Cloud Database Security issues: A Review

Mohamed Razeed Mohamed Nowfeek

Department of Information Technology
Advanced Technological Institute
Sammanthurai.

nowfeekmit@gmail.com

Abstract

The newest advancement in the IT sector is cloud computing, commonly referred to as on-demand computing. Because of features like accessibility, scalability, and others, this technology is attracting a variety of organizations. In addition, there are significant security issues in cloud databases. In this work, we describe how to overcome several security issues in cloud databases, such as trust, authenticity, confidentiality, encryption, key management, multitenancy, and data splitting. Furthermore, cloud database as a way of improving the services of the cloud service providers when deployed.

Keywords: *Cloud Computing, Privacy, Security, Cloud Database*

INTRODUCTION

The concept of cloud computing implements with the advancement of the communication, digital data processing and changes in storage requirements. Simply described, using a network of remote servers connected to the internet, cloud computing is a method for processing, storing, and managing data on demand while only paying for what you really use. It provides access to a pool of shared resources instead of local servers (Ahmed and Hussan, 2018). Basically, the cloud service providers provide different cloud services to its users.

When using cloud computing, data is dispersed across several places as resources that may be accessed remotely by various users throughout the cloud. In cloud infrastructure, robustness and secure computing are extremely important. Any organization that tries to store data either on host files or on a public cloud loses the ability to have physical access to the servers housing its own data. This makes potentially sensitive data susceptible to insider assaults. Insider attacks are ranked as the sixth highest threat to cloud database, according to a recent report from the Cloud Security Alliance. Persons with physical access to data center servers must undergo extensive background checks in order to prevent dangers of this nature. Data centers must be regularly checked for any suspicious activity.

Architecture of the Clouds

Software as a Service (SaaS): This model gives browser-based software applications over the Internet. The client is not allowed to change the Infrastructure (operating systems, servers, storage and network). (Eugene, 2013)

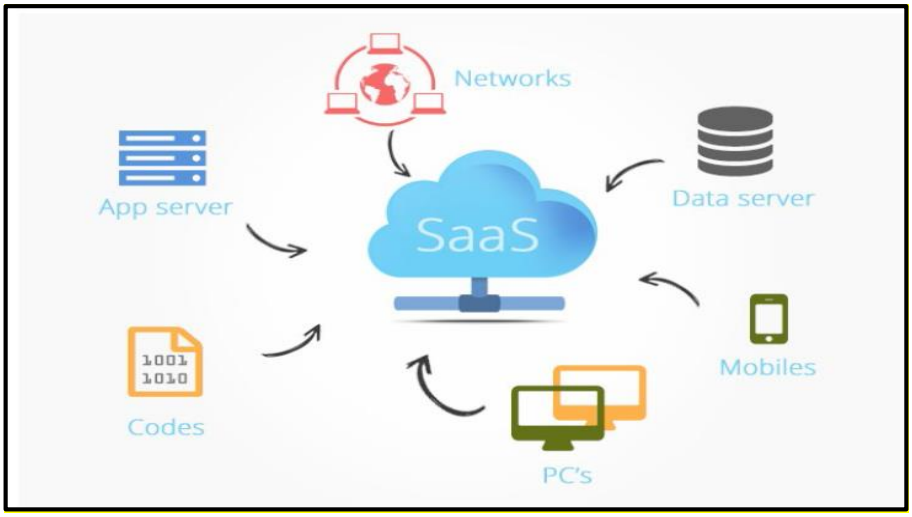

Figure 1. SaaS

Infrastructure as a Service (Iaas): It gives an online administration access to assets, for example, handling disk space, limit, and many others. The client is given the permission to install software in that infrastructure (Eugene, 2013).

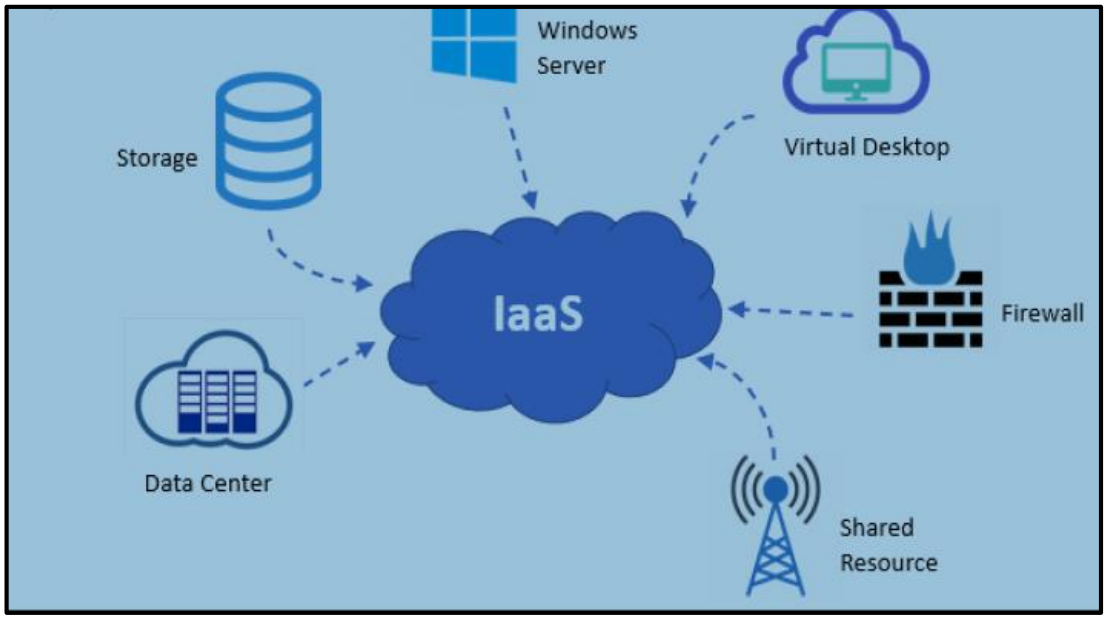

Figure 2: IaaS

Platform as a Service (Pass): In this model, developers are given an environment and platform empowering them to make services and applications accessible via Internet (Eugene, 2013).

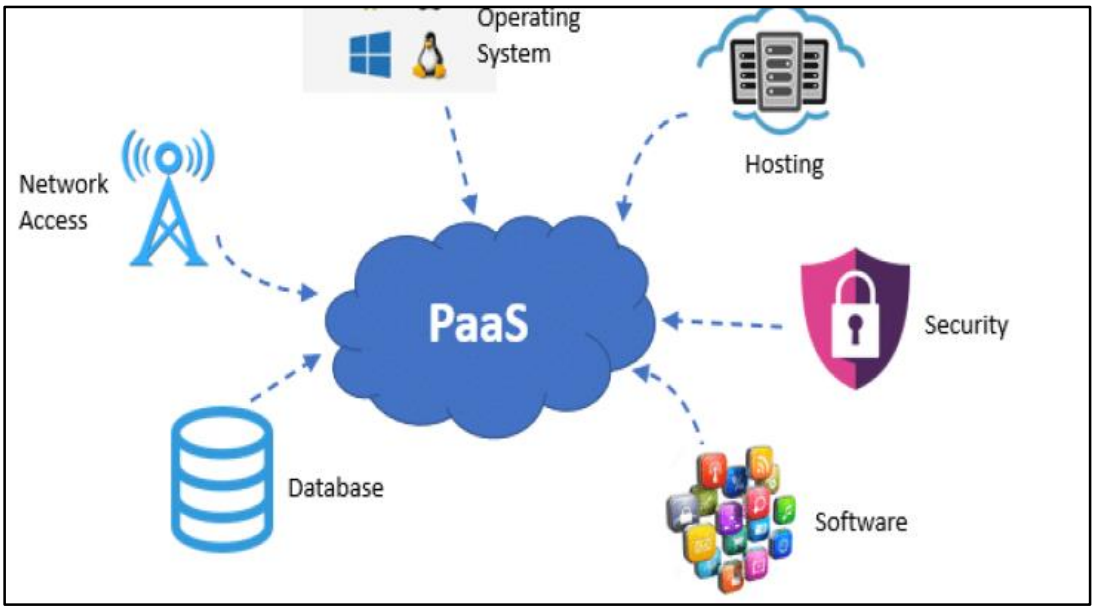

Figure 3. PasS

Database as a service (DBaaS): As a Service (DBaaS) is an operational and architectural paradigm that enables IT suppliers to provide database functionality as a service to a larger number of customers.

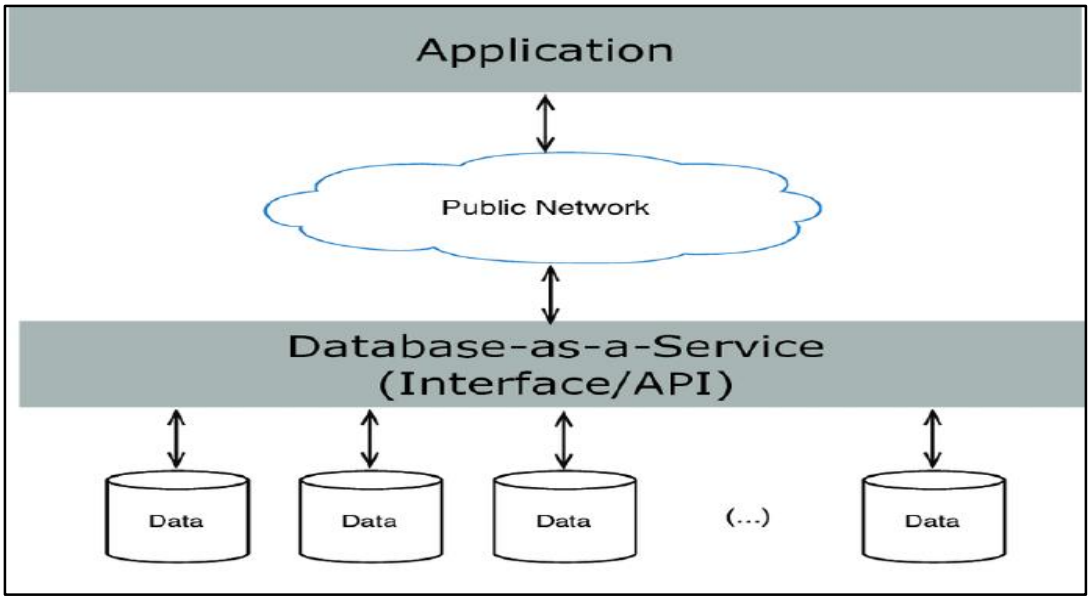

Figure 4. DBaas

Nowadays most of the industry-oriented people are focusing on the cloud database service. The term "cloud database" refers to a database service that is created and accessible using a cloud platform, performs the functions of a traditional database, and incorporates the most recent cloud computing technology. To implement the database, users may need to install software on a cloud infrastructure that they may access on demand.

Popular databases in cloud computing (Bhatti and Rad, 2017)

- StromDB
- PostgreSQL
- MongoLab

Google Cloud

- Google Cloud SQL
- GC Bigtable

- Google Cloud Datastore
- GC Spanner

Microsoft Azure
- MA Table Storage
- Microsoft Document DB
- Microsoft SQL Database
- Oracle Database
- IBM

Amazon
- DynamoDB
- Amazon Aurora
- Simple DB
- Amazon RDS

The reasons to move for the cloud database system are
- Virtual access, using a vendor's API or web interface
- Runtime capacity expansion of the database
- Flexibility to accommodate the changes
- Disaster recovery mechanisms

Since all those are positive measures it should be highly considered the security issues on the cloud databases. It is not possible to implement the security mechanisms as on traditional databases. Privacy, security, and ethical concerns are individually highlighted as three major difficulties in the cloud database paradigm, and there is yet no clear answer to address those concerns.

Database as a Service (DBaaS) has the following advantages:
- Flexibility to accommodate the changes.
- Cost savings
- Runtime capacity expansion of the database.
- Simpler, less costly management
- Software quality.
- Virtual access, using a vendor's API or web interface.
- Disaster recovery mechanism.

Although it is not possible to establish proper security methods as on traditional databases, it is possible that users should be worried about security issues on clod databases given that all of those are good actions. Security, privacy, and ethical concerns are examined separately as three common difficulties in the Cloud Database Paradigm, but no concrete solutions are identified to address them.

Literature Review

We are now talking about the security problems with cloud databases and the solutions that have been offered to fix them. The majority of researchers have researched the security concerns around cloud databases. They gave the means to address the problems to some extent by leveraging those facts. Let's look at a few research publications to gain a general sense of the security problems with cloud databases and how to solve them.

A. Cloud database security issues

Sharma and Sharma (2015): In this paper some obstruction and threat on the cloud database has been clearly analyzed and this paper gives privacy and security of cloud databases, possible attacks and the approach to make data secure on cloud databases. More probable attacks on the cloud database were described. SQL injection, cross-site scripting (XSS), man-in-the-middle attacks, denial-of-service attacks, and cookie poisoning are examples of such attacks. An adversary can completely take over the database for your web application by inserting arbitrary SQL code into a database query. An unauthorized person become able to get unauthorized access over the database stored in the cloud. Cross site scripting another malicious script in inserted into the actual web context which helped the enemy to gain the confidential information of the victim. Man, in the middle is tried to intrude between client and server to gain access of the data.

Izang, Adebayo, Okoro and Taiwo (2017): In this study reviewed the Ethical Issues in Cloud Computing and Cloud Databases and Legal and Regulatory Issue and Third-Party Involvement. Because in the contexts of cloud computing and cloud database the service providers should highly engage with the ethical and legal concerns about their users' secure data.

Arora and Gupta (2012): In this paper possible issues with cloud database development by highlighting database security and privacy. The risks of storing transactional data on unreliable host systems have been widely identified, and sensitive data should be encrypted before being transmitted to the cloud to avoid unwanted access.

In the review of researches on cloud database security issues, there were few researches were found related to Cloud database and most of them encounter the problem unauthorized access and modification of customers data. The solving techniques also found in their research. There were many security issues identified in cloud computing environment. Some important issues are listed below.

- Safety of Data Storage
- Data Theft by Authorized Users
- The Production Data and the Backup Data are both stored in the same physical location.
- Your Data Can Be accessed by a DBaaS Provider
- Attacks on the database's DDoS and performance
- Users from outside the company can access the database.
- Hidden Sensitive Data
- SQL Injection Attacks
- Neighbor Tenants Can Access Data
- DBaaS Regulatory Compliance

Nayak and Mishra (2015) suggested in their study of "Cloud database security" that cloud database security is an important concern when accessing the database by clients. The unauthorized access of cloud database is the main issue for the customers and their confidential. In addition, the study noted that various user identification and credential management practices are used in the cloud computing environment to prevent unwanted access. An Adaptive Encryption Technique in cloud database services was designed to address this issue. It could increase the trust of cloud customers on data storage. Also reduces the computation cost and also increased CPU utilization.

The same was found in other studies as well (Leena, 2012). "Centralized database security in cloud" also suggested that the accessing of cloud database is associated with various security issues such as password vulnerabilities, data hijacking, compromising of accountant attack, man in the middle attack, password guessing against multiple user, user password attack. In this study the simple solution of Cryptosystem algorithm suggested for database security. The algorithms TORDES and RSA strategy was suggested for the efficient, scalable for simple data access/sharing application.

Shcherbinina et al. (2020) revealed a few other potential attacks against cloud databases include SQL injection, weak authentication, data breaches, account takeover, cross-site scripting (XSS), man-in-the-middle attacks, denial-of-service attacks, and cookie poisoning.

- The term "weak authentication" refers to an authentication technique that is very weak.
- When there are data breaches, hackers are able to access private information, like credit card numbers and personal data, that is kept in cloud databases.
- Attackers can obtain data from a cloud database in an unauthorized manner through SQL Injection. In most cases, the attacker runs malicious SQL code on top of the actual SQL code. Therefore, the dangerous SQL code assists attackers in getting past cloud protection.
- When cookies are poisoned, it signifies that hackers have been changing them.
- Attackers typically conduct denial of service (DOS) attacks when they send erroneous requests from outside the server to a noisy database server. Database failures occur as a result of the server's inability to meet the actual needs.
- Attacks that place the attacker in the middle of the client-server connection in an effort to steal data are known as "man in the middle" attacks.
- When a third party makes an infiltration attempt utilizing phishing or security holes in a database system to collect credentials, this is referred to as account hijacking.

Few conclusions could be drawn from studying research publications on security concerns with cloud databases. Most studies on security issues in cloud databases focused on unauthorized access by third parties and changes to the privacy information of the cloud database that had an impact on subscribers. Many authors also went into great detail about the problems by offering some sort of solutions in their research papers (Singh and Chatterjee, 2017).

- **Latency and reliability:** The encryption and decryption processes for the data in cloud databases will be most impacted by this.
- **Platform Specificity:** It implies that we are able to operate anywhere using cloud database services without any reliance on a particular language. Thus, any attacker can do so with ease. Cloud doesn't restrict to certain languages
- **Data breach through the fiber optics:** In the beginning, fiber optics were used to transfer data from a cloud database from one service to another. At that moment, an attacker used some tech equipment to successfully penetrate the shared cloud databases' trustworthy records of data without any hindrance.
- **Security and Privacy:** A variety of attacks have taken place as a result of privacy concerns. Some individuals lack the skills necessary to properly configure modern cloud databases, which poses serious security risks for these databases.

B. Solutions for security problems with cloud databases

Least Privilege - Limits access to resources by allowing only the minimal level of access, while still allowing an application to function normally.

In order to develop separate, particular privileges, the administration must first examine the requirement.

Give every user, application, and process who accesses the database the absolute minimum privileges. Unintentional data alterations or data leaks won't occur as a result (Chetan and Singh, 2016).

Separation of Privileges - Separates critical functions that can affect the security of the database into portions that is performed by different people or systems.

Authorization and Authentication - Authorization determines who has access to what resources. The identity of an entity requesting access to a resource is verified through authentication.

Another crucial security component is authorization. Only authorized users will have access to protected information, preventing data leaks (Huang and Tso, 2012)

Defense in Depth - Ensures that security controls are in place across the entire information architecture, including the database, network, server, and operating system. Cloud Pools can be used to accomplish this policy. A shared collection of resources that numerous tenants can use is called a cloud pool.

Logging and Auditing - Keeps track of all activities by keeping a log of any acts that may be security-related.

The most crucial security component is logging. We can track down issues and occasionally retrieve lost data. These logs can be utilized to carry out particular compliance certifications that demand proof of actions that are traceable and auditable that have been taken.

Information Hiding - Cryptography and hashing functions are used to hide sensitive information.

Only authorized users or processes will be able to access the true data in a database thanks to encryption. Encrypting sensitive data will help to stop data leaks and breaches. Even if an unauthorized person gains access to data, encryption will prevent them from accessing actual data. The system's speed will suffer if the entire database is encrypted (Wi, et al., 2014)

Redundancy - The reproduction of important components in a system, or an entire system, with the goal of improving the system's reliability. Additionally, periodic DMBS backups are required in order to restore corrupt or lost data if necessary.

Monitoring - Constant monitoring of a system's status to ensure that specifications are met. This is a crucial step because if a security breach is not noticed, it cannot be addressed.

The majority of databases do not follow all of the aforementioned rules because it is not practicable to do so, due to the fact that increased security can result in a reduction in throughput and robustness. Cloud databases in particular need to reply to queries rapidly in order to be effective. In order to aid developers in implementing security in cloud databases and settings more effectively, many of these regulations are given in pattern format.

Different security approaches and techniques have been proposed to secure databases that live in the internet or the cloud. However, despite progress, hackers continue to uncover new ways to exploit vulnerabilities that go unnoticed throughout development, testing, and deployment. For online databases, access management is a fundamental and crucial security challenge.

These are the primary techniques used in cloud databases to boost security. It is impractical to use every strategy suggested above. The performance and robustness of the entire system will decline as more security mechanisms are added. Quick response times, simple maintenance, and affordability should be features of cloud databases. These factors will be lessened by including all security methods. For cloud databases, requirement engineers can choose the appropriate security level and protocol for implementation. However, hackers will discover a way to take advantage of flaws that go unnoticed during development, testing, and deployment. We have therefore ensured that the system can handle extra security standards.

METHODLOGY

For this research, conference papers, journal articles, and relevant websites were used. published in numerous databases, including Google Scholar, IEEE Explore, and ScienceDirect.

The researcher used the search phrases “security issues in cloud databases” and “solution for security problem in cloud databases” to find the right dataset from this Database. 40 related papers are as a result identified and evaluated for these search phrases.

CONCLUSION AND FINDINGS

The security issues of cloud databases are the main topics covered in this review paper. This study also discusses possible solutions. We may therefore draw the conclusion that in order to improve the service provided by Cloud databases, security issues must be reduced and the encryption process must be improved.

The field of remote data storage and database management on a third party's infrastructure is one in which cloud computing is an advanced and developing technology. It provides many advantages to the users without establishing a private server or data center infrastructure for the business activities.
Today most organization are implementing the cloud database for their huge data storage. Although cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces lot of security challenges. There are ethical issues, security, and privacy that affect the use of cloud services. But to overcome these issues, Data can be stored and retrieved from the cloud using new, advanced encryption techniques and technologies. Also, proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.
Database need effective access control security mechanisms to protect the data stored. In particular, cloud databases present a difficult problem because they can be accessed at anything through the Internet, therefore effective security mechanisms are necessary to protect them without affecting normal business operations. Not only is it important that a database as security controls but in addition, a wide variety of security policies are required at varying levels of a systems architecture to sufficiently protect it.

A novel idea that offers users a ton of advantages is the cloud database. The cloud users may be impacted by some of the security issues it also faces. Described in this article are problems with and remedies for cloud databases. The performance of the entire database is traded off in favor of those solutions. The system designer should consider the system's security requirements while maintaining system speed. Cloud database systems cannot be said to be 100 percent safe. However, we can guarantee that it offers many more features than conventional databases.

FUTURE WORK

The main security issue with cloud databases is resource sharing. Any person can access data in a cloud database. We must therefore include some encryption and decryption functionality in cloud databases. In the future, we'll store a unique user's login and password in a cloud database. There is still more that can be done in the field of cloud databases. However, there are still a lot of unresolved issues, so there is always need for more research.

REFERENCES

Ahmed, A.A., and Hussan, M.I.T., 2018. Cloud Computing: Study of Security Issues and Research Challenges. *International Journal of Advanced Research in Computer Engineering & Technology*, 7(4), pp. 2-3.

Arora, I., and Gupta, A.,2012. Cloud Databases: A Paradigm Shift in Databases, *IJCSI International Journal of Computer Science*, 9(4)

Bhatti, Harrison John and Rad, Babak Bashari. 2017. "Databases in Cloud Computing," I.J. Information Technology and Computer Science.

Chetan, and Singh, S., 2016. Enhancement of Cloud Database Security. *Far East Journal of Electronics and Communications*, pp. 635-645. doi: 10.17654/ecsv3pii16635

Eugene, G. 2013. *Cloud Computing Models*. Massachusetts Institute of Technology.

Huang, K., and Tso, T., 2012. A Commutative Encryption Scheme based on ElGamal Encryption. *Database Encryption*, 4, pp.156-159.

Izang, A.A., Adebayo, A.O., Okoro, O.J., and Taiwo, O.O., 2017. Security and Ethical Issues to Cloud Database**.** *The Journal of Computer Science and Its Applications*, (24)

Leena, M.A.R., 2012. Centralized Database Security in Cloud. *International Journal of Advanced Research in Computer and Communication Engineering*, 1(8)

Nayak, D.S.K.M.A., 2015. Cloud Database Security. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(5)

Sharma, A., Sharma, *S.*, 2015. Storage of Database on Cloud with Security. *International Journal of Current Engineering and Scientific Research*, 2(9)

Shcherbinina, Y., Martseniuk, B., and Filonenko, A. (2020). DATABASE SECURITY AND STUDY OF DATA ENCRYPTION METHODS IN CLOUD STORAGE. Системи Управління, Навігації Та Зв'Язку. Збірник Наукових Праць, 3(61), 104-106. doi: 10.26906/sunz.2020.3.104

Singh, Ashish and Chatterjee, Kakali. 2017. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79. pp. 88-115 <https://doi.org/10.1016/j.jnca.2016.11.027>

Wi, Y., Kwak, J. 2014. A Study on Cloud Database Management System Protection Profile for the Secure Cloud Environment. *Journal of the Korea Institute of Information Security and Cryptology*, 24(2), pp. 411-429. doi: 10.13089/jkiisc.2014.24.2.411