Journal of Multidisciplinary Engineering Science Studies (JMESS)
ISSN: 2458-925X
Vol. 3 Issue 6, June - 2017

Cloud Computing & Big Data challenges & Security Challenges

Dr. Alshafie Gafaar Mhmoud Mohmmed
Computer Science department,
Emirates Collage of Science & Technology, Sudan
dr_shaf@yahoo.com

Prof. Saife Eldin Fatoh Osman
Dean of Emirates Collage of Science & Technology
Computer Science department,
Collage of Science & Technology, Sudan
saifefatoh@hotmail.com

***Abstract*— During past few years, the internet has accelerated the use of computing devices like computers and mobile Phones. These devices are generating huge amount of data for the users on daily basis. Cloud computing provides computing, storage, services and applications over the Internet. It is one of today's most popular technologies due to its low cost computing with increased flexibility, scalability mobility and enhanced storage. Data generated by users over internet are stored on some remote location with respect to the user. This is the reason why IT organizations have shown their interests over security of cloud computing implementation. The main objective of this paper is to provide the critical review of the different vulnerable security issues of the cloud computing systems.**

***Keywords*— Cloud Computing, Challenges of Cloud Computing**

I. INTRODUCTION

CLOUD COMPUTING

Cloud Computing manipulates and configures the data and accesses the applications online. Online infrastructure, data storage and applications can be offered through cloud computing.

The user can access applications in the cloud network from anywhere by connecting to the cloud using the internet. Some of the real time applications which use cloud computing are Gmail, Google Docs and Dropbox etc.

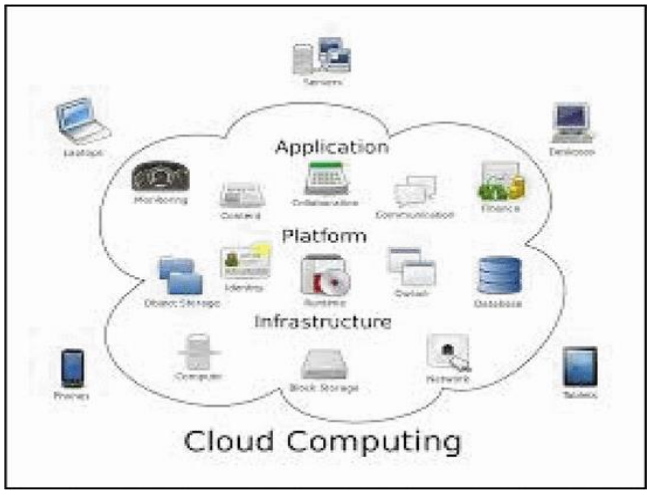

Fig. 1. Cloud computing

BIG DATA

Big Data is the term used to describe huge volumes of structured and unstructured heterogeneous data that are so vast that it is very difficult to process this data using traditional databases and software technologies.

Fig. 2. Big data

The term "Big Data[1]" is believed to be originated from the web search companies who had to query loosely structured very large distributed data. The five main terms that signify Big Data have the following properties:

A. Volume

Storing transaction data, data collected from sensors and live streaming data etc. contribute towards increasing Volume.

B. Variety

Big Data is a large volume of heterogeneous data. Emails, video, audio, transactions etc. are the main varieties.

C. Velocity

The data should be processed fast and it should be produced fast to meet the demand of the user.

D. Variability

This shows that the data flow can be highly inconsistent with periodic peaks.

E. Complexity

As the data is coming from the multiple resources so the complexity is the main concern. The data should be matched, linked, cleansed and transformed into desired formats before processing. Real time examples of the Big Data are Bank's Credit card transactions made all over the

world, Facebook and Twitter users generating social interaction data and Walmart customer transactions.

Some important features of Cloud Computing

Cloud computing enable users to share information and services from remote computer without having a costly and complex hardware and/or software infrastructure.
There are following important features of cloud computing:

- Cloud computing uses 'Pay as you use' business model.
- It Shares resources and information to number of users simultaneously.
- One of the essential component of cloud computing is virtualization. Virtualization is one of the hardware reducing, cost saving and energy saving technology.
- User can access applications as utilities and information, over the Internet.
- User as well as service providers can manage the application and data at any time using the Internet.
- In cloud computing user need not to install a specific piece of software to access information and services over cloud.
- Cloud computing provides online tools for development and hosting, runtime environment for programming.
- Cloud computing provides platform independent access to resources and information over the Internet all users.
- It offers on-demand self-service. The resources can be utilized without interacting to the service provider.
- Cloud Computing is highly cost effective because data and services need not to be stored to a storage device on one's PC. It minimizes the overall cost of accessing the information and services.
- Cloud Computing offers load balancing to distribute the excessive load on a particular server. This feature makes it more reliable.

II. SECURITY CHALLENGES IN CLOUD COMPUTING

Although cloud computing systems are capable enough for organizations to share information and services using internet without any need of physical infrastructure, it is vulnerable for security threats which must be solved. As information and services are shared on internet, there is a strong need to understand the different issues associated with it. There are following security challenges of cloud computing.

Confidentiality

Confidentiality can be defined as the ability for an authorized group of users or authorized systems to access protected data [3]. The increase in number of users of cloud computing systems helps in increasing the access points; hence the data becomes more exposed to external entities and more likely to be compromised [3].
1) Data Confidentiality: Data confidentiality is all about to provide access control to the data, memory and devices. It is the property that data contents are not made available or disclosed to illegal users. Therefore, we need to provide a strong secure verification system which may leads to secured access within Cloud services [3]
2) Application Confidentiality: Cloud services also provide access for software applications eliminating the needs of installing them at every system. Hence, application security can be another important factor for providing a secure cloud system [3].

Privacy

Privacy is the ability of individual user/system or group of users/systems to control the sharing of data to other users or systems. Individuals are required to follow rules set by governments concerning user's personal data privacy and confidentiality. Because, data is stored on multiple locations in cloud network, they are vulnerable to security breaches [3].

Integrity

Data integrity can be defined as the means to protect data, services and application from unauthorized modification and deletion in cloud computing systems. Data integrity can be divided into following two categories:
1. Data Integrity: Data integrity is protecting data from unauthorized deletion and modification. The cloud service provider should ensure the users that personal data are not manipulated in between. Data integrity is very important factor in order to achieve a high level of confidentiality in data and system integrity. As number of users increase, number of access points to access cloud services increases, which, in turn, requires authorized access [3]
2. Software Integrity: Software integrity is basically restricting the unauthorized access and modification in software applications provided by cloud systems. The software application owner or administrator is responsible for software integrity from unauthorized modification [3].

Availability

Availability refers to the ability of an authorized user to access a cloud system and use it to share information, use cloud resources and application even with a security interruption or a system malfunction [3]. Availability includes the availability of data, applications and physical components on request of end user [3].

III. CLOUD COMPUTING SECURITY THREATS

Cloud service providers are making an extensive effort to secure the services and systems so as to decrease the threat of attacks and gain the confidence of their customers [3].
The main function of any cloud provider is to provide a cloud service which can secure resources or information on the cloud. In general the main issues of the cloud are related to the confidentiality & integrity of the data. There are some security threats that are limiting the boundaries of

cloud services. Broadly, security threats in cloud computing can be divided in the following categories:

• Web based Threats
• Application based Threats
• Physical Threats
• Network based security Threats

Web Based Threats

1) Phishing scams: It sends the links of those websites that are designed to get the personal data like account numbers, passwords etc. to the user via email, text messages, or any social networking site using a trick.

2) Drive by downloads: In this system the applications or some software gets downloaded without the authorization or user's knowledge which contains malware, spyware or viruses.

3) Browser exploits: Designed to want advantage of susceptibilities throughout a browser which is launched directly from browser or from third party extensions like Flash player, PDF reader, image viewer, etc. This can be made possible simply by visiting certain unsafe sites which automatically installs malware.[4].

Application Based Threats

1) Malware: It is the ability to rapidly connect and exchange content with anyone, anywhere which increases the chances of a cloud data breach.

2) Spyware: It assembles and use the personal and private information like location, contact list, email & photos without proper permission and utilize this information in future for cash fraud etc.

3) Vulnerable Applications: These are applications that contain faults & errors which can perform malicious functions. It may access confidential data, perform unwanted actions, stop a service from functioning properly, or transfer unwanted apps to your device.

Physical Threats

1) Device Possession: It is the ability to rapidly connect and exchange content with anyone, anywhere which increases the chances of a cloud data breach.

2) Lost or taken devices: In case the device gets lost or given to someone then it is of big concern for the owner as all the vital information nowadays are kept in mobile Phones.

Network Based security threats

1) Network exploits: It create the foremost of flaws as they will install malware on your device without your knowledge.

2) Wi-Fi Sniffing: It intercepts the information across the network when it travels and is unencrypted by scanning or any other means.

3) Address Impersonation: It means that no authentication is provided for the source and destination network addresses which can cause information to be delivered to some other unwanted addresses.[5]

IV CONCLUSION

In recent years, cloud computing has gained much response and spread round the globe. It is giving and extending its applications in almost every field be it business, shopping, education etc. However, the risk of the threats is the biggest problem users are facing today.

V. References

1. A, Katal, Wazid M and Goudar R.H "Big data: Issues, challenges, tools and Good practices" Noida, pp. 404-409, Aug., 2013.
2. Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, Issue Date: 11-13 March 2015, Written by: Gupta, A.; Mehrotra, A.; Khan, P.M.
3. Zissis, D. and Lekkas, D. (2012) Addressing Cloud computing security issues. Future Generation Computer Systems. 28 (3), pp. 583-592.
4. What is a mobile threat?, https:llwww.lookout.comlresources/know-yourmobile/ what-isa-mobile-threat, visited on Mar 2017.
5. Solanke Vikas S., Kulkarni Gurudatt A., Katgaonkar Pawan, Gupta Shyam, "Mobile Cloud Computing: Security Threats" (2014).