CLOUD DATABASE CONCERNS AND COUNTER MEASURES

[cloud computing concerns and counter measures]

[Sai Nishit Reddy Pabbathi]

Purdue University Northwest

**Abstract**

Cloud computing is a powerful computing platform that allows individuals and companies to conduct a range of functions, including the usage of online storage space, the adoption of business apps, and more. Customized computer program development, as well as the building of a "realistic" network environment In previous years, the number of people using cloud services has skyrocketed, and massive amounts of data have been generated. Cloud computing environments have been used to store data. Meanwhile, data breaches to cloud services are becoming more common. Hackers who are always seeking to exploit the security weaknesses of the internet cause the number of attacks to rise every year. Six security concerns were addressed in this research; cloud security risks and threats were investigated. Countermeasures to security breaches in the cloud are discussed. According to DataLossDB, there were 1,047 data breach incidents during the first nine months of 2012, compared to 1,041 incidents during the entire year of 2011[1]. Hackers could also utilize cloud computing's immense computer capacity to launch attacks against users on the same or separate networks. For instance, hackers rented a server through Amazon’s EC2 service and carried out an attack to Sony's PlayStation Network [2]

**Keywords**

Cloud, cloud database, cloud security threats and countermeasures

**Introduction**

A cloud database is a database service that is produced and accessible via the internet. It performs many of the same tasks as a traditional database, but with the extra benefit of cloud computing flexibility. To implement the database, users install software on a cloud infrastructure. A cloud database is a database that runs on a cloud computing platform and provides as-a-service access to the database. Users can run databases on the cloud themselves using a virtual machine image, or they can pay for access to a database service provided by a cloud database provider. Some of the cloud databases are SQL-based, while others use a NoSQL data format. Database services ensure the database's scalability and high availability. The underlying software stack is transparent to the user thanks to database services. The majority of database providers provide web-based consoles for users to provision and configure database instances. Database services are made up of a database-manager component that uses a service API to govern the underlying database instances. The end user can access the service API, which allows them to perform maintenance and scaling actions on their database instances. The operating system, database, and third-party software required to manage the database are often included in the underlying software-stack stack. The service provider is in charge of installing, patching, and updating the underlying software stack, as well as maintaining the database's general health and performance. Vendors differ in their scalability features; some offer auto-scaling, while others allow users to scale up using an API but do not scale automatically.

 There's no denying that cloud’s convenience and low cost have transformed the game. our daily lives; nonetheless, the security concerns around cloud computing cause us concern.   Every day, you're vulnerable to cybercrime. Hackers use a variety of methods to gain access to computers. Gain unauthorized access to cloud services or interrupt cloud services in order to attain certain goals Hackers may be able to persuade a cloud to treat their unlawful activity as legitimate. As a result, illegal access to information stored in the cloud is possible.

**cloud security threats and countermeasures**

**Possible Threat Types**

Many of the same dangers that impact cloud technology also harm cloud database systems. However, due to the nature of enormous amounts of potentially sensitive data being held in databases, the consequences can be serious if left unchecked. While not exhaustive, these vulnerabilities provide an indication of the types of challenges that network managers will face as firms embrace large-scale cloud database storage systems.

**Data breaches**

As reported in the media, data breaches are likely the most common hazard to cloud databases. Hackers get access to sensitive data stored in the cloud, such as consumer credit card details or mailing addresses, and use it for personal benefit in a data breach. Data breaches are becoming more catastrophic as more information is stored online in a single area, possibly harming millions of customers or employees at once. n, Data being purposely or accidentally deleted or modified by a user or an attacker, Data stolen over the network by network penetration or any network intrusion attack, Data storage device physically damaged or stolen, Virus infection deleting one or more files[3].

**Account hijacking**

In a hijacking attempt, intruders attempt to obtain access to a user's account through phishing or exploiting security flaws in software. When burglars steal a user's account login credentials, they frequently change the password to lock them out of their accounts. Any files or other information saved in the user's cloud can now be accessed without restriction, including database information that offers data on multiple users at the same time.

**APIs**

The technical means by which a user communicates with a cloud system, governing what permissions he or she has to attach third-party applications to the system, is known as an Application Programming Interface (API). Service provider demonstrates all the APIs that are utilized by the customer to connect with the cloud. Information course of action, personality administration, service checking, all happen on the cloud. Validation and get to control is inspected by these interfaces [4] While cloud storage businesses and other Internet entities have made significant progress in building safe APIs, such as OAuth, an intruder might still exploit flaws to get access to administrator API areas**.**

**Data loss**

When an attacker acquires access to sensitive information, one conceivable conclusion is that the intruder will erase it to inconvenience the owner. If users do not retain up-to-date backups of their files, they may be permanently lost if they are tampered with. When all files are hosted on a single cloud-based server, deletions can spread to all user devices, resulting in files being lost all at once.

**Cloud servers as malware platforms**

Cloud computing's synchronization services are clearly beneficial for maintaining database files across devices and platforms. What if, on the other hand, an attacker decides to exploit the same synchronization method to concurrently spread malware across all user devices? If attackers can use cloud servers to transmit malware across a network, the damage they can cause is significantly higher than if they could only affect a small, locally stored organization network.

**Reducing Risk**

Although the risks associated with cloud databases are frightening, understanding them can help users minimize potential damage. These broad methods provide recommendations to system administrators on how to handle cloud database security in order to protect the network from intrusion scenarios.

**Understand your network**

Administrators must have a thorough grasp of where and how sensitive information is stored on the network. Each sort of network data should be categorized and labelled, including log files and data embedded in documents. Administrators should check and understand access rights so that each file type can only be accessed by the appropriate people.

**Secure network data**

Building on the preceding concept of access rights, the following step entails determining how much data each sort of user is allowed to see. Only the specific data owner should have full access, with sensitive sections designated for all other user categories. To secure user data from unintended access, encryption and masking techniques are utilized, as well as partial viewing in some circumstances (such as seeing only a select few digits of an account number online, for example).

**Monitor the network**

Effective network security teams are proactive, always scanning system security policies and logs for exceptions that could indicate data misuse. Semi-annual security audits should be conducted to provide a more systematic and structured look at how information is used and what defensive procedures are in place. Understanding what network vulnerabilities you have and how hackers could exploit these flaws for personal benefit is often the strongest defense against incursion.

**Utilize security intelligence technologies**

SIEM (Security Intelligence and Event Management) technologies are meant to allow for active network monitoring and the detection of defensive system flaws. These technologies provide continuous system analysis and can be used to detect potential security breaches in real time. While SIEM should not be used to replace individual monitoring, it can be used to enhance manual searches and provide a more comprehensive picture of network health.

**Conclusion**

Cloud computing is constantly evolving in order to provide customers with various levels of on-demand services. While many people appreciate the advantages of cloud computing, cloud security is a major concern. Clouds still have a lot of vulnerabilities, and hackers are continually exploiting them. Security issues must be detected in order to provide better service to cloud users. The security vulnerabilities in clouds were explored in this article, and countermeasures to those security breaches were introduced. We will continue to contribute to cloud research efforts in the future. security threats and defenses against cloud security breaches.

**Reference**

1. DataLossDB Open Security Foundation. http://datalossdb.org/statistics

2.Amazon.com Server Said to Have Been Used in Sony Attack, May 2011. <http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackersusing-amazon-com-server.html>

3. <https://www.techopedia.com/definition/29863/dataloss>.

4. Jitender Grover, Shikha, Mohit Sharma, 2014,IEEE 5th ICCCNT, “Cloud Computing and Its Security Issues – A Review”.