IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 1, January 2017

Review on Implementing Security using SDBaaS

Miss. Arpita R. Malpe[1], Prof P. A. Tijare[2], Prof G.S. Thakare[3]

M.E.2nd Year, Department of Information Technology, SIPNA COET, Amravati, India[1]

Associate Professor, Department of Information Technology, SIPNA COET, Amravati, India[2]

Assistant Professor, Department of Information Technology, SIPNA COET, Amravati, India[3]

Abstract: Setting important facts within the arms of a cloud provider must include the guarantee of safety and availability for facts at rest, in movement, and in use. Numerous options exist for storage offerings, while facts confidentiality answers for the database as a service paradigm are nonetheless immature. It integrates cloud database offerings with facts confidentiality and the opportunity of executing concurrency. Inside the Secure Database-As-a-Service (SDBaaS) model, clients save their database contents at servers belonging to doubtlessly untrusted service companies. To keep data confidentiality, clients want to store their data to servers in encrypted form. At the identical time, customers ought to still be capable of execute queries over encrypted data.

Keywords: Cloud, security, confidentiality, Secure DBaaS, database.

I. INTRODUCTION

Present day cloud computing structures pose serious challenge to protective user's information confidentiality. In view that users' sensitive records is offered in unencrypted bureaucracy to remote machines owned and operated by means of third party service providers, the risks of unauthorized disclosure of the user's sensitive facts by providers may be pretty high. There are numerous strategies for protecting users' data from outdoor attackers, but currently no powerful way is to be had for protective users' sensitive data from service provider in cloud computing. There may be a way to protect the confidentiality of user's records from service provider, and ensures service provider cannot accumulate user's exclusive records at the same time as the records is processed and stored in cloud computing systems.

Cloud computing is a form of internet-based totally computing that offers shared laptop processing assets and statistics to computer systems and other devices on call for. It is a model for permitting ubiquitous, on-demand get entry to a shared pool of configurable computing resources (e.g., laptop networks, servers, garage, packages and services), which may be swiftly provisioned and launched with minimum management effort. Cloud computing and storage offer users and enterprises with diverse skills to shop and system their information in third party information facilities that can be located a long way from the consumer–ranging in distance from across a metropolis to the world over. Cloud computing relies on sharing of sources to gain coherence and economy of scale.

Based totally on SaaS, DBaaS actions database management system (DBMS) from a conventional client-server architecture – wherein the data owner is chargeable for coping with DBMS and responding to user's queries – to a third party architecture – wherein data management is not treated with the aid of the facts owner. Data owner outsource their records to information provider companies. Database as a service (DBaaS) gives a extensive range of blessings including data outsourcing, multi-tenancy, and useful resource sharing and so on .As shown in figure below depicts that the cloud provider which can also be a SaaS provider that provides the services to the user of the SaaS.

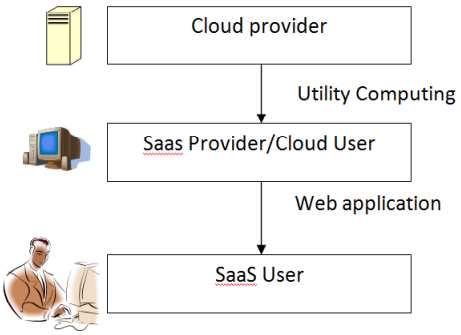

Figure 1.1: Users and Providers of Cloud Computing

The Secure DBaaS architecture is customized to cloud platforms and does not add any intermediary proxy or broker server between the client and the cloud service provider. Casting off any depended on intermediate server lets in Secure DBaaS to reap the same availability, reliability, and elasticity degrees of a cloud DBaaS.

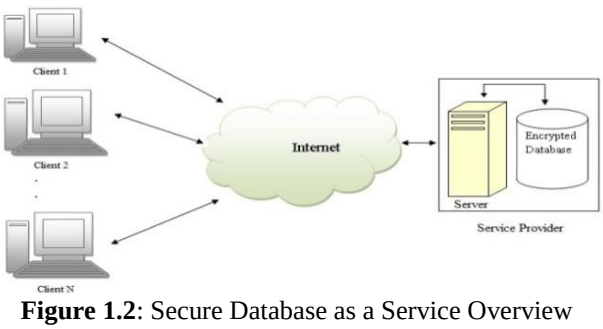

Figure 1.2: Secure Database as a Service Overview

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 1, January 2017

Secure DBaaS that helps the execution of concurrent and independent operations to the remote encrypted database from many geographically allotted clients as in any unencrypted DBaaS setup.

As described in figure 1.2 for allotted computing the clients are related to the cloud through the internet affiliation .On the cloud aspect there may be a cloud provider issuer to which the server is related to the scrambled database via using the AES encryption method. Customers can comfy their records in an encrypted database .As statistics category is stored up.

II. RELATED WORK

As in Luca Ferretti, Michele Colajanni, and Mirco Marchetti [1] proposed an architecture that degrades the risk for any intermediate part, by achieving availability and scalability as of unencrypted cloud database services. Benefits are assures file consistency in scenarios during which independent clients at the same time performs SQL requests, and the structure from the database can be modified. Decreased isolation quantities for multiple version systems have not been characterized before in spite of being implemented in different products and the disadvantage are concurrent modifications from the database structure are generally supported but at the cost of higher overhead as well as stricter transaction remote location levels.

M. Armbrust et al [2], has developed with modern thoughts for new internet offerings now not require the huge capital outlays in hardware to deploy their service or the human fee to function it. Cloud Computing will grow, so builders need to take it into consideration. Furthermore:
1. Applications software wishes to both slash hastily in addition to scale up, that's a new requirement. Such software also desires a pay-for-use licensing model to match wishes of Cloud Computing.

R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan [3] had developed CryptDB is a device that offers sensible and provable confidentiality within the face of those attacks for applications backed by way of sq. Databases. It works via executing sq. Queries over encrypted data the usage of a group of efficient square-conscious encryption schemes. CryptDB, a machine that explores an intermediate design point to offer confidentiality for applications that use database management systems (DBMS). CryptDB leverages the standard structure of database-subsidized applications, which includes A DBMS server and a separate software server CryptDB's technique is to execute queries over encrypted facts, and the important thing insight that makes it practical is that square makes use of a nicely-described set of operators, every of which are capable of help efficaciously over encrypted information.

V.Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani [9] have proposed, the approach of database services has arises in privacy interest on the role of the client storing data in third party database service providers. It also provides algorithms for distributing data and partitioning the query at the client to queries for the servers is done by a bottom up state based algorithm. Finally the outcomes at the servers are integrated to acquire the solution at the client.

As in H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra [5] NetDB2, a database model on-line affords a useful mechanism for organizations to acquire data management like a service. Database as an e-mail finder service makes the benefit of extra overhead of far flung get right of entry to statistics, an infrastructure to guarantee records privacy, and program layout. Records privateers may be accomplished in unique stages via utilising encryption strategies with both software program and hardware levels. NetDB2 version also performs create/eliminate furniture, views, triggers, crawls, summary information types, square queries, create and call consumer described features and stored strategies, producing and deleting crawls, and so forth. A few DBMS engines provide the risk of encrypting understanding at the record gadget level thru the alleged transparent statistics protection feature. This feature makes it viable to assemble a reliable DBMS over untrusted garage. The DBMS is relied on and decrypts understanding earlier than their use.

M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei [6] A at ease Searchable mystery Sharing Scheme (AS5) to tolerate statistical assaults based on adversary's information about outsourced data distribution. In AS5 facts stocks are generated uniformly across a site to prevent statistics leakage approximately the outsourced statistics. In a searchable secret sharing scheme in which the ordering relation between values is preserved in their corresponding stocks, whilst the distribution of shares is different from the unique records distribution. Searchable secret sharing scheme to be relaxed in opposition to adversaries powered by a priori information of outsourced statistics to tolerate statistical evaluation on statistics stocks.

III.PROPOSED WORK

A. CLIENT SIDE

1) In SQL Query Processor/Parser, in the database system, the query processor can also be called the query executor. Query parser, takes query textual content and produces a parse tree (or produces syntax or semantic structure). Input query is pre-processed to SQL. A query processor is a module within the DBMS that performs the responsibilities to manner and to optimize. In parser it exams the proper syntax of the query. Optimizer will execute query it will take information from the DBMS Catalog consists of the data dictionary which defines the format, contents and type of the query, the result of the query contains the tenant information.

2) Generate Tenant information: the information extracted by using the query parser may be handled because the tenant data this data will be the real processing information that would be held inside the entire SQL query. Because the tenant information is the actual information of the client.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 1, January 2017

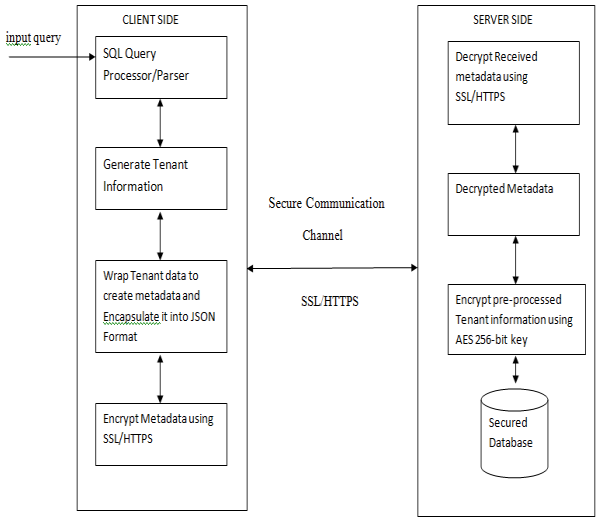

Figure 3.1: System Architecture

3) Generate metadata**:** the tenant data is wrapped to create metadata, on the way to consist of all the semantic records related to the tenant records generated. This Meta information will incorporate all of the semantic information regarding the SQL query that wishes to be operated over secure database device. After this module the complete metadata will be wrapped in JSON format for submit-processing on cloud side.

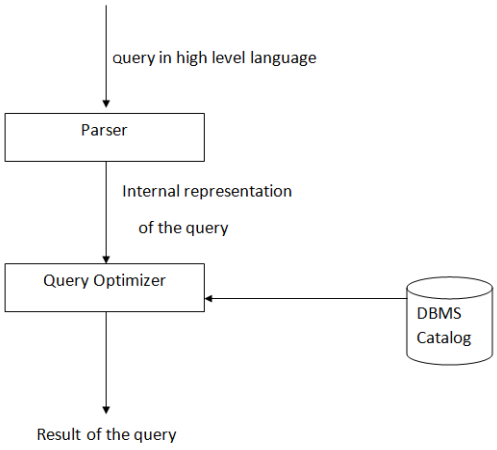

Figure 3.2: Query Processor

As described in [7] JSON (JavaScript item Notation) is a light weight statistics-interchange format. It is simple for humans to study and write. It is simple for machines to parse and generate. It is based on a subset of the JavaScript Programming Language, fashionable ECMA-262 3rd version - December 1999. JSON is a textual content layout that is absolutely language independent however makes use of conventions which can be acquainted to programmers of the C-own family of languages, inclusive of C, C++, C#, Java, JavaScript, Perl, Python, and many others. Those properties make JSON an excellent information-interchange language.

JSON is constructed on systems: A collection of call/price pairs. In various languages, this is realized as an object, file, struct, dictionary, hash table, keyed list, or associative array. An ordered list of values. In maximum languages, this is realized as an array, vector, list, or series. These are common data structures. Really all modern programming languages aid them in one shape or every other. It makes feel that a statistics format that is interchangeable with programming languages additionally be primarily based on these structures.

In JSON, they take on those forms: An object is an unordered set of call/price pairs. An item begins with (left brace) and ends with (right brace). Each call is accompanied by means of: (colon) and the name/fee pairs are separated by means of, (comma).

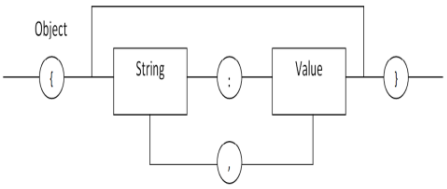

Figure 3.3: JSON Syntax

4) Encrypt Metadata: on this we are going to secure the metadata generated inside the previous step, so one can transfer these facts over cozy communication channel to cloud. So it can be the usage of HTTPS/SSL to soundly encrypt and transfer data to cloud server which protects in opposition to guy-in-the-centre attacks. Additionally, it provides bidirectional encryption of communications among a client and server, which protects against eavesdropping and tampering with or forging the contents of the communication.

5) Https connection: The HTTPS uniform resource identifier (URI) scheme has same syntax to the usual HTTP scheme, aside from its scheme token. However, HTTPS signals the browser to apply on delivered encryption layer of SSL/TLS to defend the traffic. SSL/TLS is especially appropriate for HTTP, when you consider that it can provide some protection despite the fact that best one facet of the verbal exchange is authenticated. That is the case with HTTP transactions over the net, where normally handiest the server is authenticated (by way of the customer examining the server's certificate).HTTPS creates a comfy channel over an insecure community. This guarantees affordable protection from eavesdroppers and guy-in-the-middle assaults, provided that good enough cipher suites are used and that the server certificates is confirmed and depended on.

Because HTTPS piggybacks HTTP totally on top of TLS, everything of the underlying HTTP protocol may be encrypted. This includes the request URL (which unique net page was asked), question parameters, headers, and cookies (which frequently incorporate identity statistics approximately the consumer). But, due to the fact host (internet site) addresses and port numbers are necessarily a part of the underlying TCP/IP protocols, HTTPS can't shield their disclosure. In exercise this means that even on a correctly configured internet server, eavesdroppers can

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 1, January 2017

infer the IP deal with and port number of the net server (sometimes even the domain call e.g. www.Example.Org, but no longer the rest of the URL) that one is communicating with, in addition to the quantity (statistics transferred) and length (period of session) of the verbal exchange, even though now not the content of the communication.

B. SERVER SIDE

1) Decrypt Metadata :In this we are going to decrypt the metadata generated on client aspect, here we are able to be the use of popular HTTPS/SSL decryption mechanism with a purpose to decipher meta records generated on client aspect, with a purpose to procedure this data to enforce put up-processing on server facet.

2) Encrypt/Decrypt pre-processed tenant data: In this we are able to be encrypting all of the tenant records like tables names, column names, in addition to all of the SQL. Table facts, so here we can be using AES encryption with 256 bit secret key. The advanced Encryption preferred or AES is a symmetric block cipher Encryption popular, we will chose 128, 192 or 256-bit long key size for encryption and decryption.

3) Secure Database: On this the encrypted records is saved inside the database by way of 256-bit AES encryption key.

C. AES Encryption

In [8] the important thing length used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, known as the plaintext, into the final output, called the cipher text. The wide varieties of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Excessive-level description of the algorithm

- Key Expansions—round keys are derived from the cipher key the use of Rijndael's key time table. AES requires a separate 128-bit round key block for each spherical plus one more.

1. Initial round.

- AddRoundKey—each byte of the nation is blended with a block of the add round key the use of bitwise xor.
- Rounds

1. SubBytes—a non-linear substitution step where every byte is changed with some other according to a lookup table.

2. ShiftRows—a transposition steps wherein the remaining 3 rows of the kingdom are shifted cyclically a sure quantity of steps.

3. MixColumns—a mixing operation which operates at the columns of the nation, combining the four bytes in each column

4. Add round Key.

1) The SubBytes Step

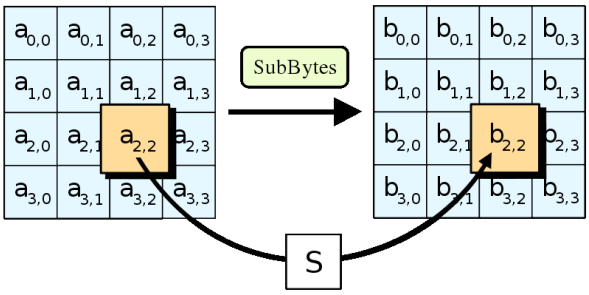

Figure 3.4: SubBytes Step

Inside the Sub Bytes step, every byte inside the state is changed with its entry in a hard and fast eight-bit look-up table, S; $b_{ij} = S(a_{ij})$.

2) The ShiftRows step

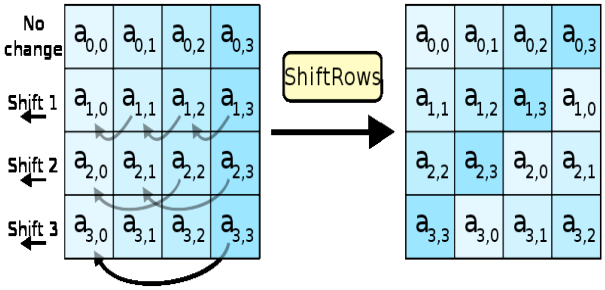

Figure 3.5: ShiftRows step

In the ShiftRows step, bytes in each row of the state are shifted to the left. The number of places each byte is shifted differs for each row.

3) The MixColumns step

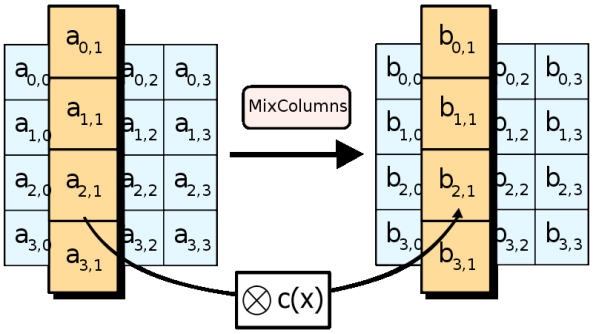

Figure 3.5: MixColumns step

In the MixColumns step, each column of the state is multiplied with a fixed polynomial

4) The AddRoundKey step

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 1, January 2017

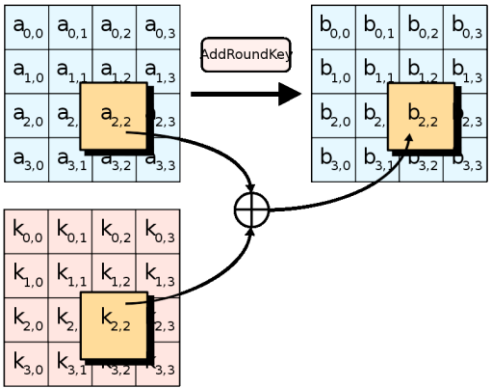

Figure 3.6: AddRoundKey step

IV. CONCLUSION

In the proposed work its miles modern structure that guarantees confidentiality of records stored in public cloud databases. In contrast to present day strategies, it does now not rely upon an intermediate proxy that we do not forget a single factor of failure and a bottleneck restricting availability and scalability of ordinary cloud database offerings. The proposed structure does not require adjustments to the cloud database, and it's far without delay relevant to present cloud DBaaS. An progressive architecture that guarantees confidentiality of information stored in public cloud databases.

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] M. Armbrust et al. "A View of Cloud Computing", Comm. of the ACM, vol. 53, no. 4, pp. 50-58, 2010.
[3] 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.
[4] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database ServicesProc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.
[5] H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra "Providing Database as a Service" H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, Proc. 18th IEEE Int'l Conf. Data Eng., Feb. 2002.
[6] 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.
[7] http://www.json.org/
[8] http://www.wikipedia.org/wiki/Advanced_Encryption_Standard