SECURITY ISSUES OF MAINTENANCE FOR CLOUD DATABASE: AN ANALYSIS

Swati V. Khidse[1], Dr. Santosh S. Lomte[2]
[1]PhD Student, [2]Principal, VDF School of Engg. & Tech, Latur, Maharashtra, India.
[1]Department of Computer Science & Engineering,
[1]Dr. B. A. M. University, Aurangabad, Maharashtra, India.

Abstract*—In cloud computing technology, user can store large amount of data in cloud database. Users can use resources as and when required, share resources between different computers and other devices by means of the internet. Because of this flexibility it is becoming very significant. As a result, cloud computing technology has recently become a new model, by which services are delivered over the internet. In cloud computing, resources are shared between different computers and other devices by means of the internet. There are many issues, which have been observed in a cloud database environment that need to be addressed. These issues can be: Security, Protection, Identity Management, Management of resources, Management of Power and Energy, Data Isolation, Availability of resources and Heterogeneity of resources. The first point of security, in cloud computing is secure storage. This paper presents an analysis of the challenges and key aspects of security issues of maintenance for cloud database.

***Index Terms*—Security, Authentication, Authorization, Provenanceability, Confidentiality, Cloud Database**

I. INTRODUCTION

Cloud computing is a newly emerging technology for the future, with its roots based on the rapidly increasing demands on data centers that need to be catered to. It is defined as the use of computing resources to access data over the internet. It is a mechanism to enhance the existing capabilities of Information technology.

National Institute for Standards and Technology (NIST) [1] defined cloud computing as "a model, which can enable conveniently the network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, Applications and services) on demand, that can be rapidly provisioned and released with minimal management effort or service provider interaction". Figure 1 illustrates the essential proprieties and main aspects of this new paradigm [1].

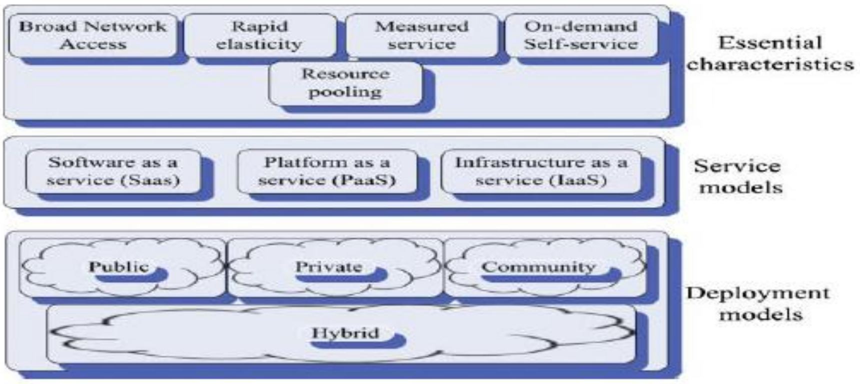

Fig. 1: NIST Definition of cloud computing

Cloud computing technology will change the entire scenario of the IT industry in future. It is cost efficient approach, with reduced exigency of buying the software or the hardware resources. It is an on demand form of utility computing. Recent search trends have shown a paradigm shift towards cloud. According to Google search trends here has been an immense increase in people's interest towards cloud computing from 2005 to 2013, as shown in Figure 2.

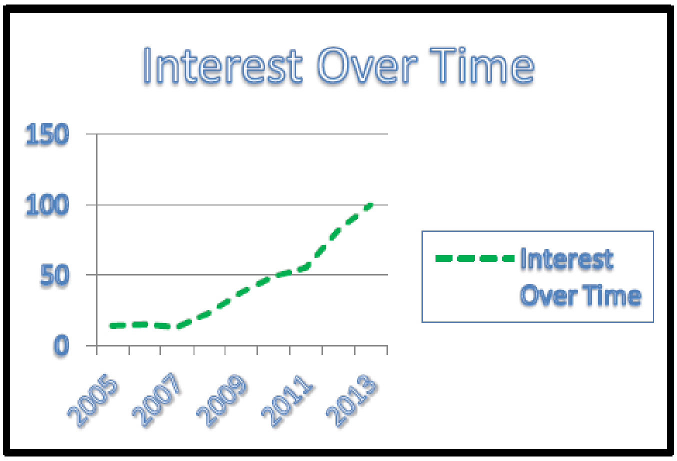

Fig. 2: Google Search Trends for last 8 years

Cloud database

Database is the core of nearly every application. Whenever an application performance or availability problem arises, there's a good possibility it's related to the underlying database's performance. Database performance impacts their users. The cloud developers and other moves in technology are making entire IT department more application-focused. But at the end, applications are what matters to the business organization and to end users.

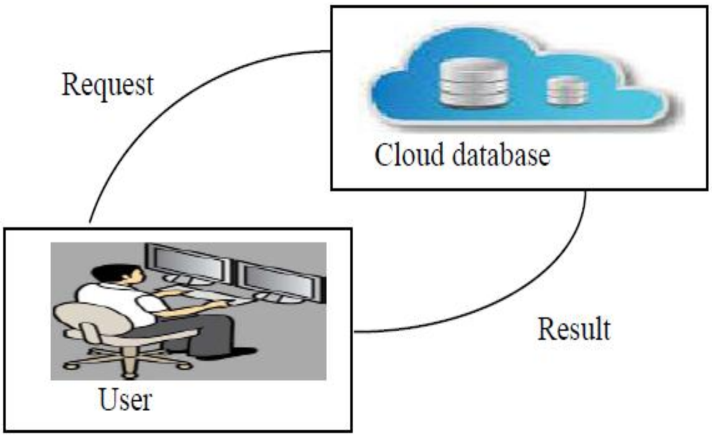

Fig. 3: Basic idea for cloud database as a service

II. SECURITY IN CLOUD COMPUTING

According to NIST cloud computing involves virtual environment which exposes cloud data to several vulnerabilities and threats. Although cloud computing provides advantages but at the same time imposes a great amount of threat to security of data which is stored off premise rather than on-premise [2]. Some of the top threats identified are:

a) Data Loss/leakage
b) Insecure API's
c) Malicious Insiders
d) Traffic Hijacking
e) Abuse of cloud computing
f) Unknown Risk profile
g) Shared Technology vulnerabilities
h) Distributed denial of services
i) HTTP or XML based denial of service attack

III. CLOUD DATA BASE MANAGEMENT SYSTEM

DBMS on the cloud can be of varied forms from relational [2]. For example Google's big table is not relational; Microsoft SQL Azure is a fully relational DBMS. Cloud DBMS is a distributed database that enables computing resources to be made available as service via internet rather than as a product. In cloud DBMS applications are connected to database which is available on cloud. Some key responsibilities of cloud service provider of data are:

a) Scalability
b) Data replication
c) Recovering from failure
d) Allocation or reallocations of servers
e) Availability
f) Privacy
g) Securing data
h) Metering
i) Service availability across geographical locations
j) Simple APIs
k) Operational ease

IV. SECURITY AND PRIVACY ISSUES OF CLOUD DATABASE

Cloud database is a novel approach that seeks to ensure scalability, availability and cost saving. There are various security and privacy cloud storage issues [3] [4] [5] that are faced by users at enterprise level and individual consumer during the use of the service. Most of the issues are related to the security of the data in the cloud. This problem should be ensuring for significant cloud usage businesses.

Integrity

In general, it seeks to guarantee the consistency and accuracy of user data stored in cloud database. Consequently, it aims at preventing unauthorized users from changing sensitive information. To accomplish this objective, various techniques are used, such as encryption, checksums, etc. Furthermore, it is vital to deploy permissions and access control tools. To enhance security, backup is also used to store the affected data.

Confidentiality

Confidentiality is used to protect user information from unauthorized users. Only authorized users can have access to sensitive data. In cloud database, user data should be kept secret against the cloud provider himself. For that, user's data need to be encrypted before transmitting them to the cloud database. Several cryptographic techniques are used to achieve this purpose.

Authentication

This technique seeks to determine and validate user's identity. The authentication server entails users to provide their identification information (login and password). It should be match to the stored credential. Authentication guarantees that only authorized user have access to cloud database, it is fundamental mechanism of access control.

Authorization

The objective of this process is to secure access to the cloud database. For this, it defines and specifies access rights to services, resources and activities. As a result, it denies and grants access to users' data. Thus, cloud providers deploy a security policy to guarantee that all users within an enterprise comply with security rule requirements.

Availability

Users should have access to cloud database anywhere and anytime. Many factors affect the availability of the delivered service: for e.g. Denial of service (DoS), network deficiency, etc. Cloud provider use multiple techniques to overcome this problem: load balancing, fault tolerance techniques and replication.

Auditing

It provides full visibility into database activities. So, it is essential to record all the events that happen within a database system. For achieving this goal, monitoring tools are used to create a report. It contains mainly vital information used to determine when and by whom database' objects are accessed or modified.

V. SECURITY ISSUES OF MAINTENANCE FOR CLOUD DATABASE

There are several security issues of maintenance for cloud database [5] [6] [7] which need to be concern for efficient working of cloud computing environment. Some issues are discussed here.

Provenanceability

It refers to virtual machine provenance mapping. By building VM background tree makes it easy to get information about its parent image. Basic objective is to gather information about creating a new image, modifications, vulnerabilities, etc. in cloud computing environment. This can be used for tracing malicious actions of illegal content inside VM image.

Encryption and Key management

Data leakage in cloud computing can be prevented by using encryption technique. Before storing data in cloud database, it is encrypted using encryption algorithm. User having the correct key of encryption algorithm will able to see the correct data. Key management is difficult in cloud computing. It is having several issues like: storage and safeguarding of keys and trusted cryptographic services.

Data and Storage

Cloud computing platform aimed at providing cost-efficient computational resources. Clients' data reside on servers that can belong to different data centers. It is major source of multiple challenges: resource provisioning, load balancing, job scheduling and scalability. Migration to cloud computing has several security risks [8]: multi-tenant environment, data backup, improper media sanitization and data recovery vulnerability.

Log file collection of all access

It refers to collection of all the access log to the cloud database i.e. authorized access and unauthorized access. When the access is authorized the user will have access to their data in database. When an unauthorized person is trying to access the data, proper notification will be send to the authorized user of this activity.

Protection against attacks (Long term viability)

The cloud provider should provide safety measures in case of bankruptcy, Denial of Service attacks, Brute force attack etc. In such situations customer's data should be available and it should be in the last safe state.

Trust

There should be agreed guideline between service provider and the user. So that user will have trust on cloud provider that the data provided is correct and it is not leak anywhere in the cloud storage.

Isolation

It refers to complete seal of user's data inside the cloud computing environment. Because of multi-tenant environment, cloud computing resources are at the risk of information disclosure. Thus there is a need for strong isolation in cloud environment.

Virtualization

In cloud computing several virtual versions of the same physical resource, such as server and device are created. Various operating systems and applications can run on a single physical server, thus reducing operating costs while enhancing performance and reliability. It has some outstanding features: scalability, fault tolerance, and storage migration. Virtualization technique brings security problems: VM image sharing, VM isolation, VM escape, Hypervisor issues and VM migration.

Web Technology

Cloud providers rely on web-based technologies for offering remote services to their clients. Computational resources are accessible via the Internet. Clients use application programming interfaces (APIs) to manage and gain access to cloud resources. APIs enable clients to connect application-layer with clouds. On the other hand, APIs brings risks and security challenges :Injection SQL, Cross-Site Scripting (XSS), broken authentication and session management, Cross-Site Request Forgery (CSRF), etc [4].

Network Security

In cloud computing, data is flowing over the network (internet). It is prone to hazardous circumstances and network issues. Network failure reasons can be: misconfiguration, lack of resource isolations, network traffic modification [9].

VI. CONCLUSION AND FUTURE SCOPE

Cloud database aims at reducing operating costs and improving availability and reliability. As a result, this technology has penetrated the public and private organizations due to its advantages. It provides a scalable structured repository for storing and managing data. Cloud computing offers advantages, but still organizations are very reluctant to store their data on the cloud. One of the biggest obstacle in the implementation of cloud computing is security of data. Cloud data security encompasses security constraints from end-user and cloud provider's perspective, where the end-user will be primarily concerned with provider's data security policy, how and where their data is stored, and who has access to the data. For a cloud provider, On the other hand, from cloud providers point of view- cloud computing data security issues can range from the physical security of the infrastructure, access control mechanism of cloud environment to the execution and maintenance of security policy. Cloud security is most important because, it is probably the biggest reason why organizations fear the cloud.

User's data is stored on cloud database. Like normal database, cloud database is also having several security issues. Certain security issues are concern over maintenance of cloud database. This need to be solved with proper care in such a way that it should not affect the overall performance and privacy of cloud database. This module can be integrated with the cloud architecture, thus there will be no need to depend on third party for the work to be done.

REFERENCES

[1]. Peter Mell ,Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology U.S. Department of Commerce, September 2011.

[2]. Mansaf Alam and Kashish Ara Shakil, "Recent Developments in Cloud Based Systems: State of Art".

[3]. Anup Mathew, "Survey Paper on Security & Privacy Issues in Cloud Storage Systems," EECE, Term Survey Paper, April 2012, pp 1-13.

[4]. Jayalakshmi K, Uma K M, Veena A & Lavanya Santhosha, "QUANTITATIVE ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING," International Journal of Research in Engineering & Technology, Vol. 5, Issue 8, Aug 2017, pp.51-60.

[5]. Mbarek Marwan, Ali Kartit and Hassan Ouahmane, "Applying Homomorphic Encryption For Securing Cloud Database," 2016 IEEE, 978-1-5090-0751-6, pp. 658- 664.

[6]. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on Computer Science and Electronics Engineering, 2012 IEEE, pp. 647-651.

[7]. Christos Kalloniatis, Haralambos Mouratidis, Manousakis Vassilis, Shareeful Islam,Stefanos Gritzalis, Evangelia Kavakli, "Towards the desidn of secure and privacy- oriented information systems in the cloud: Identifying the major concepts," 2013 Elsevier, pp. 759-775.

[8]. Diogo A, Liliana F, B. Soares and Joao V. Gomes, Mario M, Freire, Pedro R and M. Inacio, "Security issues in cloud environments: a survey," International Journal of Information Security, Springer, April 2014, pp. 113-170.

[9]. Kashif Munir, "Security Model for Cloud Database as a Service (DBaaS)," IEEE, 2015, 978-1-4673.