International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Accessing the Encrypted Cloud Data in a Simultaneous, Independent and Role-Based Fashion

Sharvari A. Pawar [1], Suresh B. Rathod[2]

[1] Department of Computer Engineering, Sinhgad Academy of Engineering, Pune University, Pune, Maharashtra, India

Abstract: ***In today's tech-savvy globalized world where ample data is available over a single click; its storage is a concern. A solution to this is the use of cloud where large amount of data can be stored. The feasibility and usefulness has made cloud computing a popular and rapidly growing field. But placing vital and confidential data outside the premises of an organization and in hands of cloud providers should come with guarantee that our data should be secure and available at any point of time. Many cyber threats are observed in cloud, due to lack of security awareness .To overcome these cyber trials in cloud, we have proposed an architecture, in which data is encrypted and then stored. There are many data storage techniques available, but we are trying to combine cloud database service along with data security and also can perform independent and concurrent operations on encrypted data. The client can perform certain basic SQL operations on the database in cloud. Apart from independence and concurrent access to this encrypted data, we also provide role based access to this data i.e data access will differ from person to person in an organization according to its designation.***

Keywords: Cloud computing, Cloud Security, Confidentiality, RBA.

1. Introduction

A new Dawn in the field of computing, cloud computing fast emerging as a storage solution. Cloud computing provides us with infrastructure, computing power and with some commercial apps which are used for CRM, SCM etc. Cloud provides us these resources as a Service so there is no any necessity of buying these resources and investing bulk amount unnecessarily. The user just needs to pay for the services he wants to use or have used. There are three different types of services in cloud such as, IaaS, SaaS and PaaS.

1.1. Cloud Services

1.1.1. Infrastructure-as-a-Service

One of the models of service delivery, where the entire infrastructure required in computing such as severs, network related equipment, software etc is provided as a service when demanded by the user. User needs to pay for the resources [3].

1.1.2. Software-as-a-Service

This model enables software that is built by the cloud provider in cloud, to be delivered over the network to the users who demand it. This model eliminates the overhead of risk of licensing, most compatible version etc. It is most common delivery model for certain common business apps such as CRM, SCM, and CM etc. Google Apps, salesforce.com are certain SaaS provider [4].

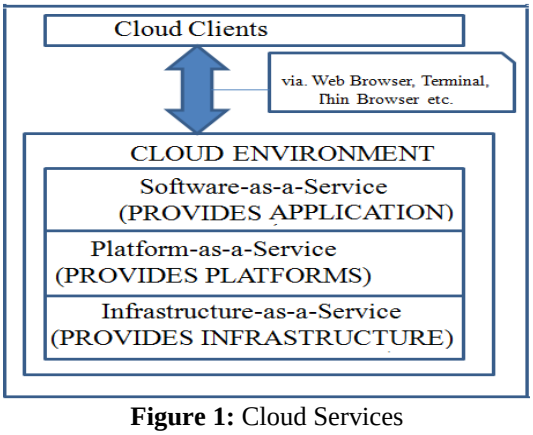

Figure 1: Cloud Services

1.1.3. Platform-as-a-Service

This model provides computation platforms for the user. Mostly developers are users of this service. The developer needs to just concentrate on coding and the logic; code is then deployed on the cloud PaaS service. The cloud then manages everything from storage to computation. Google App Engine is one of the most famous PaaS provider [5].

1.2. Cloud Types

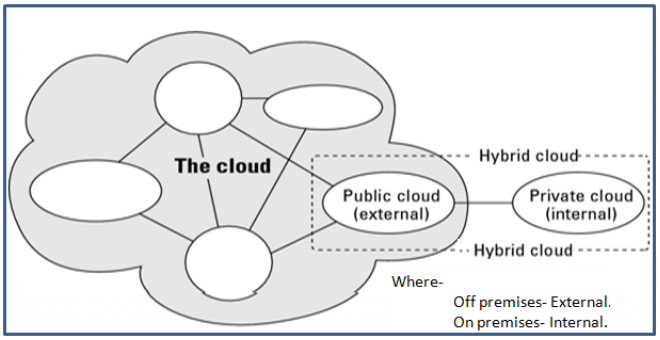

Figure 2: Cloud Types

1.2.1. Public Cloud

Public cloud is most basic cloud computing model, in which all the resources of the cloud are publically available to the users over internet. It is less secure than the other cloud models, because all the data is directly placed in the cloud.

1.2.2. Private Cloud

Due to security and confidential problems in public cloud, private cloud came into picture. Private cloud is set within an organization i.e. resources can be used only by that particular organization.

1.2.3. Hybrid Cloud

It is combination of public and private cloud. An organization can have a private cloud in a public cloud, is a best example of hybrid cloud.

1.2.4. Community Cloud

The group of organization of same community or group owns a common cloud. This cloud is maintained by the third trusted party.

1.3. Various Cloud Issues

Some of the major issues of cloud computing are Data security, Costing model, Charging model, Service Level Agreement, migration and Cloud interoperability Issues[6].

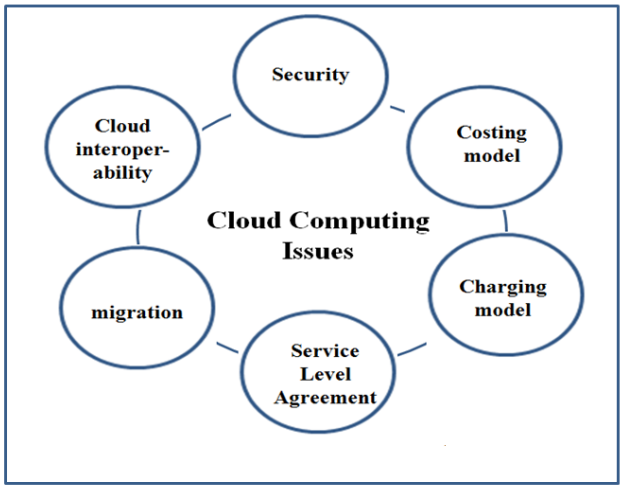

Figure 3: Cloud Issues

We are focusing on the security issues [7] in cloud in this paper. A recent report by Kaspersky Security solutions, a Russian based cyber security company places countries like U.S, China and India prone to cyber attacks. So security is the major issue in computing world.

2. Literature Survey

Preliminary work in this field was limited to cryptographic file systems and secure storage solutions. There is a previous study regarding network file systems [8], in which study is made regarding how to keep data securely onto untrusted servers. An another architecture [9] i.e. Depot is a two level architecture which guarantees security of data stored in cloud, even after malicious attacks i.e. it can tolerate the faults, attacks and can preserve confidentiality. But [8] and [9] don't support the computations on the encrypted data, so this architecture are not much helpful in implementing our goal. Many service providers guarantee confidentiality [10] by dividing the data of a single user and then storing it onto different clouds so as the cloud provider will be unable to get the data in whole. The data is reconstructed by aggregating these cloud providers. But the disadvantage is that if all the divided parts are gained by some of the cloud providers the confidentiality is at stake. Author [11] has given an architecture in which execution of queries of range is possible and makes possible to being robust against aggregate cloud providers. RBSecureDBaaS has made revolutionary changes on this front by skipping multiple cloud providers and using SQL supported encryption algorithm so as to execute common SQL operations on data in cloud.

Transparent Data Encryption feature characterizes the encryption of data at the file system level and building trusted DBMS over untrusted storage [12], [13]. Decryption of data is carried out in cloud before their use, as DBMS is trusted. RBSecureDBaaS cannot rely on this approach as we consider the cloud provider as untrusted.

Author [14] provides a simple and robust solution for firing queries on remote and encrypted databases on untrusted servers. This is done by using indexing information which is attached to the encrypted databases. In this approach DBMS is treated as a non trustful database where it is assumed as operations are executed over encrypted data. A modified DBMS engine is required, as it is not compatible with DBMS software used by cloud providers. On the other hand, RBSecureDBaaS doesn't require a modified DBMS engine as it is compatible with standard DBMS engine.

Encryption techniques are used in [15], [16] just as RBSecureDBaaS, so as to maintain compatibility in untrusted DBMS. They also perform SQL operations over encrypted data along with compatibility with common DBMS engines but, unlike RBSecureDBaaS [15], [16] make use of intermediate and trusted proxy. In [16] encryption of data in blocks is proposed instead of separate data items. When a data item is demanded by a client, the proxy has to process the whole data block, decrypt it and further set aside the unwanted data from it. For this process, modifications in the original SQL operation are required. This results in heavy overheads on the proxy as well as the DBMS server. Dependency on trusted proxy is a hindrance to outsourcing of the service along with questions of easy availability and accessibility of trusted proxies. Thus applicability of [15], [16] is limited.

RBSecureDBaaS crosses this hurdle by skipping intermediate proxy and directly connecting the client with the cloud service providers.

3. Proposed System

RBSecureDBaaS is designed to allow number of clients to access the untrusted database from cloud simultaneously & independently. Each client has its own limit for accessing the database depending on the role of the client in the overall architecture of the system.

We are assuming that an organization wants to use the untrusted database service from an untrusted Database cloud provider. The tenant then installs the RBSecureDBaaS in each of the machines (from Client 1 to N).Then these clients allow the users to connect to the cloud database. These users can then read and/or write the data or can perform basic SQL operations on the cloud database. The entities managed by

the RBSecureDBaaS are plaintext, metadata, encrypted data and encrypted metadata.

- Plaintext data- This is the data of the organization which need to be kept confidential and to store and process remotely in the cloud database.

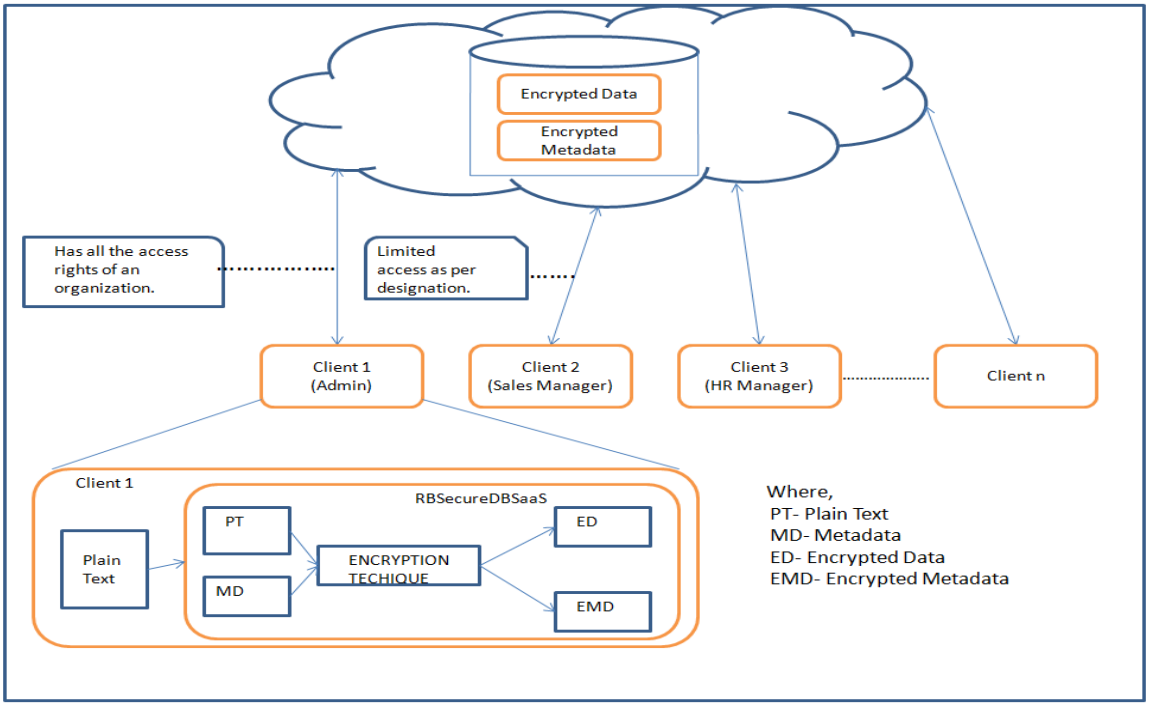

Figure 4: System Overview

- Encrypted data- The plaintext is converted to encrypted form, this is done by RBSecureDBaaS. RBSecureDBaaS adopts many cryptographic techniques to convert plaintext to encrypted data and encrypted data structures as the names of the tables and columns of the tables are encrypted using same encryption techniques.
- Metadata- It is set of data about the organization's data. RBSecureDBaaS produce this metadata so as it plays important role in encrypting and decrypting of data.
- Encrypted metadata- The above metadata of each and every table in database is encrypted by the RBSecureDBaaS and stored in cloud database.

The existing architectures, unlike RBSecureDBaaS, stores the cloud data in cloud database and its metadata on client side [16], splitting the metadata and storing one part in cloud database and other on intermediate proxy [15].
These architectures don't fulfill our aim of accessing the cloud database simultaneously, concurrently and role based. Hence, we are not using these obsolete architectures. In our architecture, we are introducing a approach where all the data and metadata is stored in cloud database in encrypted format. These data and metadata can be retrieved by the clients using SQL operations.

We can use control models such as Role-Based Access Control (RBAC) [2], Attribute Based Access Control (ABAC) for achieving role based access for each client in our system.

Some of the features which this system provides are:-

- SQL operations in RBSecureDBaaS are carried out simultaneously by the clients over the encrypted data within the cloud.
- It maintains confidentiality of the data, even though it in stored in the cloud, by encrypting it.
- A number of spatially distributed clients can access the cloud database simultaneously and independently.
- Most SQL operations deliver delayed results for the fired query due to mediator (server) and/or cryptographic overheads. RBSecureDBaaS does not use a mediator, thus delivering real time data, maintaining genuinity as in original cloud database.
- The client data and metadata stored in cloud database is always in encrypted form and the decryption is processed in RBSecureDBaaS. Thus, trustworthiness of the broker is immaterial.
- It provides various accesses to cloud data for variable users/clients depending upon their designation/role in the organization i.e. Role-Based Access.

4. Conclusion

In this paper, we have proposed RBSecureDBaaS architecture, that to some extend provides data security in cloud environment. This system tries to implement the database and database retrieval efficiently in cloud environment. Clients are capable of reading and writing data on cloud database, and each client has limited access as per his\her designation for organizations security purpose. Further work is, we can try and improve the SQL aware encryption techniques.

References

[1] Luca Ferretti, Michele Colajanni, and Mirco Marchetti "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE transactions on parallel and distributed systems, VOL. 25, No. 2, February 2014.
[2] Lan Zhou, Vijay Varadharajan, and Michael Hitchens , "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", IEEE transactions on information forensics and security, VOL. 8, No.12, December 2013.
[3] Amazon elastic compute cloud web services. http://aws.amazon.com/ec2.
[4] Netsuite saas portal. http://www.netsuite.com.
[5] Salesforceforce.com platform. http://developer.force.com.
[6] Kuyoro S. O, Ibikunle F. and Awodele O**.,** "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), VOL. 3, No. 5, 2011.
[7] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication.
[8] J. Li, M. Krohn, D. Mazieres, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.
[9] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.
[10] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, "Distributing Data for Secure Database Services," Proc.Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.
[11] M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, "AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing," Proc. Fifth Int'l Workshop Autonomous and Spontaneous Security, Sept.2013.
[12] "Oracle Advanced Security," Oracle Corporation, http://www.oracle.com/technetwork/database/options/advanced-security, Apr. 2013.
[13] G. Cattaneo, L. Catuogno, A.D. Sorbo, and P. Persiano, "The Design and Implementation of a Transparent Cryptographic File System For Unix," Proc. FREENIX Track: 2001 USENIX Ann.Technical Conf., Apr. 2001.
[14] E. Damiani, S.D.C. Vimercati, S. Jajodia, S. Paraboschi, and P.Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational Dbmss," Proc. Tenth ACM Conf. Computer and Comm.Security, Oct. 2003.
[15] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan,"CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles,Oct. 2011.
[16] H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.

Author Profile

Miss. Sharvari Ashokrao Pawar received the B.E degree in Information Technology from Parvatibai Genba Moze college of Engg.Pune,Maharashtra, India in 2012 .Presently pursuing M.E degree in Computer Engineering from Sinhgad Academy of Engg. ,Pune ,Maharashtra, India.

Prof. Suresh B. Rathod received the B.E degree in Information Technology from STBCE, Tuljapur, Maharashtra ,India in 2007.He has also completed his M.E from SCOE, Pune, Maharashtra, India.