INTERNATIONAL JOURNAL OF ADVANCED STUDIES IN ECOLOGY, DEVELOPMENT AND SUSTAINABILITY
p-ISSN: 2354-4252 | e-ISSN: 2354-4260
Volume 6, Number 1, February, 2019

Cloud Computing and Database Security

Sani Bala
Department of Office Technology and Management,
Federal Polytechnic, P. M. B. 1012, Kaura Namoda, Zamfara State

Abstract

Data confidentiality and privacy are the security concerns and success of every serious organisation. This research work addresses the social and technological impact of cloud computing on the database security. It addresses many challenges and risks associated with the cloud computing on the database security, the possible control measures that may reduce the observed risks associated with the cloud computing on the database security. The methods used by this research work are only limited to online scholarly journals. As the objective of the research to discussion about the cloud computing on database security, by searching the articles, printing the articles, reading the articles, paraphrasing the articles, summarising the article's contents to the best of my understanding and were adopted as a method followed to obtained reliable and accurate data. Some of the find of this research work are the cloud software developers should develop a database intrusion detection system (DBIDS) to detect intrusion as soon as it occurs. The cloud service providers prefer more than one confirmation protocol to provide better security to control the user's identity. The data shared with the multiple applications through computer-generated machine should protect by entering some coded keys to the user who uses the services on the cloud. The research work observed that despite the effort made by the software companies to properly and effectively secured database from unauthorized accesses/exposure, there is need to enhance the database security through innovative efforts and research.

Keywords: Cloud, Database, Database Security, and Cloud Computing

Corresponding Author: Sani Bala

URL:
http://internationalpolicybrief.org/journals/international-scientific-research-consortium-journals/intl-journal-of-ecology-vol6-no1-feb-2019

Background to the Study

Cloud computing is based Internet computing where information and data are saved on the network resources, and allows data and information to be accessed from everywhere in the world. It became the highest software platform for distributing information and data over the web. The stage and security solution involving is not yet ready. (Paul, *et al.* 2012; Sweta, *et al*. 2013).

Cloud computing is ways of forming the computer system and enabling convenient on the network demand access to distribute information technology configurable resources. Cloud computing implied some of the technical aspects of building computer systems, but the challenge faced in the information technology environment still stands. Because managers reviewed that information technologies are expensive, difficult and promise of the cloud computing leads many things that, Information technology will be cheap and easy. The global market for cloud computing will experience an increase significantly in the following years and replace the information technology environment forecast by the specialists (Kamal, 2011; Ogigau, 2012).

Database security is the processes and procedure that protect a database from accidental actions by applying the modern security devices. The database is still violated from both internal and external users, the researchers develop Database Intrusion Detection System (DBIDS) to identify Instruction as soon as it occur and supersede its malicious affect and the primary objectives of database security is to prevent authorize tempering of data, to prevent unauthorized access of data, and to protect that the data remain available when needed (Coffin, 2011; Rezk, 2012; Acharya, 2013).

Literature Review

Cloud Services

The word cloud in the information technology refers to collections of services, information, applications, and substructure comprised of pools of network computer, information, and storages resources. (Kamal and Kaur, 2011). The core concept of cloud computing is reducing the processing load on the user's station by frequently improving the handling ability of the cloud to simplify the user's station to a simple output and input devices, and to provide the demand services.

Table 1: Cloud Layers and providers. (Divakarla, 2010; Kamal, 2011).

	Services	Providers
Platform as a service (PaaS)	* Platform which allows a software developer to create programs that can be run in the cloud.	• Mobile Me • Google Docs • Zoho
Software as a Service (SaaS)	* Develop software that is capable to run in the cloud. *Support running multiple instance of it.	• Google App Engine • Force.Com • Microsoft Azure
Infrastructure as a Service (IaaS)	*Consists of Database servers and storage *Highly shared and scaled computing infrastructure accessible using internet browser	• Sun's Cloud Services • Amazon S3

Cloud Computing Trend for Future Direction

A survey of 785 respondents spanning manufacturing professional, users and hawkers in 2012 by North Bridge venture partners presented 65% to 35% Hawker to client ratio (Skok, 2012). There is an anticipation of 6% spending growth in the level of adoption of SaaS which has 82% of present usage. According to the reviewer, there is a forecast of 75% built applications on PaaS by 2017 (83% increment for 2012). PaaS and IaaS are expected to have important growth to 72% and 66% in the five years coming compared to the present 40% and 51% respectively (North Bridge, 2012). The extensive data methodical challenge and the need to incorporate flexibility with scalability will make more organizations adopt hybrid cloud thereby moving some of their services to the public cloud integrating more technologies, vendors and ecosystem.

Figure 1 and 2 shows a bar chart of the cloud computing tendency for the next few years.

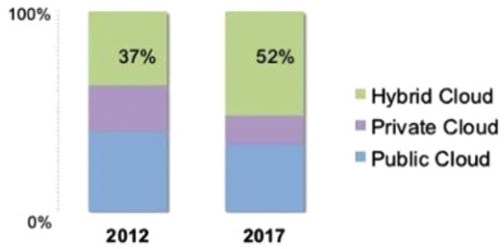

Figure1: Cloud computing trend (2012 – 2017).
Source: (Nusca, 2012)

Figure 2: Future Trend of Cloud computing.
Source: (Nusca. 2012)

The reduction in risk ratio (from 10% to 3%) of data for sovereignty and patriot act will boost confidence in cloud computing adoption. This is complimented with the improvement in security and compliance measures (Nusca, 2012).

Fig. 3: Future of Cloud Computing (2012).
Sources: (Skok, 2012).

Figure 3 above, shows the future of cloud computing based on the 2012, future cloud computing survey results released by the leadership dinner. They revealed several important changes in respondent's plans and observations concerning the cloud application.

Basic Challenges of Cloud Computing
(Divakarla, and Kumari, 2010) he noted the following basic challenges of cloud computing.

Threshold Policy
This requires that a database should be carefully tested to ensure it works properly. It also requires developing, or improving and implementing a threshold policy in a pilot study before moving the program to the production environment. The database should be carefully checked to determine how unused resources are to be de-allocated and turned over to other work. Check how the policy detects sudden increases in the demand and results in the creation of additional instances to fill in the demand.

Unexpected Behavior
It demands that through assessments of the database to reveal unexpected results of validation or releasing unused resources. The observed problems should be carefully before running the application in the cloud. This is to assure all foreseen problems are managed and eradicated.

Hidden Costs
Cloud computing ensures not tell what hidden costs are. For example the experiencing network costs, businesses that are far from the location of cloud providers could experience latency, particularly when there is heavy traffic.

Security Risks on Cloud Computing
Paul *et al* (2012) noted that numerous security concerns have to be considered and addressed while using cloud computing. Addressing these challenges will make the cloud computing very robust and highly secured. He noted the following challenges as follows:

Confidentiality
The cloud providers sometimes employ party companies to store data and information of their customers. It is possible that they can use the data and expose it. Cloud providers have to make sure that the personal information is not being shared with third party companies.

Data Integrity
When data is on the cloud anyone can access it. Cloud does not differentiate between sensitive data and common data thus enabling anyone to access those sensitive data and leads to lack of data integrity in the cloud.

Data Theft
Most of the cloud providers try to lease a server from other service providers because it reduces cost and makes operations more flexible. There is a high chance and tendencies that the data stored in their servers can be stolen by malicious users.

Data Loss
The cloud providers may shuts down their servers due to maintenance work or due to some problems. During this period of maintenance services, the clients won't be able to access those data because it is no more available for them as the cloud provider does not exist anymore. These activities sometimes lead to the loss of data for the customers.

Data Location
The customer does know where his data is located. The cloud provider does not disclose where all the data are stored. The data's won't even be in the same country of the customer. It might be located anywhere in the word.

Deletion of Data
There are possibilities that the data which are no longer needed is deleted by the user but are still there somewhere in the cloud. It is a serious problem in the cloud. Consumers must be vigilant and make sure that the data deleted from the cloud are no longer kept. Cloud providers must make sure that the data which the client deletes is completely removed from the cloud so as to prevent unauthorized access by another user.

Malicious Insiders
Cloud provider does not give information on how it grants workers access to data and information in the cloud. The consumers do not know whether the works in the cloud company are granted access to the stored data. If the employees are not properly supervised by the cloud company, the customer's data can be easily exposed by an employee of the cloud company and consequently be seen and manipulated by another person. Cloud providers must follow guidelines and policies for preventing employees from accessing the data and information of its clients and strictly adhered to such guidelines and policies.

Account or Service Hijacking
Cloud computing hacker can easily hijack a customer's or user's account and can easily manipulate and steal confidential data of the user. A customer would never want his data or information to be stolen. The cloud providers must put strong protection and prevent hackers and malicious people from gaining access to customer's data and information.

Data Segregation
Data can be stored in the shared mode or in private mode as per user wishes. However, most user's data and information are kept in the shared environment. Due to this reason, there is high chance and tendencies that the user's private data can be seen by other users.

Users Activities
User's activities here refer to the set of activities and operations that may be performed by the users on his data which can cause consequential damage loss to the stored data. The user's activities such as clicking links in e-mail messages, instant messaging, visiting fake websites, etc. can download malware to a local workstation. The malware can launch attacks on Internet network there by reducing its efficiencies or even caused serious damage to the stored data. Paul *et al* (2012).

Steps to Make Cloud Computing More Secure

This section concern with the major steps that should be followed to ensure safety and prevent malicious attack on the cloud computing.

Paul *et al* (2012) noted that, the following are the steps that make cloud computing more secured:

a. Make sure to develop good policies around passwords; how they are changed, protected and created.
b. Don't allow the staffs to get access of your passwords.
c. Installing exception monitoring system.
d. Check whether any third party companies are able to access your data.
e. Make sure that not any third party companies access your data.
f. If a user registers for any cloud computing services, the confirmation checks should be applied.
g. The cloud service provider and the customer must sign an agreement form stating clearly the responsibilities of parties, terms and conditions of contract and breakup.
h. Measures of data backup should be there in the cloud. In case of data loss, the backup data can be used to regain the loss data.
i. The cloud provider must have strict authentication and validation policy for employees.
j. The minimum set of standard for cloud computing must be stated.
k. The cloud providers should be trustworthy reputed and accredited.

Database Security Considerations

According to Basharat *et. al.* (2012) says that, in order to eradicate the security threats of every organization, the security policy must be described, and the security policy should be severely enforced. A strong security policy must contain well defined security features and they are:-

Access Control

Make sure that all databases communications and other system objects, are according to the policies and controls defined, and make sure that no interference occurs by any attacker neither externally nor internally and thus, protects the databases from potential errors, the errors that can make crash as big as stopping firm's operations. Access control helps in minimizing the risks that may directly impact the database security on the central servers. For example, if any table is accessed accidentally the personalized results can rotate backed and the accessed control can restrict their deletion.

Inference Policy

This is required to protect the data at a certain level. It determines how to protect the information from being disclosed. It occurs when the interpretations of data in the form of facts or analysis are required to be protected at a specified higher security level.

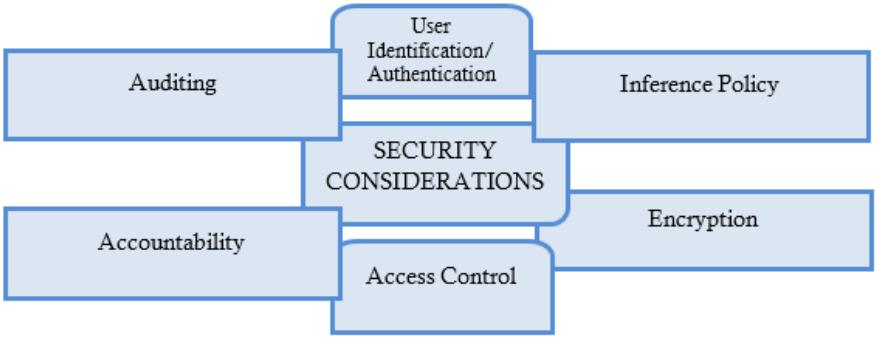

Figure 4: Critical Areas under Consideration
Source: Basharat, *et. al. (*2012).

Method of Data Collection
The data presented in this work are only limited to online scholarly journals. The articles searching dealing with database security, cloud computing and related words were made in obtaining the data so far presented. As the objective of the report is the discussion about the cloud computing on database security, by searching the articles, printing the articles, reading the articles, paraphrasing the articles, summarizing the article's contents to the best of my understanding and were adopted as a method followed to obtained reliable and accurate data.

Findings
The following findings were made by the researcher:

1. That cloud software developers develop a Database Intrusion Detection System (DBIDS) to detect Intrusion as soon as it occurs.
2. That cloud computing investors should invest in applying the security measure to ensure that the data are being kept private and secure throughout its lifespan in order to reduce the hazard.
3. That cloud service providers prefer more than one confirmation protocol to provide better security to control the user's identity.
4. That data shared with the multiple applications through computer-generated machine should protect by entering some coded keys to the user who uses the services on the cloud.

Conclusion
The findings in the present study shows that despite the thorough effort by the software and allied companies to provide an efficient and reliable security measures on the database, the current security measures do not guarantee zero risk on the database but only reduce the risk in our contemporary information technology world. It therefore became necessary to quickly and effectively enhance the current security measures to a more robust and efficient. This can be achieved through innovative research, auditing to the users and hard work by the cloud computing and allied companies.

References

Basharat, I. (2012). Database security and encryption: A survey study [online]. *International Journal of Computer Applications, 47* (12), 0975 (888)

Coffin, M. M. (2010) Database Security: What students need to know [online]. *Journal of Information Technology Education*.

Divakaria, U. & Kumari, G., (2010). an overview of cloud computing in distributed systems. [Online]. International Conference on Methods and Models in Science and Technology (ICM2ST-10). 978 (7354-7354). [Accessed on 28 Nov 2018]. Available at: http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=c2934aed-5207-4b05-8ad1-bdac12ea2492%40sessionmgr4001&hid=4114

Kamal, S., & Kaur, R. (2011). *Cloud computing security issue: Survey, (online).* The 2nd International Conference on Methods and Models in Science and Technology (ICM2T-11) AIP Conf. Proc. 1414(149-153). [Accessed on 23rd November, 2018]. Available at: http://web.ebscohost.com/ehost/pdfviewer/pdfvsiewer?vid=3&sid=6bdb5bb4-27f9-40fa-a8de-1d8d17d709ef%40sessionmgr4004&hid=4114

Nusca, A., (2012). *The future of cloud computing: 9 trends for* (*2018) [online].* [Accessed on 30th November, 2013). Available at: <http://www.zdnet.com/blog/btl/the-future-of-cloud-computing-9-trends-for-2012/80511.

Ogigau, F. N. (*2012).* Cloud computing security issues [online]. *Journal of Defense Resources Management, 3* (5).

Paul, R., Talreje, M., Sahu, A., & John, K., S. (2012). Security issue in cloud computing [online]. *International Journal of Computer Science and Engineering (IJCSE), 4* (0975-3397).

Rezk, A., Ali, A. H. & Barakat, S. I. (2012). Database security protection based on a new mechanism [online]. *International Journal of Computer Applications, 49* (19), 0975 (8887).

Skok, M. J. (2012). *Future of cloud computing* [online]. The 2nd Annual Survey results from 39 collaborators. [Accessed on 30th November, 2018]. Available at: http://www.slideshare.net/mjskok/2012-future-of-cloud-computing-2nd-annual-survey-results

Sweta, J., Patel, A. & Acharya, V. (2013). Case study of database security in campus ERP system [online]. *International Journal of Computer Applications*, *79* (15), 0975 (8887).