ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

Secure Database as a Service-a Review

Prof Swarnalata Bollavarapu[1], Kamal Mistry[2]

Assistant Professor, Department of Computer Engineering, MPSTME, Mumbai, India [1]

M-Tech Student, Department of Computer Engineering, MPSTME, Mumbai, India [2]

Abstract: Cloud computing is one of the emerging field in the IT industry and is widely adopted across the globe due to the easy accessibility and availability of the data from any location in the world over the internet. The era of cloud computing has reduced the overhead of hardware resources and maintenance due to this many industries have started using the different services provided by the cloud example Software as a service or platform as a service. In the recent years Database as a service has become boon in cloud computing era, it will reduce the overhead of installing and maintaining database on the client side, like any other services database as a service is also being provided on the pay per usage policy. In recent years many cloud service providers had started providing database as a service, among them few are: Amazon, Microsoft, Google etc. are good service provider.This paper discusses about the Database as a service and the security challenges faced by the database service provider. CRYPTDB and Monomi system is discussed to overcome the security challenges in database as a service.

Keywords: Cloud computing, CryptDB, Database as a service, database security, Challenges

I. Introduction

Cloud computing is defined as accessing the data from remote location via the internet without having any overhead on client machine. According to NIST definition of Cloud Computing —Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]Cloud computing is now a days working as a backup for any data, now a day's people have lots of important data and they need back up for the same so due to the hike in cloud computing services they make the use of cloud services for storing their data, example Google drive gives up to 5GB storage space. The different types of service model provided by cloud computing is shown in figure-1 1) Software as a service: example Email, virtual desktop and google apps, 2) Platform as a service: example Web server, Google App Engine.3) Infrastructure as a service: Virtual machine, storage, and server.These service models are also known as SPI (Service, Platform and Infrastructure).

Apart from these the other emerging cloud services that fall into the SPI model is Database as a service that can be a part of software as a service or platform as a service depending on the way it is delivered by the service provider. The major challenge in the database as a service is providing data security, while performing any CRUD operations on cloud. The two systems which are used for providing security in cloud database are CRYPTDB and MONOMI.

A. *Essential characteristics [1]*

*On-Demand Self Service:*Consumer makes the usage of cloud services as per their demandwithout even interacting with the cloud service provider example google drive.

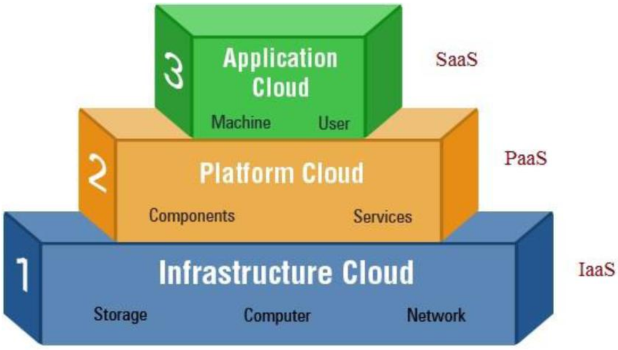

Figure 1 Cloud Computing Service models [13]

Broad network access: Heterogeneous thin or thick client platforms like mobile phones, tablets, laptops and workstation access the capabilities available on the network through standard mechanism.

Resource pooling: In order to serve multiple consumers using a multi tenant model, with different physical and virtual resources given to them dynamically or taken back when work is done according to the consumer demand, the service providers pool their computing resources. Here consumer is not having any idea from where the resources are provided but able to specify location at higher level of abstraction (ex. country, state etc.). Some examples of resources that are pooled are storage, bandwidth, memory and processing.

Rapid Elasticity: Sometimes what happens that the consumers demand is very high at point of time, so in order to avoid delay at the consumer end the cloud has a most important feature called as scalability, the resources are provided to the consumer can be elastically provisioned and released.

*Measured Service:*Service provider charges user on the basis of their usage of cloud servicei.e. pay per usage

DOI 10.17148/IJARCCE.2015.43102

policy. Types of services like storage, processing, bandwidth etc. are leveraged at some level of abstraction as cloud system automatically control and optimize resources. And the monitoring, controlling and reporting of resources usage are done in order to provide transparency for provider as well as for consumer using the service.

The rest of the paper is organized as follows. Section 2 gives an overview of Database as a service. Section 3 describes the specific issues with respect to the database as a service. Section 4 discusses about the secured database system/architecture by different authors for the security issue of database as a service. Section 5 focuses on inferences. We conclude the paper in section 6.

II. DATABASE AS A SERVICE

Database as a service is a new emerging cloud service model which is a subtype of SAAS or PAAS like any other services in cloud this is also provided on the pay per usage policy. Database as a service means outsourcing your database in which the database is deployed on the cloud environment which is to be maintained by the service provider; due to this it reduces the overhead of installation, storage and maintenance of the database on client machine. Outsourcing of database is widely accepted by the consumer because now a day's database contains much information and its size exceeds to Gigabyte, so it's better to use database as a service. In database as a service environment client machine must be lightweight, possibly just accessing the cloud database through browser. Database as a service is provided in 2 way 1) we buy the infrastructure as service from the cloud service provider, we deploy our choice of database, maintain it and use as per our need 2) We can subscribe for Database as a service in this we just need to connect our application with the database and rest will be done by the database service provider.

III.ISSUES IN DATABASE AS A SERVICE

Cloud computing has become the boon in last few decades but still there are several issues which are of major concern and need to mitigate those issues. The most important issue is the data privacy, as our data is on the cloud so we are always in the insecurity of confidentiality, integrity and availability of our data. Some of the issues/threats that were focused in cloud security alliance were: Data Loss, Data breaches, Insecure API, Denial of service, Abuse of cloud service etc [10]. Migrating database on cloud reduces the overhead of hardware cost and maintenance but brings the various security concerns with respect to the database security. To ensure the confidentiality of the data which is stored at the cloud database must be properly encrypted. To ensure integrity, the access to the data stored at cloud database provider's platform needs to be controlled and monitored properly for all users including the database administrators.

A. Database Security Challenges on Cloud[13]

*Availability:*Availability in simple terms means the extent to which system resources are accessible and usable to individual users or organizations.. It is one of the critical security aspects that organizations need to take into account when considering cloud database services. Database does not require 100% availability but some of the application suffers a lot if database is down for certain period of time. Moreover, the level of availability of a cloud database service, data backup options and disaster recovery mechanisms should be addressed properly within an organization before considering a move to cloud environment.

Access Control Issues in Public Cloud: As we are outsourcing the database on cloud we loss the logical, physical and personnel access control and due to this it brings the inbuilt security risk. Therefore proper access control procedures must be used by the service provider for ensuring security of the data.

Data Breach: As our data is on the cloud environment so it is always vulnerable to attacks. By these attacks one client's application could allow an attacker access not only to that client's data, but every client's data over the same cloud.

*Malicious Insider:*In this the data which is there on the cloud is not only vulnerable to attacks by attacker but also by malicious insider like DBA or cloud service provider.

Apart from the above security challenges the other security challenges are data sanitization,data loss, Insecure API, Denial of service, Abuse of cloud serviceetc.

IV.SECURED DATABASE SYSTEM/ARCHITECTURE

In this section we have covered 2 methods proposed by different researchers for providing security to the database on cloud.

A. CryptDB [3]

It is a system proposed by the researcher Of MIT for processing queries over encrypted data. The goal of crypt db system is to provide confidentiality of the data. CryptDB protects against two types of threats to confidentiality:

1)the curious in-house or 3rd party DBA with full access to the DBMS, who reads but doesn't alter data or queries

2) an attacker who has taken control of the DBMS and application servers and can access the encryption keys.The design challenge of the crypt DB system is to minimize the amount of confidential information to the DBMS sever and minimizing the amount of decrypted data.

To address these challenges crypt Db uses 1) Introduce a db proxy which executes queries over encrypted data 2) SQL aware encryption strategy i.e. "onions of encryption".

DOI 10.17148/IJARCCE.2015.43102

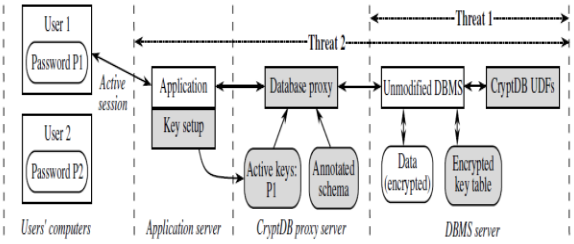

Figure 2 CryptDB Architecture [3]

The above figue-2 shows the architecture of crypt DB consisting of application server, CryptDB proxy server and DBMS server.

Application Server: runs the application code and issues DBMS queries on behalf of one or more users is modified so that it provides the db proxy with encryption key

DBMS server: All its data is encrypted including tables& columns still it executes the queries over encrypted data assuming as it is executing the plain query. It has user defined functions (UDFs) installed to allow it to compute on ciphertexts for certain operations. It also has some auxiliary tables (ex. Encrypted keys) used by the db proxy

Proxy Server: It is the important block of the entire architecture as all the encryption, decryption and key management is handled by the proxy server. It also stores the key for keeping the track of current level of onion encryption

1) Processing Queries in CryptDB:

- Db proxy intercepts application's query and rewrites it by identifying table and column names & encrypting constants with the key of the encryption scheme best suited for the operation and the user.

- Db proxy checks if the DBMS needs to adjust encryption level before executing the query if yes issue an UPDATE query that invokes a UDF to adjust the encryption level layer of the appropriate columns

- Db proxy sends the encrypted query to the DBMS server

- DBMS executes query using standard SQL (invoking UDFs for aggregation or keyword searches) and returns the encrypted results

- Db proxy intercepts and decrypts results, and sends them to the application

2) User Defined Function[7]:

A function contains instructions in order to perform a specific task, and provides to repeat this task easily. User-defined function is also a function, and it is created by a user. This user needs to have permissions to perform the processes in the database, or database owner abbreviated as dbo can be used. Dbo is a user which can perform all activities in the database. If there exist a table called square which has two columns as edge length and order number of the square, then a UDF is written to calculate the area of the squares inside the database.The following table-1 is a sample square table.

Table I
Sample square table [7]

Square	
Number	**Edge Length**
1	10
2	5
3	7

Here is an example of creating a UDF.
Create function dbo.area (edge float)
returns float
return (edge*edge).
An example query to use this UDF can be like as follows:
Select number, area (edge length) as Area from Square;

Table II
SQL result [7]

Number	Area
1	100
2	25
3	49

3) Onion Layer of Encryption:
The figure 3 describes about the onion layer of encryption. There are 7 different layer of encryption considering outermost to be the most secured layer of encryption. Inner onion layers are progressively weaker and are accessed as required by the query

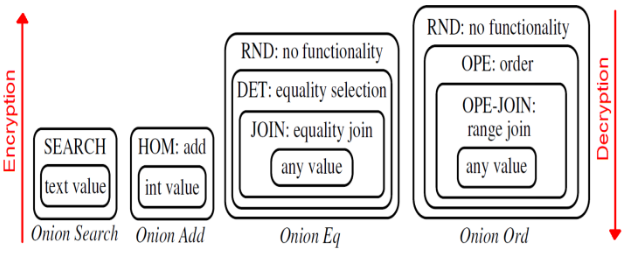

Figure 3 Onion Layer of Encryption [3]

Table III
Onion Layer of Encryption

Onion Encryption	Operation
Randomized Encryption	Most secured, used with select but no predicates.
Deterministic Encryption	Allows equality check, used with selects with equality predicate
Homomorphic Encryption	Enables addition and multiplication operations.
Equi-Join	It is used For equality check
Range Join	Occurs rarely, involves order check
Word(Search)	allows LIKE on full word searches, but not regular expressions, and requires a call to a UDF

DOI 10.17148/IJARCCE.2015.43102

B. Monomi[6]

Monomiarchitecture consists of 3 major components as shown in the figure 4 below.

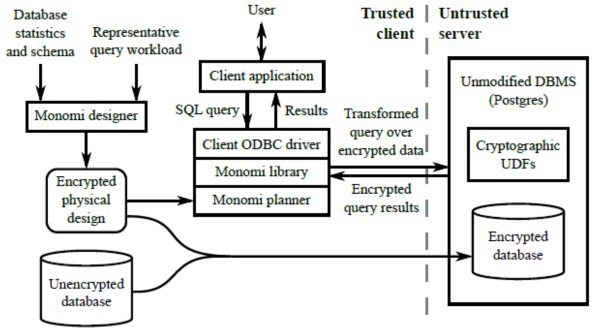

Figure 4 Monomi Architecture [6]

First **Monomi designer** run on trusted client machine for design of untrusted server.

Second, during normal operation, applications issue unmodified SQL queries using the **MONOMI ODBC library**, which is the only component that has access to the decryption keys. The ODBC library uses the planner to determine the best split client/server execution Plan for the application's query.

Third, **Library** issues more than one query to the encrypted database, which does not have access to the decryption keys and can execute operations over encrypted data. After the processing is done the result is sent to the client library which has access to the decryption key there the result is decrypted and output is given back to application.

*1) Split client/server execution:*In this technique there are some queries which cannot be only executed on server itself. So monomi suggested the split client/server execution where part of query is executed on server and then the intermediate result is fetched by client and further processing is computed on the client machine. For selecting the best split client/server execution we need proper designer and planner.

2) Designer and Planner:The goal of MONOMI's designer is to decide how to encrypt the data (physical design). MONOMI's planner, on the other hand, determines how to best execute queries given a particular physical design. MONOMI's designer is invoked during the setup phase, when the user is preparing to load his database into MONOMI. The user provides the designer with a query workload (n queries). The query workload does not need to exhaustively enumerate every possible query the user will run, but it should be representative of the operations that the user is expecting to perform over the data. The user also provides a sample of the data that will be loaded into the database, which is used for estimating statistics about the data, and need not be the exact data that will be eventually loaded on the server.

V. INFERENCES

The following table gives the detailed information about the onion layer of encryptions. These encryptions are applied on the basis of the input query, for example if any query related to equality operation comes as an input query then deterministic layer of encryption is applied on that query.

Table IV
Detailed SQL aware encryption in CryptDB

Scheme	Operation	Details
RND	None	AES
HOM	+,*	Paillier
DET	Equality	AES in CTR
Search	Like	Song's Search
OPE	Order	Boldyreva et al. '09

Table V
CryptDB VS Monomi

Sr. NO	CryptDB	Monomi
1	It executes query over encrypted data	It is first system for executing analytical workload over encrypted data.
2	Architecture is divided into 3 major components: 1 application server 2 proxy server 3 DBMS server	Architecture is divided into 3 major components: 1 Monomi's designer 2 Monomi's ODBC library 3 execution plan(designer and planner)
3	It uses onion layer of encryption	It is based on CryptDB encryption scheme
4	It executes queries on server	Execution of query is splitted between client and server
5	CryptDB executes 4 out of 22 TPCH queries [5]	Monomi executes 19 out of 22 TPCH queries[5]

Crypt Db

Advantages:

1) Designed for OLTP queries

2) Capability of executing queries over encrypted data.

3) Dynamically adjusting encryption level

4) Minimum information leakage on untrusted server

Disadvantages:

1) No efficient additive + multiplicative Homomorphic cryptosystem.

2) No efficient additive + order preserving Homomorphic cryptosystem.

Monomi System

Advantages

1) First system for executing analytical queries over encrypted data.

2) Execution of query is splitted between client and server

DOI 10.17148/IJARCCE.2015.43102

3) It improves the query performance

Disadvantages:

1) Increased hardware cost.
2) Complex system setup.

VI. CONCLUSION

Cloud computing is the emerging field in IT industry and many of the things are now migrated to cloud due to the reducing hardware cost and pay per usage service. It provides various services like infrastructure, Platform, Software to the users and recently started with database as a service for the cloud. This paper discuss about the database as a service for cloud and its security challenges like data loss, availability, access control in public cloud, data ingerity etc. To overcome these security challenges we had discussed about cryptDB system which works with the onion layer of encryption and is efficient for executing queries over the encrypted data it applies the layer of encryption on the basis of input query but cryptDb does not support additive+multiplicative homomorphic cryptosystem. After that we had discussed Monomi which is the first sytem for executing analytical workload over encrypted data it excutes 19/22 tpch queries which is more as compared to cryptdb's 4/22[7], execution of query is splitted on client and server.

REFERENCES

[1] "NIST Cloud Computing Definition", NIST SP 800- 145
[2] Carlo Curino, Evan Jones, RalucaPopa, Nirmesh Malviya, Eugene Wu, Sam Madden, Hari Balakrishnan, Nickolas Zeldovich," Relational Cloud: a Database Service for the cloud", Conference On Innovative Data Centre and Research,2011.
[3] Raluca Ada Popa, Catherine M. S. Redfield, Nickolas Zeldovich, and Hari Balakrishnan," Crypt DB: Protecting Confidentiality with Encrypted Query Processing", Symposium on Operating Systems Principles, 2011.
[4] Carlo Curino, Yang Zhang, E van Jones, Sam Madden, "Schism: a Workload-Driven Approach to Database Replication and Partitioning", Very Large Databases, 2011.
[5] Database as a service: https://cloud.oracle.com/database
[6] Stephen Tu, M. Frans Kaashoek, Samuel Madden, Nickolas Zeldovich. "Processing analytical queries over encrypted data", Very Large Databases, 2013.
[7] Mehmet Sabir Kiraz, Fatih Birinci and Ziynet Nesibe Dayıo "Secure Database in Cloud Computing: Crypt DB Revisited", International Journal Of Information Security Science, 2013.
[8] CloudComputing:http://www.slideshare.net/ronak2454/issues-in-cloud-computing-9710875
[9] Atul Kahate ―Cryptography and Network Security‖ Tata McGraw-Hill,3rd edition, 2013
[10] Aaron Alva, Olivier Caleff, Greg Elkins, Allen Lum, Keith Pasley, Satheesh Sudarsan, Vinoth Sivasubramanian, and Rajeev Venkitaraman, "The Nortorious Nine Cloud Computing Threats", 2013.
[11] Weis Joel, Jim Alve-foss,"Securing database as a service issues and compromises",IEEE,1540-7993, vloume 9, issue 6, 2011
[12] HakanHacıg¨um¨us,BalaIyer,Sharad Mehrotra,"Providing database as a service", IEEE, 1063-6382, 2002
[13] Imal sakhi, "Database Security in The Cloud" 2012

ACKNOWLEDGMENT

This literature review was supported by my mentor **Prof. Swarnalata Bollavarapu**. I am grateful to her for sharing her pearls of wisdom with me during this literature work.

BIOGRAPHIES

Ms. Swarnalata Bollavarapu has received M.E. (Computer Engg.) from Thadomal Shahani Engineering College, Mumbai. She has around 10 years of teaching experience. She iscurrently working as Assistant professor in Department of Computer Engg.at MPSTME, NMIMS University,Mumbai.

Mr. Kamal Mistry has received B.E. (Computer Engg) from Vidyalankar Institute of Technology, Mumbai. He is currently pursuing M-Tech in Computer Science at MPSTME, NMIMS University, Mumbai.

DOI 10.17148/IJARCCE.2015.43102