International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Dynamic and Scalable Architecture for Accessing the Cloud Databases and Securing Cloud Services Using Public Key Infrastructure

Rex Cyril B[1], Dr. S. Britto Ramesh Kumar[2]
Asst.Professor and Research Scholar[1], Asst.Professor and Research Scholar[2]
Department of Computer Science, St.Joseph's College(Autonomous), Tirchy, Tamil Nadu, India

ABSTRACT

Cloud computing, a revolutionary term for the long-dreamed idea of computing as an application. Cloud Computing can provide numerous advantages for real world applications, such as rapid useful resource elasticity, on-demand self-service, usage-based pricing, outsourcing, pervasive network access, etc. In Cloud computing, large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. The cloud goals to cut fees, and assist the customers focus on their middle business instead of being impeded by means of IT obstacles. Cloud storage, Data as a Service (DaaS) and Database as a service (DBaaS) are the different phrases used for information management within the cloud. Differ on the basis of how data is stored and managed. Cloud storage is a virtual storage that enables users to store documents and objects. Cloud database should support features of cloud computing as well as of traditional databases for wider acceptability. The potential challenges associated with cloud database are scalability, high availability and fault tolerance, data consistency and integrity, confidentiality and many more. This paper proposes a dynamic and scalable architecture for cloud database services and provides complete protection on data security, data privacy and data breaches on cloud computing with the help of Public Key Infrastructure.

Keywords : Database as a service (Dbaas), PKI executes, Data security, Data privacy and Data breaches**.**

I. INTRODUCTION

For corporate organizations, cloud computing gives the capability to outsource computing infrastructure to attention on center talents with better efficiencies that is tons useful to them. Cloud computing is based on virtualization, which allows the multitenancy and on-demand use of scalable shared resources by all tenants. It may be very fine to apply cloud offerings for the commercial enterprise man or woman, to consumer, groups can put off the need for the professionals who preserve and help the underlying complexities for a number of the maximum suited new IT technologies, which include highly scalable, variably provisioned systems. An apparent gain to clients is that computing resources, along with digital servers, information garage, and network talents, are all load balancing and automatic expandable. Resources are allocated as wished, and loads can be transferred routinely to higher locations, generating a sturdy, dependable provider. The idea is easy sufficient. A large organization with many computing sources, together with big statistics centers, reaches a settlement with customers. Customers can run their packages, shop their records, and host digital machines, and so forth, using the company's sources. Customers can terminate their contract, keep away from startup and renovation fees, and enjoy the company's capability to dynamically allocate their resources. Cloud computing service vendors typically following resource types, which create a more not unusual type of cloud type: infrastructure, platform, or software.

ADVANTAGES OF CLOUD COMPUTING:

- Archival and Disaster Recovery Purposes
- Cloud Storage Security and Privacy Threats
- Greater Accessibility and Reliability
- Lower Complexity and Costs

CLOUD COMPUTING MODEL APPLICATION METHODOLOGY:

Cloud computing is a new model for imparting commercial enterprise and IT services. The provider transport version is based totally on future development attention while assembly contemporary development necessities. The three stages of cloud computing service (IaaS, PaaS and SaaS) cowl a massive range of services. Besides computing and the carrier transport model of storage infrastructure, various models which include information, software, program, application, programming model etc. Can also be applied to cloud computing. More importantly, the cloud computing version entails all aspects of employer transformation in its evolution, so technology structure is best a part of it, and multi-factor development along with organization, procedures and distinctive enterprise models must additionally be beneath consideration. Based on popular architecture methodology with first-rate practices of cloud computing, a Cloud Model Application Methodology may be used to guide industry client analysis and clear up capacity troubles and dangers emerged at some stage in the evolution from current computing version to cloud computing model. This methodology also can be used to instruct the investment and selection making analysis of a cloud computing model, determine the manner, well known, interface and public provider of IT belongings deployment and control to promote enterprise improvement. The diagram beneath suggests the general reputation of this system (Fig.1).

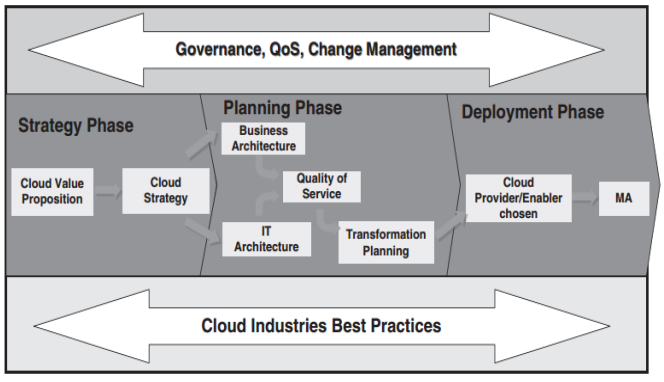

Figure 1. Cloud computing methodology overview

Condition needed to achieve customers' target, and then will establish a strategy to function as the guideline.

OBJECTIVE OF THE RESEARCH:

The main objective of the research is to develop a cloud computing environment to provide maximum security and privacy to achieve greater agree with of users to shift on a cloud. The specific sub objectives are, to broaden an at ease mechanism for cloud computing, which growth the security and privateness of the person in cloud offerings.

SCOPE OF THE RESEARCH:

IT industries are very much interested to switch over to Cloud databases to provide efficient services for their clients. The cloud database as a service is a Novel paradigm which could support several Internet-primarily based programs, the current trends in security and scalable database architectures are not reliable for efficient database services, Hence solving the issues of security and scalable database architecture is vital in national and international level.

II. LITERATURE REVIEW

1. Jean Raphael Ngnie Sighom, Pin Zhang and Lin You (2017) discuss some of these approaches and evaluate the popular ones in order to find the elements that affect system performance. Finally, we will propose a model that enhances data security and privacy by combining Advanced Encryption Standard-256, Information Dispersal Algorithms and Secure Hash Algorithm-512. Our protocol achieves provable security assessments and fast execution times for medium thresholds[1].

2. Kire Jakimoski (2016) proposed a method in which many security issues have been considered in order to enhance the data security in the cloud computing like appropriate use of administrative privileges, wireless access control of the data in systems that use wireless networks, boundary defense and data recovery in the cloud[2].

3. Sultan Aldossary, William Allen (2016) presented about the troubles which might be preventing humans from adopting the cloud and give a survey on solutions that have been made to decrease the dangers of those troubles. For instance, the statistics stored inside the cloud want to be exclusive, retaining integrity and available. Moreover, sharing the statistics saved within the cloud amongst many customers remains a difficulty since the cloud provider issuer is untrustworthy to

control authentication and authorization [3]. They additionally indexed some troubles associated with data saved in cloud storage and answers to those problems which vary from other papers which recognition on cloud as general[5].

4. G. Ranjith, J. Vijayachandra, P. Sagarika and B. Prathusha (2015) proposed a public auditing scheme in which the codes are regenerated primarily based on statistics garage [7]. They targeting privacy public auditing processes and algorithms that helps regenerate code based totally facts garage, which enables the auditing scheme that consists of a setup, audit and repair and additionally dangers, threats and attacks that prevent the auditor from detecting the data losses and corruption.

5. Nisha Bawaria, Kamlesh Namdeo, Pankaj Richhariya (2015) offered a method for access control and identification control for the cloud environment in some way to fulfill the contemporary protection demanding situations and provide a trustful surroundings for customers in addition to a service provider. Diameter-AAA provides authentication, authorization and billing offerings and is likewise able to handle identity attributes based on multiple different domains. They used it as a global authentication server, which may be carried out as principal and a comfortable authentication gadget that handles multi cloud environment as well as the single cloud service company[8]. The comparable draft is likewise partially available as an internet draft.

6. Shweta Dinesh Bijwe and Prof. P. L. Ramteke (2015) Delivered a brand new transactional "database-as-a-carrier" (DBaaS) called Database/Relational Cloud. A DBaaS guarantees to move an awful lot of the operational burden of provisioning, configuration, scaling, performance tuning, backup, privateness, and get right of entry to control from the database users to the service operator, supplying lower average expenses to customers. Database as a provider has several important troubles and issues, together with facts Scalability, Elasticity, Availability, Security, expectation problems[9]. Proposed answers consist of chance management, higher contractual agreements, database encryption, and authenticity strategies. By bettering this case, the DBaas service in cloud computing is effective to manipulate nowadays's massive developing facts units.

III. EXISTING SYSTEM

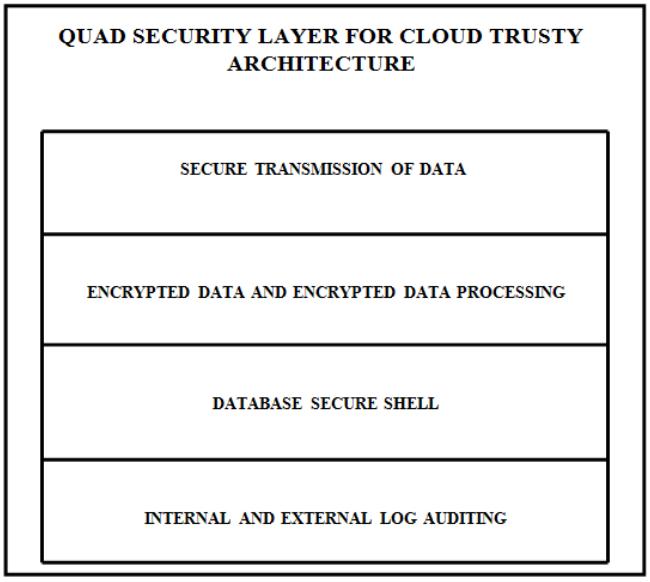

Figure 2. Existing System Architecture.

The above figure explains the existing system in which the Quad security layer for cloud trusty architecture is used.

A. Secure Transmission of Data

Initially, data is encrypted and then merged with the fake data stream to create confusion. It will be merged in different data benches[6]. This generated stream is transmitted to the receiver. On the receiver side, first data will be extracted from data benches from a specified location and then data stream will be collected.

B. Encrypted Data and Encrypted Data Processing

In this manner the user is sending data at client side, the data will be encrypted and merged with fake data to make secure stream for transmission. This secure stream is received at cloud side. After receiving this stream, the original encrypted data will be extracted. This encrypted data will be processed with encrypted data stored in the database. After processing, this encrypted data will again merge with fake data and this secure stream will be sent to the client. At client side the secure stream will be received and original data will be extracted. The extracted data will be finally decrypted, and presented to the user [10].

C. Database Secure Shell

In this manner the Server will communicate for data access through database with the help of Secure Access

Gateway. The Secure Access gateway will keep record of each query for data by using different Log Stamps like Time Stamp, Identity Stamp, Network Address Stamp, Location Stamp, Application Stamp etc. The Secure Access Gateway gets the request from Server and according to this request, the data will be provided to the server. Each time the server requests for any query from the database, the Access Log Stamps will be maintained. This Access Log Stamps will be used for auditing in the next layer. This will increase the data security, because only Access Logs Stamps are accessible for Auditing[5].

D. Internal and External Log Auditing

- **Internal Auditing**

In Internal Auditing the organization will perform an audit by their appointed or hired auditors. There are two types of such auditing. One is Interim audit and the second is Final Audit. The Interim audit will be conducted regularly and after a specific time span. Like after every Quarter (3 Months). The final audit will be conducted annually.

- **External Auditing**

An external audit the user will audit his logs by himself or any hired auditors. The user can inspect activities on the basis of logs that either the data is accessed by authorized person. The user can realize the data breaches on the basis of access time, access location and access network. This will make cloud computing more reliable and trustworthy for any user. As the cloud is much facilitated service, but the user doesn't rely on cloud computing due to data breaches. This fact is affecting on growth of cloud computing.

DEMERITS OF EXISTING SYSTEM:

There might be a chance for the intruders or attackers stealing the data over the cloud. TO reduce this chance of stealing the data, the proposed system is done.

PROPOSED SYSTEM:

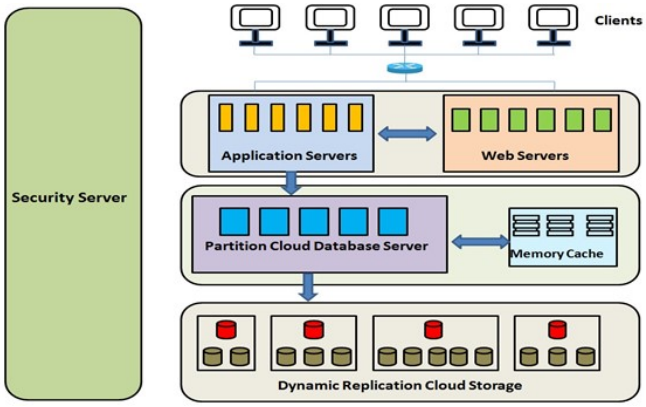

Figure 3. Architecture of proposed system

The above figure shows the architecture of the proposed system for secured cloud storage.

COMPONENTS OF PROPOSED SYSTEM

The proposed system consists of following components

- Application servers
- Web servers
- Partition Cloud database servers
- Memory cache
- Dynamic Replication Cloud Storage
- Security Server

PROCESS FLOW

The client or user sends an HTTP request to access the cloud database service through the server. The webserver such as Apache tomcat or Glassfish handles the HTTP requests from clients and send the user details to the user authentication server.

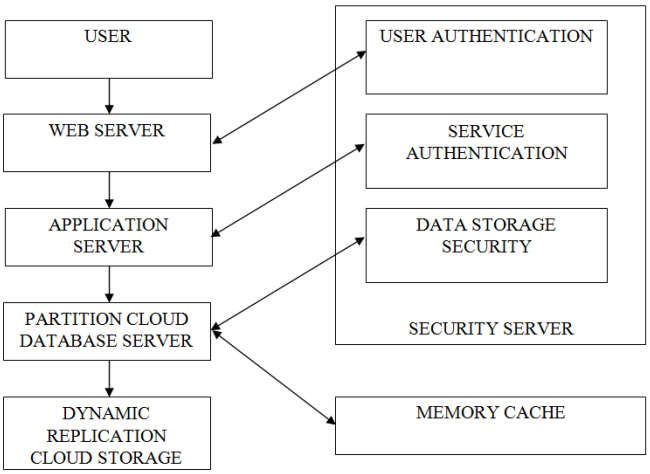

Figure 4. Flowchart for the proposed system

The user authentication server will verify the user details with the help of public key infrastructure, whether the given user is a valid person or not. If the user details is not valid then the web server will access the application server. After the validation , web server requests the application server. The application server refer the service authentication service before executes the specified application logic. The service authentication verifies the service level agreement between the cloud vendors and cloud database providers.After the service authentication, the partition cloud database server partitioned the database logically and each partition is controlled by a separate cloud database server.This server has one cloud database server which controls the whole database. An enhanced elliptical curve cryptography based Public Key Infrastructure(PKI) is used for the certification procedure to provide a secured cloud storage model.

The results of database queries are stored in dedicated cache servers. Typically, these servers keep the query results in their main memory so that accessing the cache is as fast as possible. Cheap machines can be used for caching. Furthermore, adding and dropping MemCache machines is trivial at any point in time. Each database server controls a copy of the whole database. The most important design aspect of replication is the mechanism to keep the replicas consistent. The replication is transparent and the storage is associated to the database servers.

IV.CONCLUSION

This proposed architecture proposes a dynamic and scalable architecture for cloud database services and provides complete protection on data security, data privacy and data breaches on cloud computing with the help of Public Key Infrastructure. PKI executes the service without loss of any part of the data and provide strong Scalable and secured database services in a cloud environment.

V. REFERENCES

[1]. Jean Raphael Ngnie Sighom, Pin Zhang and Lin You, "Security Enhancement for DataMigration in the Cloud", 2017.

[2]. Kire Jakimoski, "Security Techniques for Data Protection in Cloud Computing", 2016.

[3]. Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", 2016.

[4]. Jyotika Chhetiza, Nagendra Kumar, "A Survey of Security Issues and Authentication Mechanism in Cloud Environment with Focus on Multifactor Authentication", 2016.

[5]. Jianfeng Wang, Xiaofeng Chen," Efficient and Secure Storage for Outsourced Data: A Survey", 2016

[6]. M. Omer Mushtaq, Furrakh Shahzad, M. Owais Tariq, Mahina Riaz, Bushra Majeed, "An Efficient Framework for Information Security in Cloud Computing Using Auditing Algorithm Shell (AAS)", 2016.

[7]. G. Ranjith, J. Vijayachandra, P. Sagarika and B. Prathusha, "INTELLIGENCE BASED AUTHENTICATION - AUTHORIZATION AND AUDITING FOR SECURED DATA STORAGE", 2015.

[8]. Nisha Bawaria, Kamlesh Namdeo, Pankaj Richhariya, "High Performance AAA Security for Cloud Computing in Hierarchical Model", 2015.

[9]. Shweta Dinesh Bijwe, Prof. P. L. Ramteke, "Database in Cloud Computing - Database-as-a Service (DBaas) with its Challenges", 2015.

[10]. Anjali Nayak, Dr. Sadhna K Mishra, "Secure Architecture Using Multiuser Key Distribution for Cloud Database", 2015.