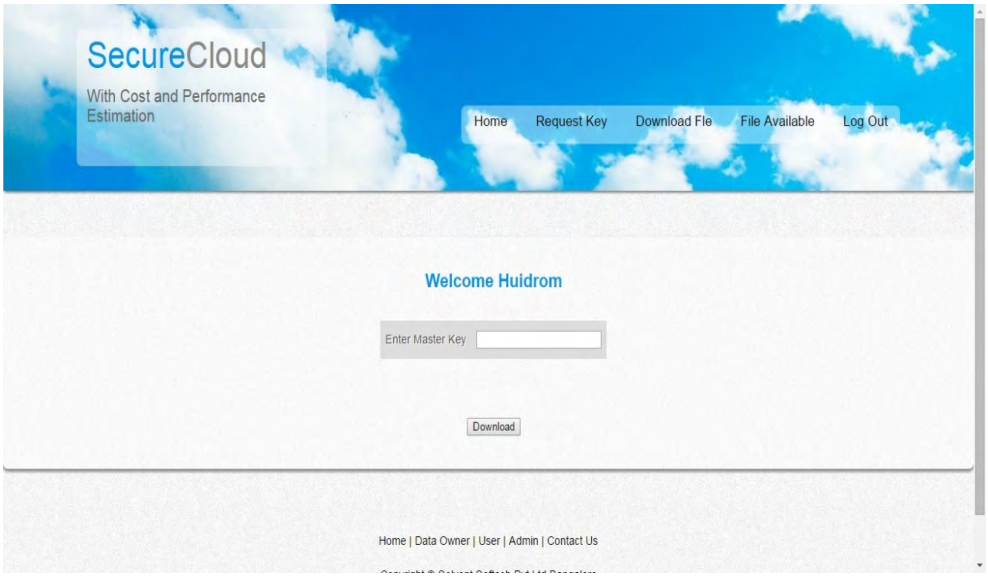

Figure 7. Enter Master Key

Above figure now shows that end user will click on the file which he/she want to download, and it will redirect to this page where he/she need to enter the master key to download the file.

V. CONCLUSION

With the implementation of this application tenants of the system can use the database in the cloud without consideration of data confidentiality. This system is very much suitable for public cloud storage where there is lack of security. It permit user to download a file only when the data owner pass the master key to download the file so chances of misuse is really less. With proper specification of actual cost of cloud service uses there is a no way to fraud on users of this system. Since this system provides the above stated benefit and its user-friendly interface we can say that it will obviously satisfy the users.

REFERENCES

[1] Ferretti, L.; Pierazzi, F.; Colajanni, M.; Marchetti, M., "Performance and Cost Evaluation of an Adaptive Encryption Architecture for Cloud Databases," Cloud Computing, IEEE Transactions on , vol.2, no.2, pp.143,155, April-June 2014 doi: 10.1109/TCC.2014.2314644J.

[2] Wayne A. Jansen, NIST , "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences – 2011

[3] Mohammad Sajid,Zahid RazaZahid Raza,"Cloud Computing: Issues and Challenges", International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV

[4] Rahumed, Arthur, et al. "A secure cloud backup system with assured deletion and version control." Parallel Processing Workshops (ICPPW), 2011 40th International Conference on. IEEE, 2011.

[5] Carroll, Mariana, Alta Van Der Merwe, and Paula Kotze. "Secure cloud computing: Benefits, risks and controls." Information Security South Africa (ISSA), 2011. IEEE, 2011.

[6] Joshi, Mahima, and Yudhveer Singh Moudgil. "Secure cloud storage."International Journal of Computer Science & Communication Networks 1.2 (2011): 171-175.

[7] Lin, Hsiao-Ying, and Wen-Guey Tzeng. "A secure erasure code-based cloud storage system with secure data forwarding." Parallel and Distributed Systems, IEEE Transactions on 23.6 (2012): 995-1003.

[8] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." Computers, IEEE Transactions on 62.2 (2013): 362-375.

[9] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[10] Kalpana, Parsi, and Sudha Singaraju. "Data security in cloud computing using RSA algorithm." IJRCCT 1.4 (2012): 143-146.