Cloud Database Security: Issues and unique Challenges

Mr.Deshmukh Harshad[1], Mr.Sathe P.P.[2], Mr.Tathe S.N.[3]

[1]Student, Vishwabharati college of Engineering, Ahmednagar Maharashtra,India
[2]Student, Vishwabharati college of Engineering, Ahmednagar Maharashtra,India
[3]Asst.Prof., Vishwabharati college of Engineering, Ahmednagar Maharashtra,India

---

Abstract - Cloud Computing is a computing system-based model that provides users with convenient and customizable services to access various cloud applications. It provides a way to store and access cloud data from anywhere by connecting the cloud application using the internet. Cloud computing and related security issues are one of the widely discussed research questions of today's generation. In addition, the countermeasures listed in the survey must clearly illustrate the problem they address. we also provide a concept model. In addition, we address these issues to the extent they are relevant and provide two instances of vendors and security features that have been used for cloud databases. Finally, we provide an overview of the security risks associated with open cloud databases and suggest possible future paths. This paper also summarizes the most important security techniques for data protection and cloud security in cloud computing. In addition, data protection security techniques will be recommended to increase security in cloud computing. It will focus primarily on the issue of data security and provide solutions.

Keywords: Virtualization, Database security, Cloud computing, Cloud Security, security vulnerabilities, attacks.

1. INTRODUCTION

The adoption of cloud computing has been largely influenced by security concerns. Running software on a foreign hard drive and using a foreign CPU can be terrifying to many, as can the idea of putting important data there. Data loss, phishing, and botnets are examples of security issues that pose serious risks to an organization's software and data [2]. In addition, the multi-tenancy structure of the cloud computing model and shared computing resources have created new security risks (such as Botcloud Attack) that require innovative solutions.

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". Although cloud computing provides a way to store data on a remote device, it has many security issues that are very important today, including network security, data protection, application integrity, virtualization security and identity management Therefore, data security challenges when using cloud computing should be properly addressed and minimized.

The goal of this paper is to review the cloud security challenges from the set of controls, practices, policies, and technologies that work together to protect cloud systems, infrastructure, and data. As well as show the technologies configured by various studies to protect cloud data and protect individual privacy[11]. DBaaS, often known as cloud database, is a unique type of database designed for use in virtualized computing environments or cloud environments. Its primary purpose is cloud storage of large amounts of data [4]. Database as a Service (DBaaS) is emerging as a viable way to offer reliable and adaptable data storage services for cloud applications, given the diverse uses of cloud applications[5]. Problems with scalability, performance,

availability and costs are solved by cloud IT systems [6]. Cloud databases require more than setting up a relational database on a cloud server; they also require optimizing database performance and adding additional nodes online as needed. Microsoft SQL Azure, Amazon RDS and Apache Cassandra database are some prominent examples of DBaaS [7]. Relational or NoSQL databases can be used as a general type of database in cloud computing. Not only SQL or NoSQL databases are useful for large-scale applications for processing semi-structured and unstructured data, including big data [8]. The four primary models used by NoSQL databases to store data are document-based, graph-based, key-value-based, and column-based [8]. NoSQL databases are an excellent choice for cloud computing infrastructure because they are typically built to scale across multiple data centers and operate as distributed systems [9].

A network infrastructure is the structure of a cloud computing network, usually with many cloud components such as a message queue that cooperated within a free link [5]. Cloud computing architecture refers to virtual computer components and sub-components. Generally, these composites are frontend platform, backend, cloud system and network. There are also composites. The front and back ends are connected via a network, usually via an Internet delivery system.

The diagrams below gives a schematic overview of the cloud computing architecture Fig.1 shows Architecture of Cloud Computing:

• Frontend: This is the cloud computing platform that is part of the company. This includes interfaces and applications that are critical to the performance of cloud networks, such as a web browser.

• Back End: It is the cloud itself that has a back end. It includes most of the resources needed for cloud computing. This consists of large data stores, virtual machines, security systems and hardware.

- Server uses middleware-identified Protocol which help to communicate between connected

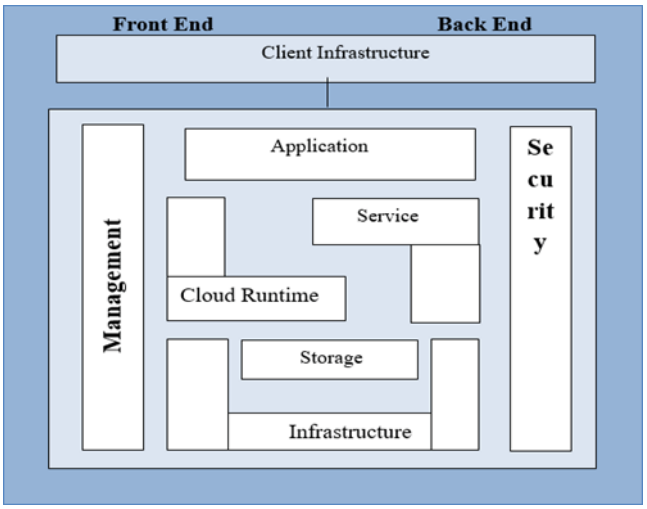

Fig -1: Architecture of Cloud Computing

2. CLOUD INFRASTRUCTURE

Networking includes servers, storage devices, networks and network management, implementation tools and software virtualization applications and these tools are required to support the computational requirements of the cloud computing model, Fig. 2 shows the cloud infrastructure Service.

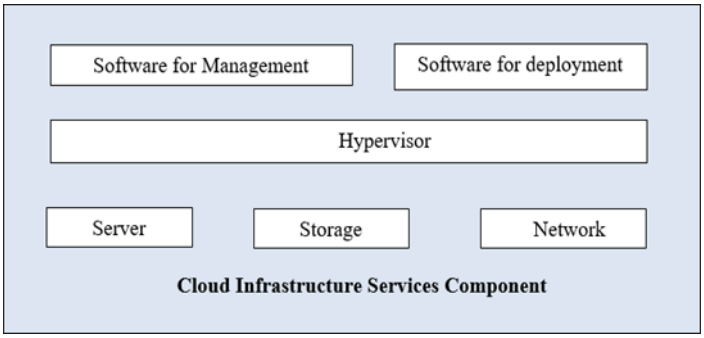

Fig.2. Cloud Infrastructure

1. Hypervisor: It is the software or low-level manager of the virtual machine. This allows multiple tenants to share individual physical instances of cloud services.

2. Management Software: Contributes to infrastructure maintenance and configuration.

3. Deployment software: It helps to install and integrate the program into the cloud.

4. Server: The server helps in measuring resource sharing and provides other services

such as resource allocation, resource management, security, etc.

5. Storage: Multiple storage replicas are stored in the cloud. When one device fails, one can be replaced and cloud computing secured.

6. Network: The most important part of cloud infrastructure. It enables the connection of cloud services to the Internet. The network can also be delivered as a service over the Internet, allowing the user to customize the network path and configuration.

3. CLOUD BASED DELIVERY

1. Software as a Service (SaaS):

The Software as a Service (SaaS) business model involves cloud providers who use and manage cloud software and clients who run the software over the Internet (or intranet) from their cloud. clients. There is no need to install any application-specific software for user client devices, so all cloud applications run on the cloud server. SaaS is flexible and multiple servers allow the server system administrator to load applications. SaaS typically costs a company or agency a monthly or annual fee.

2. Development as a Service (DaaS):

Web technology resources are usually shared together. It's the same as local development tools embedded in traditional (non-cloud) development tools.

3. Platform as a Service (PaaS):

Platform as a Service is a cloud service providing service to users of the operating system and databases. Middleware is similar to conventional (non-cloud) systems and servers.

4. Internet infrastructure as a service (IaaS):

Software and equipment in a conventional (non-cloud) model on the Internet are virtualized within their systems, all physical computers, all servers, networks and system management. Companies pay a monthly or annual fee to run virtual cloud servers, networks and storage to minimize the need to maintain the data center, environment and on-premises hardware. SaaS provides applications that match those installed in a conventional (non-cloud) application.

Data Security Challenges and Issues

Cloud computing security is a major issue that needs to be addressed these days. And data protection is the most important challenge in cloud computing [4]. Data loss can have a serious impact on an organization's brand, business and trust. If security measures for data operations and transmissions are not properly achieved, data is at high risk. The strongest security measures are to be implemented by identifying security issues and solutions to address those issues. Figure 4 shows the data security challenges and it is clear that data leakage prevention and data segregation and protection have a greater impact on security challenges. Therefore, to ensure the security of information and to ensure that data is not compromised by security vulnerabilities, cloud computing should implement additional security measures along with conventional security controls.

To improve security in cloud computing, it is important to offer authorization, authentication and access control to data stored in the cloud.

Security Issues Related to Other Data

Data location, multi-tenancy and backup in cloud computing have less data security concerns. The data is stored in a different geographic area of various cloud computing related to legal regulations. If the data is not logically and physically stable, CSC data is constantly at risk. If the physical and logical location of data is not secure, CSC data will always be at risk. In this situation, the data is vulnerable to malicious hackers and insiders. A multi-tenant cloud design allows multiple users in a physical or virtual storage model to store their data in the same location.

• For all possible administrative, contractual, and other jurisdictional issues, the CSC should know the rationale and physical location of the data, at least by city, state, and data center.

• Establish information location and jurisdictional policies.

• Isolate data from different users using intelligent data separation techniques.

• Use strong encryption

4. Cloud Database Structure

Cloud computing database environments exist in several variants. For example, some use a multi-instance architecture, while others use a multi-tenant approach. With the multi-instance feature, each user has access to a separate database management system (DBMS) running on a virtual machine (VM), giving them complete control over a number of security-related responsibilities. Whereas the multi-tenant model gives cloud users access to a pre-defined environment that they can share with other tenants – typically by assigning a unique user ID to each tenant's data. In the latter case, maintaining a secure database environment is the responsibility of the cloud service provider. The five-layer design of the cloud database management system was presented by the authors in, as can be seen in fig. 1. the five levels are the outer layer that interacts with users[14]. This is followed by a conceptual middleware layer that encapsulates the specifics of heterogeneity into a conceptual layer that uses several types of databases, including DB2, SQL, and Oracle. The conceptual layer takes care of data processing and replaces the overall logical structure of the database. The physical middleware layer hides the specifics of several heterogeneous platforms in use, including Windows, macOS, and Linux. The physical layer, which is the last layer, deals with how the data is physically represented.

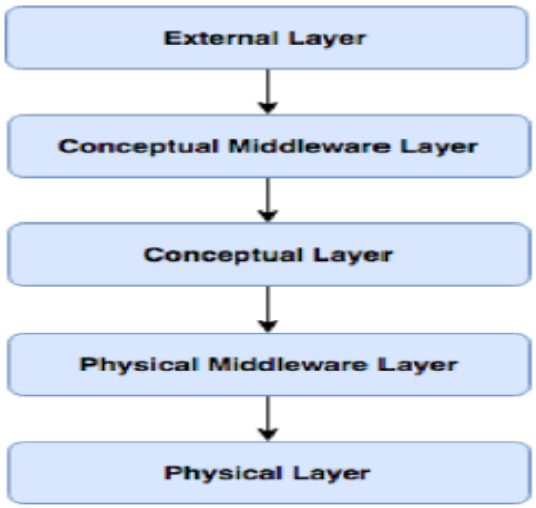

Fig.3 Cloud database management system

A cloud database allows data to be shared and distributed between multiple locations with the added benefit of authentic information and specific permissions. As a result, it is important to ensure data security, scalability and consistency. A cloud-based DBMS is needed to solve these and other data-related problems. In general, shared-nothing and shared disk are the two primary DBMS designs used in cloud environments. First, the shared-nothing distributed computing architecture is one in which each node is independent of every other node and can operate independently, meaning that each node has its own memory and disk storage without having to share them. Second, a computing design known as shared disk architecture combines memory on each node with shared disk storage[15]. As each database server processes and stores a portion of the database, it partitions the data. Since shared disk and shared nothing systems have drawbacks and problems, much work has been done on cloud database management system architecture.

5. Cloud database security and data protection challenges

The idea that DBaaS is a fantastic option for businesses with less financial resources has been discussed [14]. However, it can also lead to many security issues as a third party (i.e. the provider) takes over the maintenance of the database and its underlying security instead of the data owner. One of the main risks for data stored in cloud storage is security.

•**Data Confidentiality :** to ensure data protection from any attacks.

• **Data Integrity**: Users should not store their private data such as passwords to ensure integrity.

• **Data Availability:** depends on the agreement between the seller and the client.

• **Homomorphic En**cryption:- encryption is intended to protect data privacy; Rivest proposed homomorphic encryption. Cloud data operations and data confidentiality can be solved by implementing this encryption. It guarantees that the results obtained from the ciphertext match the results obtained from the

cleartext; moreover, this process does not require data decryption. A significant advance in this kind of encryption is that a completely homomorphic encryption approach can perform any action that can be performed on plaintext without the need for decryption.

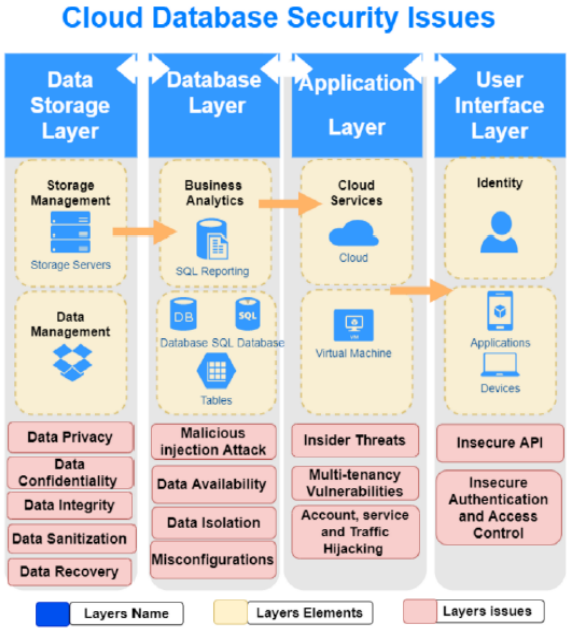

Fig.4 Conceptual model to find cloud Database security issues

6. CONCLUSIONS

In this paper introduced for finding database security issues in cloud and finding solutions based on the analysis and discussion of cloud database security challenges. Effective encryption: We desperately need strong encryption methods that are also suitable for cloud systems. The proposed algorithms should reduce the delay by not placing a particular burden on the cloud activities. Confidentiality and integrity can be protected with proper encryption techniques. Enhanced privacy plans: With all cloud services, privacy is a top priority. There needs to be more privacy protection programs. These programs should protect client data and mitigate any wrongdoing by service providers. Extended Trust Programs: Most cloud users are concerned about how much trust they can place in cloud service providers. As a result, it is crucial to increase the level of trust by getting the help of a third party appropriately.

REFERENCES

[1] Curino, C., et al., Relational cloud: A database-as-a-service for the cloud. 2011.

[2] R. V. Rao and K. Selvamani, “Data security challenges and its solutions in cloud computing,” Procedia Comput. Sci., vol. 48, pp. 204–209, 2015.

[3]Mongo, D., Nosql databases explained.

[4]Hussain, S.A., et al., Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 2017. 13(1): p. 57-65.

[5]Marko Hölbl (2011). Cloud Computing Security and Privacy Issues, Council of European Professional Informatics Societies(CEPIS), pp 1- 4

[6] Robert Koletka and Andrew Hutchison (2011). An Architecture for Secure Searchable Cloud Storage, IEEE Information Security South Africa (ISSA), Johannesburg, pp1-7

[7] Sun, Y., et al., Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 2014. 10(7): p. 190903.

[8] Boneh, D. The decision diffie-hellman problem. in International Algorithmic

[9]L. Arockaim, S. Monikandan (2014). Efficient Cloud Storage Confidentiality to Ensure Data Security, IEEE International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, pp 1-5

[10] L. Arockaim, S. Monikandan (2014). Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage, International Journal of Current Engineering and Technology, vol. 4, pp 1265-1270

[11] Izang, A., et al., Security and ethical issues to cloud database. Journal of Computer Science and Its Application, 2017. 24(2): p. 65-75.

[12] Malhotra, S., et al., Cloud Database Management System security challenges and solutions: an analysis. CSI transactions on ICT, 2016. 4(2-4): p. 199-207.

[13] Kumar, P.R., P.H. Raj, and P. Jelciana, Exploring data security issues and solutions in

cloud computing. Procedia Computer Science, 2018. 125: p. 691-697
[14]Sun, Y., et al., Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 2014. 10(7): p. 190903.
[15] Boneh, D. The decision diffie-hellman problem. in International Algorithmic Number Theory Symposium. 1998. Springer.
[16] Kaur, A. and M. Bhardwaj, Hybrid encryption for cloud database security. Journal of Engineering Science Technology, 2012. 2: p. 737-741.