Journal of Engineering Sciences
Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

SECURITY ISSUES OF BIG DATA IN CLOUD ENVIRONMENT: - A REVIEW

Mr. Pravin R. Nerkar[1], Dr. Manoj K. Ramaiya[2]

[1]*Research Scholar, Computer Science & Engg., Sage University, Indore, India*

[2]*Associate Professor, Advance Computing, Sage University, Indore, India*

***Abstract*— Big data is larger, more complicated data sets, especially from new data resources. These data sets are so voluminous that conventional data processing software just can't manage them. But these heavy volumes of data can be used to address business problems you wouldn't have been able to tackle before. As the today's need to use different application and the need to store large data for such application has increased. But problem with traditional data storing way and this is not sufficient to work in such local environment for long time. So instead of storing data locally put it on cloud so as to use it by anyone from anywhere. It uses the servers hosted on the internet to store, maintain and process data, rather than a local server or a personal computer. But this way again comes with issues of big data storage security and privacy. So this paper focus on some cloud services issues for data security and privacy.**

***Keywords*— Big Data, Cloud, Security, Privacy.**

1. INTRODUCTION

Advanced field of data science is a "Big data". It actually checks how big data sets can be confined and evaluates in order to consistently gather insights and information from them. Earlier, traditional data processing solutions are not very productive with respect to capturing, storing and analyzing big data. So big data focused on characteristics knows as 'Five Vs' [1][7].

1. Velocity - Velocity refers to the speed at which the data is generated, collected and analyzed. Data continuously flows through multiple channels such as computer systems, networks, social media, mobile phones etc.

2. Volume- Term volume defines the how much large data that is produced. The value of data is also dependent on the size of the data. So the size of data is important dimension for the big data term.

3. Value- Data collection is not just enough for any system but important is how much value that data having. Whether it useful or not and how much credential it going to be generate for future. What you do with the collected data is what matters. With the help of advanced data analytics, useful insights can be derived from the collected data. These insights, in turn, are what add value to the decision-making process.

4. Variety- It focused on how the data is shown or represent. In data collection it comes from number of different sources and their formats are different from structured to unstructured.

5. Veracity- Big data comes from number of data sources and it is not always guaranteed that all data is accurate and useful. It is very important to check quality and correctness of data before processing.

2. CLOUD COMPUTING MODEL AND SERVICES

Cloud computing has been evolved as a next step in the computation environment. Cloud environment is a combination of hardware and software that provide different services over the network as per the user requirement. In the cloud environment, application and computing resources are facilitated as a service over the internet when it required, so it refers to offering computing services from servers in a network. Typically cloud services are available on demand, can be accessed over a network, share resources between multiple applications and tenants, scale elastically based on dynamic computing needs, and provide measured service.

Cloud computing models and services are typically based on the ownership of the infrastructure and based on the general architecture visible to users [2].

2.1 CLOUD MODEL

Public cloud:- A cloud service offered to the general public. It is a type of cloud hosting in which the cloud services are delivered over a network that is open for public usage. The cloud provider owns, manages, and operates all computing resources placed within the provider's facilities and those available resources provided to users are shared across all customers. Because of the sharing of cloud across many customers it is limited to customization [2].

Private Cloud:- A cloud infrastructure operated for a single organization. The cloud can be handled by the organization or a third party, and it can be hosted on premises or at a third-party datacenter. In general, private clouds give high-superiority service. As the private cloud are dedicated to and owned by one customer organization, such type of clouds are typically more customizable than other forms of clouds.

Community cloud:- In this model service or setup is shared by number of users or organization belongs to same community. The system is managed by one or more of the organizations, by a central provider, or a combination of the two and organizations using such model are also sharing performance and security concern. Organizations employ this cloud service have shared missions, governance, security requirements, and policies.

Hybrid cloud:- A cloud service that is a combination of two or more of the deployment models like public, private, or community. In general a private cloud that is connected to one or more third-party public-cloud service providers for certain applications. It permitted users to aggregate services of other package for better performance and capability.

2.2 CLOUD SERVICES

Software as a Service (SaaS):- SaaS is the most usual form of cloud computing and a fully-developed software solution ready for purchase and use over the internet. SaaS access the internet or web to facilitate user by providing application or software which are managed by third party vendor and interface is on end user side. The SaaS provider manages the infrastructure, operating systems, middleware, and data necessary to deliver the program, ensuring that the software is available whenever and wherever customers need it. Many SaaS applications run directly through web browsers, eliminating the requirement for downloads or installations. Examples are Microsoft Office 365, Salesforce, Google Apps [3].

Platform as a Service (PaaS):- Platform as a Service provides the framework needed to build, test, deploy, manage, and update software products. PaaS is a cloud computing service that provides the platform to user to develop and run software without caring about basic infrastructure. User don't need to bother about basic element that is security and network it is leave to service provider.

Infrastructure-as-a-service (IaaS):- It provides a completely virtualized computing infrastructure that is managed over the internet. An IaaS provider handled the physical end of the infrastructure (servers, data storage space, etc) in a data center, but allows customers to fully customize those virtualized resources to suit their specific needs. It helps to provide resources on demand for all applications and services deployed in the system. Examples are Microsoft Azure, Amazon Web Services (AWS).

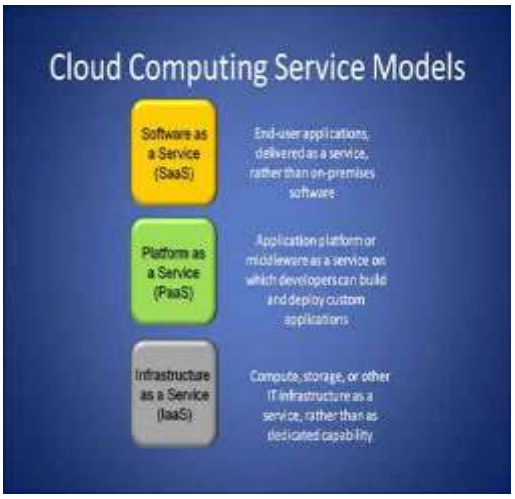

Fig.1 Cloud Service Model

3. SECURITY ISSUES IN CLOUD

Users are storing data on cloud because of generation of voluminous data and limited storage. But security is very important aspects in every system. Users always want security as far as storing their data on other system.

1. Location detection: - Data storage is the prominent work of cloud which is in discussion, but finding it could be the challenge that location at which place it is actually. So without knowing the [4] location of data it could misinterpret and violated.

2. Data Reliability:- Data reliability is major aspect of cloud. As users are storing data on cloud it should be reliable and authorized user can accessed it. Data are stored in encrypted format and authorized user used it legally by decrypting it, but it should not be to use it by unauthorized user. Data are used concurrently by multiple users for the updating but there should be legal agreement for communication between cloud and user[5].

3. Data Security:- On the level of basic security[8] of data it is provided by provider at some extend in terms of encryption . Data encryption is a process that helps to fix various external and malicious threats. Unencrypted data can be easily accessed by unauthorized users and these data is very vulnerable for susceptible data, as it does not provide any security mechanism. Unencrypted data risks the user data which leads to cloud server to escape various data information to unauthorized users.

4. Loss of Control: This is one of the major issues for security where customer hosted their data, application and resources on the cloud provider side. Users don't have specific control over his data so it might be possibility for provider to use data for any manipulation which can be which issues. Every time Cloud provider takes backup of data and place this data at different data centers by that time user can't predict where that data is actually place or whether data is on their original place [3]. So user can loss control over the data and it could be say that provider unable to manage resources precisely.

5. Trust Chain in Clouds: Trust plays an important role in attracting more consumers by assuring on cloud providers. Due to loss of control, cloud users rely on the cloud providers using trust mechanisms as an alternative to giving users precise control over their data and cloud resources. Therefore, cloud providers build confidence amongst their customers by assuring them that the provider's operations are certified in conformity with organizational safeguards and standards.

6. Data confidentiality:- For the user to store data on cloud is very trust work and data confidentiality is important to store private and confidential data. Authentication and access control strategies are used to ensure data confidentiality [6]. As user trust on cloud provider for storing their data but it is impossible to trust blindly for sensitive data. For data protection some basic encryption techniques are used on key level but for complex need other solution need to be used.

4. CONCLUSION

Cloud Computing is a huge change from the conventional way businesses think about IT resources. There is no escape form cloud technology to not use for personal or business work. In development of cloud computing there is also stoppers about data storage and privacy. It is always true that no any technology is hundred percent trustful it need to find alternative solution for the problems. This paper surveyed on some of issues about data security and privacy on cloud. Number of techniques have been given by some researchers to get more security for data however it having some spaces to be filled to make these techniques more productive.

REFERENCES

[1] Nabeel Zanoon, Abdullah Al-Haj, Sufian M Khwaldeh " Cloud Computing and Big Data is there a Relation between the Two: A Study" in International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 17 (2017) pp. 6970-6982

[2] Rohan Jathanna, Dhanamma Jagli "Cloud Computing and Security Issues" Int. Journal of Engineering Research and Application ISSN : 2248-9622, Vol. 7, Issue 6, (Part -5) June 2017, pp.31-38

[3] Ali Gholami and Erwin Laure "BIG DATA SECURITY AND PRIVACY ISSUES IN THE CLOUD" in International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.1, January 2016

[4] Monjur Ahmed and Mohammad Ashraf Hossain "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD" in International Journal of Network Security & Its

Applications (IJNSA), Vol.6, No.1, January 2014

[5] S.Subbalakshmi, Dr. K.Madhavi "Security challenges of Big Data storage in Cloud environment: A Survey" in International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 17 (2018) pp. 13237-13244

[6] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu "Data Security and Privacy in Cloud Computing" International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages.

[7] Rongxin Bao, Zhikui Chen, Mohammad S. Obaidat "Challenges and techniques in Big data security and privacy: A review" wileyonlinelibrary.com/journal/spy2 , Published on: 22 March 2018 DOI: 10.1002/spy2.13.

. [8] I. Ahmad, H. Bakht, and U. Mohan, "Cloud Computing – Threats and Challenges", Journal of Computer Management Studies, vol. 1, no. 1, 2017. Journal of Computer Management Studies, vol. 1, no. 1, 2017.

Journal of Engineering Sciences