Security Issues in Cloud Computing and their Solutions: A Review

Sabiyyah Sabir
Department of Computer Science & Engineering
University of Engineering & Technology (UET)
Lahore, Pakistan

***Abstract*—Cloud computing is an internet-based, emerging technology, tends to be prevailing in our environment especially computer science and information technology fields which require network computing on large scale. Cloud computing is a shared pool of services which is gaining popularity due to its cost effectiveness, availability and great production. Along with its numerous benefits, cloud computing brings much more challenging situation regarding data privacy, data protection, authenticated access etc. Due to these issues, adoption of cloud computing is becoming difficult in today's era. In this research, various security issues regarding data privacy and reliability, key factors which are affecting the cloud computing, have been addressed and also suggestions on particular areas have been discussed.**

Keywords—Cloud computing data protection; encryption; digital signature; security issues

I. INTRODUCTION

Cloud computing or cloud-based environment is a service that is internet based and that gives the facility of sharing computer resources along with other devices on demand. It is a mechanism to enable on demand shared resources. For example, server, data center, networks storage applications which can store data. That can be generated with minimum effort. Cloud computing provides the facility to the organizations and users to keep their data on private or third-party storage location and these location/data centers may be located far away from user may be in some other city or country in the world.

National institute of Science and Technology (NIST), gives the cloud computing's definition as "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

Figure 1 shows the characteristics of cloud services which help others to understand and comprehend the cloud computing in a better way. These characteristics are explained as under [2]:

A. *On Demand Self-Service:*

It refers to the service which enables provisioning of cloud resources to vendors on demand or whenever they are required such as network storage, service time without the interaction of human.

B. *Broad Network Access:*

Services are accessible over the network which are retrieved through some standardized mechanism which promotes the usage of heterogeneous platforms (workstations tablets, laptops, mobile phones).

C. *Resource Pooling:*

Resources of cloud Provider are pooled over server. Consumers are assigned different resources which are either physical or virtual one. Generally, consumer have no idea of exact location the resources provided to them except at the abstraction level like; state, country or data center.

D. *Rapid Elasticity:*

Services can be elastically released and monitored, for consumers services available to them can often appear as unlimited which can be scaled in quantity anytime.

E. *Measured Services:*

Cloud system are so designed that they can monitor the resources usage; for example, processing, bandwidth and active user accounts, storage to deliver transparency to provider as well as consumer. At some level of abstraction, they can optimize the resource usage by keeping a check through metering capability.

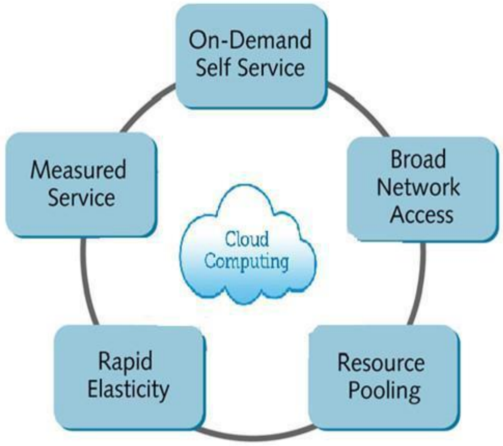

Fig. 1. Cloud Computing Characteristics.

Paper is divided into following sections; section tells about introduction of cloud computing, section II tells about the cloud computing models, section III is related work, section IV is factors affecting cloud computing, section V possible threats regarding cloud computing, section VI is about solutions to the security issues and section VII concludes the paper.

II. Cloud Service Models

Following service models are defined by

NIST which includes three categories [3]:

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

Figure 2 explains the overall three models of cloud computing which are served to the clients according to their needs. These models are explained as under:

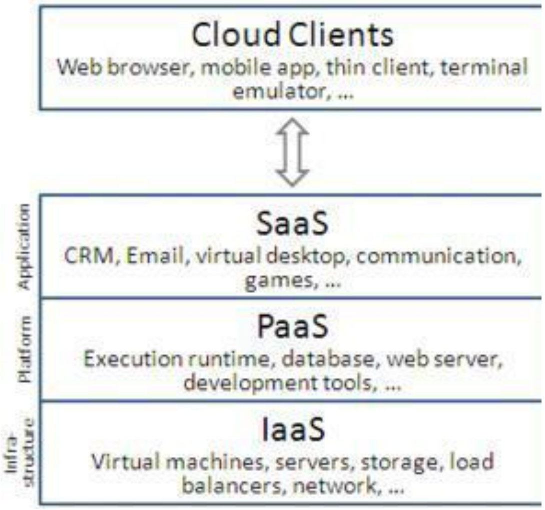
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig. 2. Different Cloud Service Models.

A. Infrastructure as a Service (IaaS):

Iaas is all about providing the virtual machine, operating system or networks to the end users. Some other computing resources are also supported in IaaS, where the customer or client can run arbitrary operating system on virtual machines or any other software. Clients can control only the operating system or the software which he is running but he loses his control on the infrastructure which is providing him all these services.

B. Software as a Service (SaaS):

In this kind of scenario, user is only using the applications which are being provided by the vendor and those applications run on the cloud services. Same application is accessible by many other clients as well through some common mechanism, for example by using web browser, or email. Again, the clients or users have no control over the application or underlying infrastructures, network server or operating system upon which these applications run.

C. Platform as a Service (PaaS):

In PaaS, the client is able to create their own desired application by using some programming language, linked libraries. These languages or libraries are supported by the vendor. After creating the user desired application, it is deployed on the server provided by the vendor. User has also the authority to configure its application or can change the configuration settings later on.

The benefits of cloud computing might be very appealing but it has got huge number of risks and security issues like data leakage, data loss, intruders attacks, malicious insiders etc.

III. Related Work

Ayush Agarwal et al. (2016) highlight the emergence of cloud computing along with its security concerns like data loss, data breaches, insecure API's, account hijacking, denial of service [4]. Prachi Garg et al. (2017) have worked on different cloud security aspects like basic security which includes Cross site scripting attacks, Sql injection attacks, Man in the middle attacks [5]. Pradeep Kumar Sharma et al. (2017) security concerns for cloud like cost model charge model [6], service level agreements and issue of migration should be dealt. Naseer Amara et al. (2017) highlighted the security threats, architectural principles and cloud security attacks with their techniques that can minimize the effects of malicious attacks (mitigation techniques) [7]. Sh. Ajoudanian et al, (2012) said that following four parameters were the most crucial. (a) Data Confidentiality, used to avoid leakage of information to any unauthorized individual or system [8].

IV. Factors Affecting Cloud Security

There are numerous key factors which may affect cloud computing performance because it is surrounded by many technologies e.g load balancing, network, concurrency control, virtualization, operating system, database, memory management etc [9]. Figure 3 shows these concerns which are discussed as above.

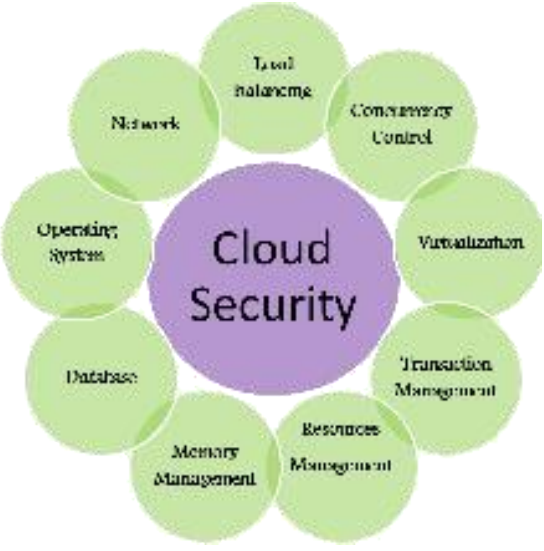

Fig. 3. Factors Affecting Cloud Security.

The security factors of these technologies affecting the cloud computing are appropriate e.g. network which connects the cloud computing to the outer world has to be secured. Virtualization concept has to be carried out securely when mapping with the physical systems. Load balancing involves the handling the incoming requests traffic which sometimes overloads the server. Data mining algorithms can be applied to cope with malicious attacks.

V. Possible Threats Regarding Cloud Computing

Nowadays cloud computing is getting so much popularity that it is in the limelight of today's era. Along with its huge benefits cloud computing is facing much security issues which need considerable attention to resolve them for the betterment of this service. Following are the major concerns as described below [10];

- **Outsourcing:** in outsourcing the data, consumer might get lose the control. Some kind of appropriate mechanism is needed to prevent the cloud service provider (CSPs) to use the data against the consent of their clients.
- **Multi tenancy:** cloud is a shared pool of resources. Protection of data must be taken into account while providing the multi-tenant environment.
- **Service Level Agreements:** a clear contract between the consumer and provider is needed. The main goal of agreements is to build the trust.
- **Heterogeneity:** different cloud providers have different mechanism of data protection which leads to integration challenges.
- **Server Downtime:** Downtime is the time in which the system starts responding to the client after some service failure. Downtime should be kept minimized and power backups must be installed to keep downtime minimum.
- **Backup:** Data uploaded by the clients, should be backed up in case of any service failure. Cloud Seller should mention in SLAs that in case of any disaster, what should be the remedy or solutions to such problems. There are very rare chances of whole system failure like flood etc.
- **Data Redundancy:** Data redundancy is a situation in which same data is being kept on two different places. In case of cloud computing, it can be understood as to provide copies of same data, systems or equipment to the clients. cloud seller should try to keep data redundancy minimum.

VI. Solutions To Security Challenges In Cloud Computing

Security challenges in cloud computing need to be addressed properly. If appropriate solutions are not being provided adoption of cloud environment becomes more difficult. Apart of adoption, data transmission and operation tend to become more tedious. Figure no.4 elaborates that data protection and privacy is the most crucial factor among all [11].

Figure 4 elaborates the overall impacts of security concerns. The major security challenge is about data leakage and data segregation because cloud is a shared pool of resources. The next bigger challenge is to prevent the data leakage.

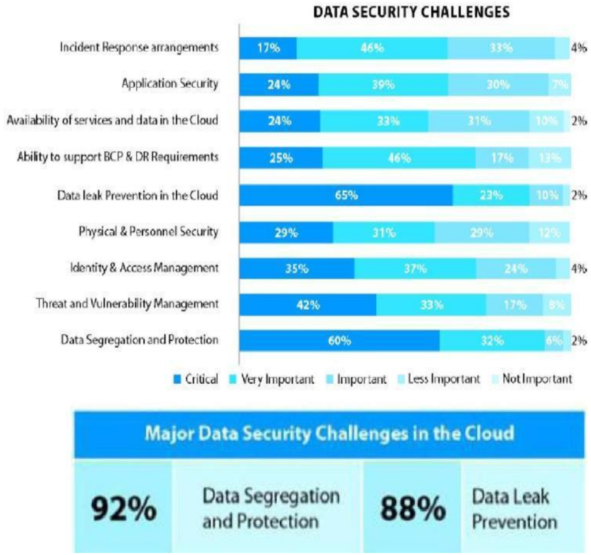

Fig. 4. Data Security Challenges.

To cope with the above challenges, following are some solutions which needs to be considered while considering about cloud computing security challenges;

VII. Data Encryption

Encryption is said to be a better approach regarding data security. Data should be encrypted before sending it to cloud. Data owner can permit some particular members to have access to that data [11]. The file or data being sent to cloud should be encrypted first then before storing it on cloud it should be again encrypted by the cloud provider; the process is known as multistage encryption. It has been observed that combination of different encryption algorithms provides better encryption on data. Experimental results show that RSA+IDEA gives the higher performance of encryption in securing the data [12].

VIII. Legal Jurisdiction

When it comes to understand and analyze the legal jurisdiction of cloud computing, the very basic aspects of cloud environment complicate the data protection. e.g presence of internet, virtualization, dynamically distributed data, multinational elements. Consumers, normally do not know that where their data resides in cloud. For example, a client from india may be using a server deployed in US, using an application which has been developed in japan and storing his crucial data at a data center which is physically located in Switzerland [13]. So, the resource allocated to the consumers should be marked to make sure that data is segregated.

IX. Distributed Denial Of Service (DDos)

Distributed Denial of service is a kind of attack in which attacker creates some zombie machine by infecting the machine over the internet. Then these infected machines are used to attack on victim. When attacks/traffic from so many infected machines are directed towards one victim, its resources like CPU, bandwidth and memory starts getting exhausted and that particular resource becomes unavailable for consumers. To cope with this Deepali [14] has introduced a layer named as fog layer which sits in between cloud server and user. All the requests made to server are filtered through this fog layer and DDOS attacks get minimized.

X. Digital Signature

Digital signature is powerful tool for securing data in cloud computing. Mr. Prashant Rewagad [15] has proposed a solution using digital signature to secure data along with Diffie Hellman key exchange with AES encryption algorithm. Diffie Hellman key exchange facility marks it useless if the key is hacked in transmission because it is useless without private key of user, which is confined to legitimate user only. This three way mechanism which is proposed in this paper makes it harder to hack security system, therefore, protecting the data that resides in cloud.

XI. Conclusion

This paper gave the overview of cloud computing, its various security aspects and keys factors which are affecting the cloud security. Cloud consumer and provider should be sure that their cloud is fully protected. Cloud computing is growing in every industry but it suffers from certain issues regarding security and protection which are a hurdle in its adoption widely. Solutions to these problems have been suggested which can be used for better performance of cloud service.

References

[1] Cloud Computing Definition. 2011; Available from: https://www.nist.gov/newsevents/news/2011/10/final-version-nist-cloud-computing-definition-published.

[2] Mell, P., Grance, T, The NIST definition of Cloud Computing, version 15 National Institute of Standards and Technology (NIST), Information Technology Laboratory. October, 2009.

[3] what is cloud computing? how it works.

[4] Agarwal, A., S. Siddharth, and P. Bansal. Evolution of cloud computing and related security concerns. in 2016 Symposium on Colossal Data Analysis and Networking (CDAN). 2016.

[5] Garg, P., S. Goel, and A. Sharma. Security techniques for cloud computing environment. in 2017. International Conference on Computing, Communication and Automation (ICCCA). 2017.

[6] Sharma, P.K., et al. Issues and challenges of data security in a cloud computing environment. in 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). 2017.

[7] Amara, N., H. Zhiqui, and A. Ali. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2017.

[8] Ahmadi, S.A.a.M.R., A Novel Data Security Model for Cloud Computing. International Journal of Engineering and Technology, 2012. 4(3).

[9] Jahangeer Qadiree, M.I.M., Solutions of Cloud Computing Security Issues. International Journal of Computer Science Trends and Technology (IJCST), April 2016. 4(2).

[10] Shahzad, F., State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. Procedia Computer Science, 2014. 37: p. 357-362.

[11] Rao, R.V. and K. Selvamani, Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 2015. 48: p. 204-209.

[12] Chennam, K.K., L. Muddana, and R.K. Aluvalu. Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in cloud. in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017.

[13] Sony, R., K. Sri, and D. Bhukya, Data Protection and Cloud Computing: a Jurisdictional Aspect. 2013. 81-91.

[14] Deepali and K. Bhushan. DDoS attack defense framework for cloud using fog computing. in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2017.

[15] Rewagad, P. and Y. Pawar. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. in 2013 International Conference on Communication Systems and Network Technologies. 2013.