Journal of Information Systems & Information Technology (JISIT)
ISSN: 2478-0677; Vol. 6 No.1 2021; [Pages 17- 27]

An Analysis of Security Issues in Cloud Databases

Muhammed Rijah
Department of ICT, Sri Lanka German Training Institute
rijah@slgti.ac.lk

Abstract. Cloud database is a kind of database service that is built, deployed and accessed through a cloud environment. Cloud database significantly stands among the next generation's database technologies. Security and privacy of data in cloud databases is mostly taken into account as it stores, manages and share a wider volume of complex data. Hence, it is highly constrained into the Cloud Computing model. Even though, cloud computing has brought a new perspective towards the IT industry, we are not assuring 100% security and privacy of the data stored as it sometimes lacks with awareness and control of data, due to issues with transaction log of data and malicious acts. Furthermore, ethical problems such as trust issues from tenants arise due to the difficulty in outsourcing information without the barriers and attacks of a third-party user. Therefore, in cloud database has been contained security and privacy concerns associated with cloud database and how the services provided by a cloud database could be improved, will be discussed throughout this paper.

Keywords: Cloud Database, Privacy, Security

I. INTRODUCTION

Cloud computing is generally known as on demand service. Cloud computing is a web-based service which provides a latest technique to use huge number of shared resources. It is a flexible and potent service spreading its wings on Information Technology industry at a very quick speed. It allows services to be consumed easily as and when required [1]. The concept of cloud computing implements with the development of communication, digital data processing and the changes with the storage requirements. Therefore, Cloud computing is defined as the practice of using a network of remote servers hosted on internet to store, manage and process data on demand and pay as per use [2]. Therefore, a large pool of shared resources can be accessed instead of the access to the local servers allowing the cloud service provides to provide a variety of different cloud servicers to its clients.

Service as a Service (SaaS): The service as a service model explains in this way, it provides browser-based software applications over the Internet where, the client will not be allowed to change its infrastructure (operating systems, cloud servers, cloud storage and network).

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

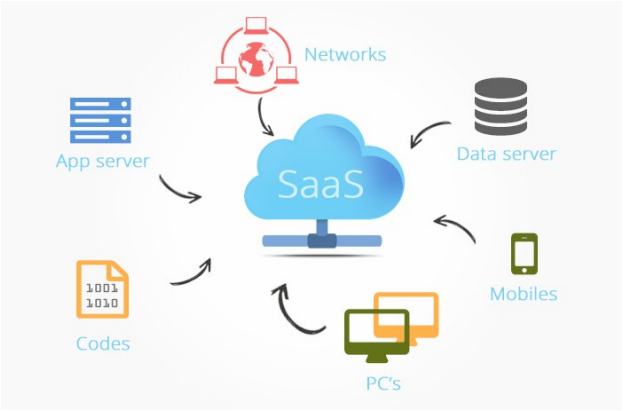

Figure 1 SaaS *Source: Internet*

Infrastructure as a Service (IaaS): The infrastructure as a service model explains in this way, where it provides an opportunity for online administration to access assets such as handling disk space while giving permission for the clients to install software in that infrastructure.

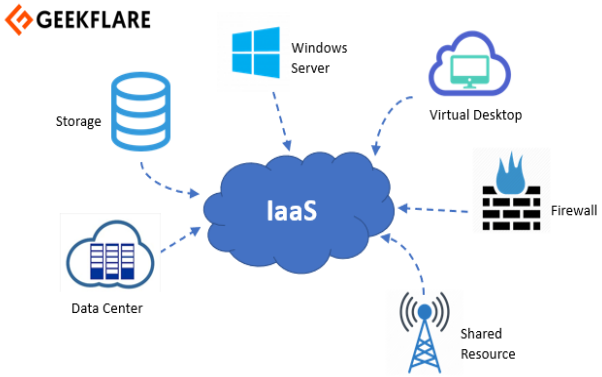

Figure 2 IaaS *Source: Internet*

Platform as a Service (PaaS): Platform as a Service model explains as this way where the developers are facilitated with an environment to empower themselves making services and applications accessible via the Internet.

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

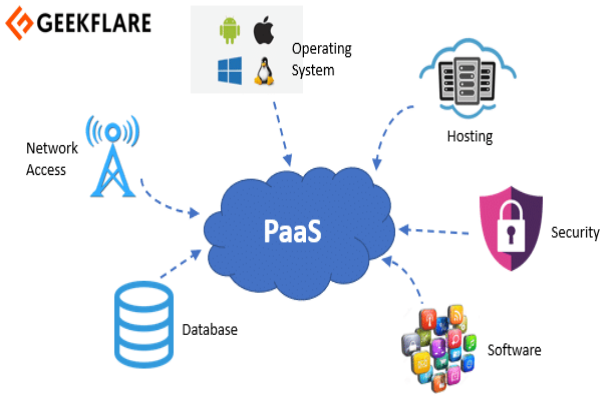

Figure 3 PaaS *Source: Internet*

Database as a Service (DBaaS): DBaaS is an architectural and operational methodology where IT providers are empowered to deliver database functionality services to one or more customers.

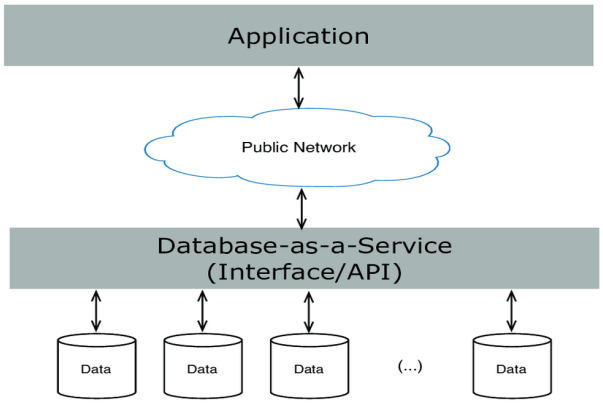

Figure 4 DBaas *Source: Internet*

Today, most of the industries are focusing on cloud database services. So, the cloud databases can be explained in the modern technological world as a database service built, maintained, and accessed under the cloud platform presenting the traditional functions.
However, the cloud database users may need to install and handle some sort of software on a cloud platform to configure the cloud database to be accessed on demand Database as a Service (DBaaS) providers are:

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

- Amazon
  - Amazon Aurora
  - DynamoDB
  - Amazon RDS
  - SimpleDB
- Google Cloud
  - GC Bigtable
  - Google Cloud Datastore
  - GC Spanner
  - Google Cloud SQL
- Microsoft Azure
  - Microsoft SQL Database
  - MA Table Storage
  - Microsoft DocumentDB
- Oracle Database
- IBM

Benefits of using Database as a Service (DBaaS)

are:

- Cost savings
- Simpler, less costly management
- Runtime capacity expansion of the database.
- Flexibility to accommodate the changes.
- Software quality.
- Disaster recovery mechanism.
- Virtual access, using a vendor's API or web interface.

Perhaps, as all those are positive measures the users should be highly concerned with the security issues on the clod databases though it is not possible to implement proper security mechanisms as on traditional databases. In Cloud Database Paradigm security, privacy and ethical issues are separately discussed as three popular issues and yet no precise solutions are found to overcome them.

II. LITERATURE REVIEW

Now we are discussing the Security Issues in Cloud Database and solutions which were provided to overcome those issues. Most of the researchers have been studied the security issues associated to cloud databases. By using those facts, they provided the mechanisms to overcome the issues up to certain level. Let's get some idea about the security issues and the solution on cloud databases explaining with a few research papers.

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

A. Security issues in Cloud Database

According to Shcherbinina et al. 2020, describe the various Security Issues in Cloud Database and some security issues and barriers in cloud databases have been critically analyzed. Also, it explains about the different types of possible attacks which affect the privacy and security of cloud databases and specially stated the approaches which we need to overcome the security issues emphasized in a research paper [4].

Shcherbinina et al. 2020 described some more possible attacks on the cloud databases. Such as SQL injection, Weak Authentication, Data Breaches, Account hijacking, Cross site scripting (XSS), Man in the middle attack, Denial of service attack, and Cookie poisoning [4].

- The SQL Injection is an attack which means the attackers get data from the cloud database unauthorized way. Normally the attacker executes some kind of malicious SQL code on top layer of the actual SQL code. So that malicious SQL code helps attackers to breach cloud security.

- Weak Authentication describes the strength of the authentication mechanism is very weak.

- Data Breaches means hackers obtain the sensitive information stored in the cloud database, such as credit numbers and personal information's.

- Account hijacking means intruders attempt to obtain access to user personal account by phishing or using holes in security of database system to discover passwords.

- Cross site scripting (XSS) is another malicious custom script which is inserted into the actual web content and by using this one attacker trying to get private and confidential data of the user on dynamic websites which are connected to the cloud databases.

- Man in the middle attacks means the attacker will try to enter the middle part of the connection of the client and the server and try to steal the data.

- Denial of service (DOS) attacks are the kind of situation attackers normally do if they will generate false requests to a loud database server from outside the server. Because of that the server is unable to meet the actual requirements database failures happen due to this reason

- Cookie Poisoning means attackers have been modifying the cookies

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

files and try to access unauthorized to the cloud database and get private data of the subscriber [4] [5].

Izang et.al [6] emphasize that there are Ethical Issues in Cloud Databases and Third-Party Involvements. Because currently the cloud database service mainly considers the ethical and legal concerns about their user's data security. In this article, mainly discussed about the three ethical issues are available on cloud related databases. Those are privacy issues, integrity of data and confidentiality. As an example, in cloud database level, we get many third-party services. By that time, we share some bits of data among with those services. So, if that services breach any of the written contracts that will directly affect the security and privacy of the cloud subscribers [6].

Wang [7] stated about cloud database development with the protecting database security and the privacy. It has been clearly mentioned about how the data store in to cloud database platform from untrusted host user. How the sensitive data protection happening on the cloud databases with the encryption functionality as mentioned on the paper, the United State of America provides the act name called "Patriot Act " with that the US government has powers to access any cloud databases in 2012 and Amazon S3 only allowed their subscribers to choose between US and EU data storage options [7].

After reviewing research papers about the Security Issues in Cloud Databases, there were few Most of the researches discussed Security Issues in Cloud Databases and most of them are mainly discussed about the unauthorized access of the third-party users and modifying the privacy data of the cloud database that affected the clout database subscribers and many authors also discussed the issues deeply by providing some sort of solutions in their research papers. Except those issues there were many security issues identified in the cloud database environment categorizing with the key area of the cloud platform. Those are, [8].

- *Privacy and Security: Many kinds of attacks have been occurred because of privacy issue. Some of peoples have lack of knowledge about the configuration things about the modern cloud database's such kind of situation it makes the big security issues for cloud databases.*

- *Latency and reliability: This will mainly affect the encrypting the data and the decryption process of the cloud database data.*

- *Platform Specificity: It means we can run on the cloud database services in any place without the language dependability. So any*

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

attacker can easily attack. Cloud doesn't restrict to special languages.

- *Data breach through the fiber optics: Early days, cloud database data transferred from one service to another service by using the fiber optics. That time some tech devices using an attacker successfully breach the trusted records of data without obstruction in it is data flow of the cloud database sharing.*

Chetan et al stated in their study of Cloud database security that described cloud database security issues while accessing the cloud database by client. The unauthorized access of cloud databases is the main issue faced by cloud database subscribers. Moreover, the authors added solutions such as user identified and initialized credential management mechanisms to protect unauthorized access. The paper also discussed the adaptive encryption techniques in cloud database services that were introduced against this type of common problem. Some of the paragraphs discuss the CPU utilization problem on the cloud database server which is hosted and the computational cost of the cloud database. Such a vast area is covered during this paper with discussing issues for the security level breaching [9].

Huang et al. [10] suggested a new asymmetric encryption mechanism which can be applied to the Cloud Databases. The suggested method follows the concept of commutative encryption and ElGamal encryption. The commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter. Re-encryption mechanism also takes place in the proposed scheme which shows that the cipher-text data is encrypted once again for duality. Such schemes are very useful in cloud applications where privacy is a key concern.

B. Solutions for Security issues in Cloud Database

- Access Control
  - It is a security technique that control who or what can access or use resources in a cloud environment

- Least Privilege
  - Set bare minimum privileges to any user, program, or process that accesses the database. This will avoid unintentional data changes or data leaks. [9]
  - The administration needs to analyze the requirement and should create separate specific privileges.

- Authentication and Authorization
  - Authentication is an important way to identify who is accessing the database or cloud infrastructure. The authentication process

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

is done through credentials or Single Sign-On (SSO). Every action done by an authenticated user will be logged with the user's signature. This will help to trace back unintentional data changes or deletions.

- Authorization is also an important security feature. Authorized users will be able to access privileged data only which helps to prevent data leaks. [10]

- Information Hiding
  - Encryption is a way to change data in a database so that only authorized users or processes will get real data. Encrypting sensitive data will help to avoid data leaks and data breaches. Even if an unauthorized party gets access to data, they won't be able to get real data because of encryption. However, encrypting the whole database will reduce the performance of the system. [11]

- Defense in Depth
  - Implement security protocols in all information transfer levels including database, network, servers, and operating system. (Muntjir & haque, 2017) suggested some multi layered security architecture based on defense in depth. This architecture will add multiple security protocols to increase the security of cloud infrastructure. Adding more security protocols will reduce the overall performance of the system. But, we can avoid external user access, traffic hijacking, man-in-the-middle attack, and data breaches like major security threats. [12]

- Redundancy
  - Sometime data redundancy happens by natural disasters, power failures, human errors like failures can happen at any time. This may lead to permanent data loss. This is why cloud infrastructures used redundancy. (Xie, Wei, Le & Li, 2020) indicated that Google's globally distributed database. It used replicated data across their data centers. With redundancy, they can survive even one or two data centers failures in a row. [13]

- Monitoring
  - Monitoring is the process of reviewing the processes in cloud databases or cloud infrastructure. This is implemented using automated software. Monitoring will help to detect downtime or data breaches easily and on time. This is a fundamental step because a security breach cannot be addressed if it is not detected.

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

- Logging and Auditing
    - Logging is the most important security feature. We can trace failures and sometimes recover lost data. These logs can be used to perform specific compliance certifications that require evidence of traceable and auditable actions that have been carried out.

- Multi-Factor Authentication (MFA)
    - Username and Password is insufficient to protect our cloud accounts from hackers. They may steal credentials and get access to our personal data.
    - Multi-Factor Authentication (MFA) ensure that only authorized person can access our cloud data. MFA is one of the cheapest and most effective security controls to keep hackers from accessing your cloud applications. [14]

In Cloud Database, these are the main approaches to increase the security of a cloud database. Implementing all approaches mentioned above is not practical. Adding more security protocols will reduce the performance and robustness of the whole system. Cloud databases should provide quick response, easy maintenance, and economical. Adding all security protocols will reduce these factors. Requirement engineers can decide what should be the security level and select which protocol needs to implement for cloud databases. But hackers will find a way to exploit vulnerabilities that go under the radar during development, testing, and deployment. Therefor we have made sure to add more security protocols the system can handle

III. CONCLUSION

The Cloud Database is a new concept that provides a huge number of benefits for users. However, it also has some security challenges which may affect the cloud users. This article discussing about cloud database challenges and solutions. There is a trade-off between those solutions and the performance of the whole database. The system designer should consider what security needs for the system and keep system performance. We cannot say cloud database systems are fully secured. But we can assure it provides much more features than traditional databases.

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

REFERENCES

[1] Kanimozhi, R. (2019). Adaptive and intelligent framework of data protection techniques for cloud storage. *International Journal Of Cloud Computing*, *8*(1), 50. doi: 10.1504/ijcc.2019.097906

[2] Yaseen, Q., Althebyan, Q., Panda, B., & Jararweh, Y. (2016). Mitigating insider threat in cloud relational databases. *Security And Communication Networks*, *9*(10), 1132-1145. doi: 10.1002/sec.1405

[3] Connolly, T. M. (2021). *Database Systems: A Practical Approach to Design, Implementation and Management 5th (fifth) edition*. Addison Wesley.

[4] Shcherbinina, Y., Martseniuk, B., & 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

[5] Database Management Challenges in Cloud Environment. (2016). *International Journal of Modern Trends in Engineering & Research*, *3*(9), 208-212. doi: 10.21884/ijmter.2016.3067.9neo0

[6] A.A. Izang, A.O. Adebayo, O.J. Okoro and O.O. Taiwo, "SECURITY AND ETHICAL ISSUES TO CLOUD DATABASE," The Journal of Computer Science and its Applications, vol. 24, 2017.

[7] Wang, L. (2014). Research on Security of Database in Cloud Computing Environment. *Applied Mechanics and Materials*, *644-650*, 1694-1697. doi: 10.4028/www.scientific.net/amm.644-650.1694

[8] A Survey: Cloud Computing Challenges & Security Issues. (2017). *International Journal of Modern Trends in Engineering & Research*, *4*(3), 57-61. doi: 10.21884/ijmter.2017.4079.cfbgf

[9] Chetan, & Singh, S. (2016). ENHANCEMENT OF CLOUD DATABASE SECURITY. *Far East Journal of Electronics and Communications*, 635-645. doi: 10.17654/ecsv3pii16635

[10] K. Huang, and R. Tso, "A Commutative Encryption Scheme based on ElGamal Encryption," Database

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]

Encryption, vol.4, pp.156-159, 2012.

[11] 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), 411-429. doi: 10.13089/jkiisc.2014.24.2.411

[12] Muntjir, M., & haque, M. (2017). Cloud Database Infrastructure: Database System Transference in Cloud Computing Management and Security. *International Journal of Computer Trends and Technology*, *47*(1), 16-28. doi: 10.14445/22312803/ijctt-v47p103

[13] Xie, G., Wei, Y., Le, Y., & Li, R. (2020). Redundancy Minimization and Cost Reduction for Workflows with Reliability Requirements in Cloud-Based Services. *IEEE Transactions on Cloud Computing*, 1-1. doi: 10.1109/tcc.2019.2937933

[14] D'Silva, F. (2021). 6 Tips for Improving Cloud Computing Security. Retrieved 19 June 2021, from https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security

[Received: 4th June, 2021; Revised and Accepted: 10th July, 2021]