# Data Securities and Challenges in Cloud

Kiran Rafi, Syeda Iqra Sajjad, Babur Hayat Malik
Department Of CS/IT
University of Lahore Chenab Campus
Kiranrafi764@gmail.com, Iqra.mashdi111@gmail.com, baber.hayat@cs.uol.edu.pk

**Abstract--** Big data is the collection of structure and unstructured both type of data. The main purpose of using big data is to minimize the security, storage and also increase the power and availability of data. Different terminologies, techniques and methods are used for the security in big data. The challenges include, encapsulate, storage, search, sharing, transfer, analysis, and visualize. Big Data have the many features i.e. volume, velocity, variety and value etc.[6]. Different challenges in cloud security are found in different environments level included user level, data level, physical level, network level etc. Security can be delicate by different attacks from attackers or intruders. The most predictable attacks are: wrapping attacks, malware, DDOS, Man in the Middle etc.

IP Spoofing, Port Scanning, Packet Sniffing Security is also one of the main issues that have to face in Big Data. In this paper first I over look on big data properties, security issues included long term viability and data availability, authentication level, data level and Generic type. The possible security approaches by using possible solutions for the three mostly probable.
Attacks i.e. wrapping attacks, malware-injection attacks and flooding attacks are also discussed.

**Key words**: Big Data, Cloud Security, Wrapping Attack, cloud challenges, Flooding Attack, DDOS

## 1. Background

BIG Data is used to describe huge sizes of organized and unorganized data that are so large. It is very problematic to procedure this data using old-style databases and soft wares. The word big data is the businesses that had to request roughly unorganized very large circulated data. Different challenges have to face for maintaining the data security, storage, sharing, analysis and visual data [1].

Big Data have the following properties [5]

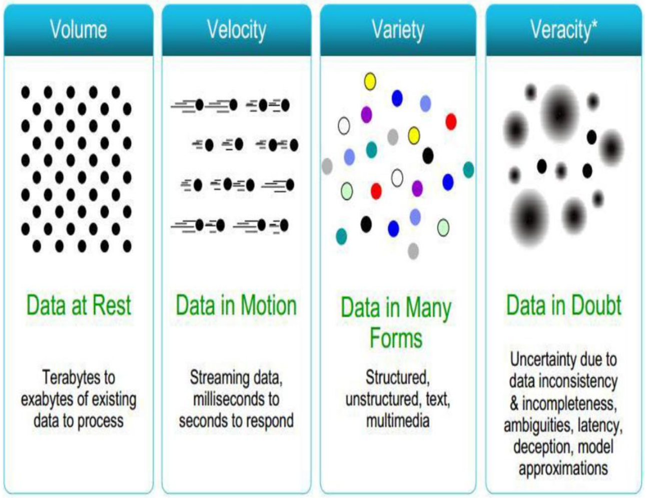
Volume
Velocity
Variety
Veracity*
Data at Rest
Data in Motion
Data in Many Forms
Data in Doubt
Terabytes to exabytes of existing data to process
Streaming data, milliseconds to seconds to respond
Structured, unstructured, text, multimedia
Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations

Figure1: [5]

## 2. Security issues

Cloud computing comes with many issues like performances, storage, optimism, flexibility, transition from legacy systems. One of main issue is security [2].

### 2.1 Long term feasibility

What security measure or conversion happens to the data security of cloud if vendor goes out of business in client's data returns and what format?

## 3. Data availability

Can the cloud vendor move all their clients' data on a different framework. Should the existing environment become compromised?

We describe the three another main types of issues.

- Traditional security
- Data Availability
- Third party data access

### 3.1 Traditional security

It include attacks in different levels mainly involves in networks attacks. This security layer have to face several issues like user-authentication, data authorization, virtual level attacks, phishing cloud supplier, forensics cloud , enlarge network attacks. These attacks broke down the speed and the security of cloud .

### 3.2 Data Availability:

These issues are created on specific application level. Different terms of issues and security failure are concern in it such as Uptime of sever, data integrity, single point of failure, denial of services, consistence's, cloud availability and many more[2].

### 3.3 Third party data access

is a legal issue in this concern lack of control and visibility of data by adding the third party influences, ear-drooping, or by accessing cloud data.

## 4. Challenges of security in cloud

The challenges of security in cloud computing platform can be categorized into several Levels included network, user authentication, data-integration level, and generic issues. [1]

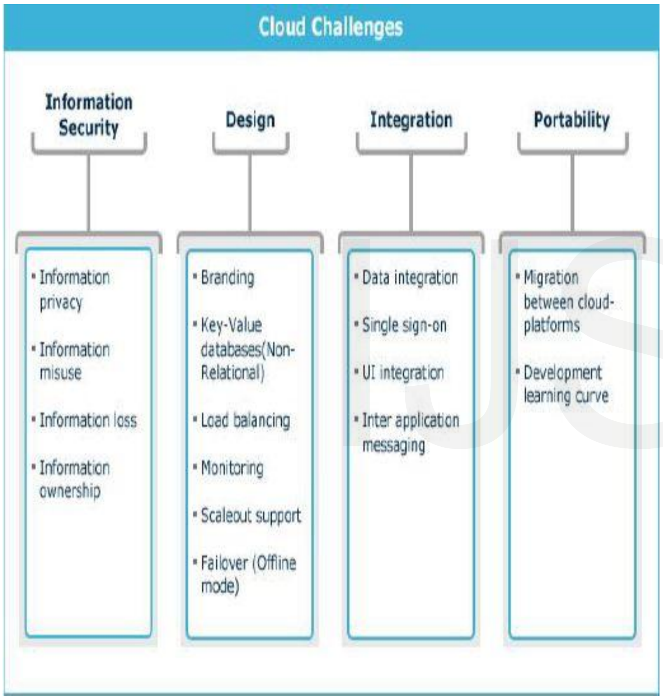

Figure 2: [2]

### 4.1 Network level

This type of challenges deals in network level. Different protocols and techniques are used to maintain security included distributed nodes, data, inter-nodes, denial of nodes access.

### 4.2 Authentication level

Different hurdles and challenges that can be faced at user authentication level for securing the unauthorized access of user inside the cloud. This authentication deal by using different methods and technique includes data duplication, administrative access for nodes, application nodes verification, encrypt and decrypt techniques (cyber, cryptography) and different logging methods.

### 4.3 Data level

These security challenges are classify at data level. The data level deals with data atomicity, consistency, accuracy, integrity and reliability. These challenges that have to face data level layer include data security, projection, data administration, back up and data distribution [5].

### 4.4 Generic types

These challenges are sort with traditional tools of security by the use of various terms and techniques

## 5. Research Challenges and Multidisciplinary Approaches

The problem of security issues in big data confronts many research challenges and approaches. We highlight some suggestive points that are described flowing:

## 6. Data Confidentiality:

Many researches, terminologies and mechanisms exist about data confidentiality but most common term which is widely includes control system access and encryption of data. The imprecise approaches of control system access are:

- Integrate the access of control policies for large amount of data.
- Authentication at particular level for getting permission about accessing big data.
- At administrative level implement control policies for accessing diverse multi-media data.
- Implementing control access policies in big data warehouses.
- Sets control access policies for automatically updating the changing in data.

Different privacy preserving techniques are also defined for maintaining the security matters. These technologies secure both public and private data. It may use many policies level agreements for securing data at data publications, different models and frameworks are design for this purpose.

## 7. Possible security approaches

The three mostly probable attacks are wrapping attacks, malware-injection attacks and flooding attacks. The direction of research on cloud computing security will be shaped differently in the next decade with the assumption of increasing events of security abuse about the users and providers of the cloud computing in the near future. Hence, the discipline of cloud computing security seems to be evolved swiftly along with striving to handle the distinctive chucks and abilities concerned with privacy and security issues caused by the evolution of this new paradigm. Technically, the development made in this field mainly deals with attacks and hacking challenges which are related to cloud computing providers and systems [11]. Cloud Computing give great services.

It has also many threats of security attacks i.e. malware attacks, wrapping attacks and flooding attacks etc. we have discussed in our paper [12].

### 7.1 Wrapping Attack

The user messages to his VM, it goes firstly to the browser server. In the server a message is created called SOAP message. The information between the server and the browser is interchanged. Before the processing the XML need some of standard roles and to be signed. So the signature values are open and the SOAP message gets all necessary information [13].

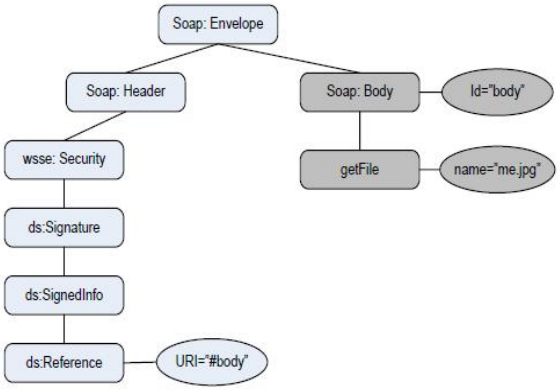

Figure 3 SOAP message before attack [14]

### 7.2 Flooding Attack

Flooding attacks can be stopped by simple approach i.e. by establishing a group of all servers in cloud as a convoy of servers. Each convoy will have a specific job i.e. one server will do file management and the second will do data management. So the servers will be untouched with each other by sending and receiving messages. In this case if a server is filled then a new server will be developed and that will have all necessary requirements [13].

### 7.3 Malware-Injection Attack

In a malware-injection attack, a challenger effort to insert malevolent service or code. It seems as one of the valid sample services of the cloud. If the attacker is successful, then the cloud service will hurt from a great hacking challenge eavesdropping. The attacker will capable to change the functionality or causing gridlocks by small changings. It will be the time consuming process for the user who waits until the job is completed. The attacker implements his services in such a way that it will run in IAAS or SAAS of the cloud servers, for example, delete Users and set Admin Rights. This type of attack is called spoofing attack [13].

## 8. Discussion Security

All types of attacks that are related to the data in transportation applies to cloud based services are man in the middle attack, eavesdropping, phishing, sniffing etc. [15]. A cloud computing state can be expressed in three classes i.e. service manipulators, service, and the cloud benefactor [11].

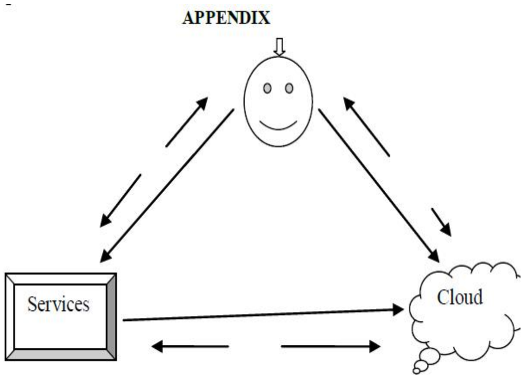

Figure 4 [11]

- An image of the customers VM in the image source system of the cloud is provided by the worker when the clients open account in the cloud. All applications are measured with high productivity and integrity which the users open. Contemplation of the integrity in the hardware level should be occupied into account, because it is very hard for an attacker to interject in the IAAS level [17].

- The modest attack that malicious code can achieve on a virtual machine challenger is to perceive it. As more security scholars trust on virtual machine challengers, malicious code examples have appeared that are deliberately complex to the company of virtual machine contesters [18].

## 9. Conclusion:

Security is also one of the main issues that have to face in Big Data. In this paper first we over look on big data properties, security issues included Long term viability and Data availability. Organizations also have to face different security challenges at network level, Authentication level, Data level and Generic type. Also discuss the possible security Approaches by using possible solutions for the three mostly probable attacks: wrapping attacks, malware-injection attacks and flooding attacks.

## 10. References

[1] VenkataNarasimha Inukollu1 , Sailaja Arsi1 and SrinivasaRao Ravuri3 International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014

[2] Sanjana Sharma, SonikaSoni, Swati Sengar Patel institute of technology,Bhopal ,School of computer science and IT,DAVV indore, shri ram college of Engineering and management, Gwalior August 11-12,2012

[3] L. Ertaul1, S. Singhal2, and G. Saldamli3 1Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA 2Mathematics and Computer Science, CSU East Bay, Hayward, CA, US 3MIS, Bogazici University, Istanbul, TURKEY

[4] International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 2, Volume 2 (February 2015) RaghavToshniwal* KanishkaGhoshDastidarAsokeNath

[5] Aarti A Gangawane Department of Computer Science & Engineering V.V.P Institute of Engineering and Technology Solapur University, Solapur

[6] G GeethakumariAgrima Srivatsava Dept. of Computer Science IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.4, August 2012

[7] The Participants of the NSF Big Data Security and Privacy Workshop (September 16-17, 2014) http://csi.utdallas.edu/events/NSF/NSF%20workshop%202014.htm Track Chairs: Elisa Bertino and Murat Kantarcioglu Workshop Chair: BhavaniThuraisingham DRAFT October 16, 2014

[8] Vishakha V. Kharche1, Prof. Alokkumar Shukla21 *Post Graduate Student, Department of CE, Padm. Dr. V.B.K.C.O.E., Malkapur, S.G.B.A. University, Maharashtra, India Asst. professor, Department of CSE, Padm. Dr. V.B.K.C.O.E., Malkapur, S.G.B.A University, Maharashtra,* 1vishakhakharche@gmail.com2alokjestshukla@gmail.com

[9] Kazi Zunnurhain1, and Susan V. Vrbsky2 Department of Computer Science The University of Alabama kzunnurhain@crimson.ua.edu; vrbsky@cs.ua.edu

[10] Attacks on Virtual Machine emulators, symantec advanced threat research Peter Ferrie, *Senior Principal Researcher, Symantec Advanced Threat Research*
4, Issue 5, May 2015

11. International Journal of Innovative Research in Science, Engineering and Technology *(An ISO 3297: 2007 Certified Organization)* Vol. Overview of Attacks on Cloud ,Ajey Singh, Dr. ManeeshShrivastava/Computing/International Journal of Engineering and Innovative Technology (IJEIT)/Volume 1, Issue 4, April 2012

12. Cloud Computing: Threats, Attacks and Solutions/Parveen Kumar/ International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 4, Issue 8, August (2016) www.ijeter.everscience.org

13. Security Attacks and Solutions in Clouds/ KaziZunnurhain, Susan V. Vrbsky/ The University of Alabama/ Tuscaloosa, AL 35487-0290/ kzunnurhain@crimson.ua.edu, vrbsky@cs.ua.edu

14. Security in Cloud Computing, Kazi Zunnurhain1, and Susan V. Vrbsky2, The University of Alabama

15. Cloud computing and security issues in the cloud, Monjur Ahmed1 and Mohammad Ashraf Hossain2 Dhaka, Bangladesh. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014 DOI : 10.5121/ ijnsa. 2014. 6103 25

16. Security threats on cloud computing vulnerabilities International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013 DOI : 10.5121/ijcsit.2013.5306 79 Te-Shun Chou East Carolina University, U.S.A.

17. Cloud computing attacks: a discussion With solutions Shikha singh1*, binaykumar pandey2, ratnesh srivastava3, neha rawat4, Poonam rawat5, awantika6 Open journal of mobile computing and cloud computing india*corresponding author: Volume 1, number 1, august 2014 Open journal of mobile