Addressing Security in Cloud Federation: A Review

Bijeta Seth, Surjeet Dalal
Department of Computer Science & Engineering, SRM University, Sonepat, Haryana, India
Department of Computer Science & Engineering, SRM University, Sonepat, Haryana, India

Abstract: Cloud computing is an upcoming paradigm which is set to revolutionize the information technology by having several benefits related to economic aspects. To utilize the cloud computing to its full extent, data is transformed, processed and stored by external cloud providers having no control on the data. Hardware and software resources cost can be reduced by shifting the infrastructure of the network. Nevertheless, one has got to be cautious to comprehend the security threats and challenges posed in adopting cloud computing. In this document, major security considerations; issues, threats and challenges which are currently faced in cloud computing are listed. Security implications in service models and delivery models are considered and security solutions are provided. A comparison between cloud using companies is discussed. Real life scenarios facing cloud attacks are discussed.

Keywords: *Cloud, Security, Challenges, Issues, Threats, Security attacks, Security solutions*

I. INTRODUCTION

We are hasty approaching a novel digital age in which we accumulate our data and execute our high-priced computations vaguely on remote servers-the "CLOUD", in accepting idiom. The Cloud can be termed as an exceptionally broad, phrase that includes numerous approaches, providing outsourcing of all types of hosting and computing resources. Cloud has common characteristics and a set of services and it is found as the result of existing five technologies such as distributed computing, utility computing, virtualization, web 2.0 and service oriented computing. A compilation of self-governing computers to assist its users as a distinct rational system is termed as distributed scheme. The rationale of distributed systems is to allocate and consume resources in a proficient manner. This is factual in the state of Cloud computing, where the resources are rented to users. Mainframe Computing, Cluster Computing, and Grid computing are the three major milestones behind distributed systems. Virtualization is a supplementary expertise in Cloud computing, which includes a cluster of solutions, allowing the generalization of the essential rudiments for computing. This practice is used in Cloud computing to offer a strategy for scaling applications on demand, such as Google AppEngine and Windows Azure. Service orientation is the mainstay configuration of Cloud computing, which adopts the notion of services as the foremost criteria for application and system. Utility computing is termed as a service provisioning representation for computing services in which hardware and software resources are packaged and accessible on a pay-per-use basis.

The paper is structured as follows: The following section will focus on analyzing the essence of cloud computing; its description, service models and deployment models. Segment 2 explains the security in a cloud environment in detail illustrating the security issues, challenges, and threats for adopting cloud computing and their solutions. The report provides a comparison between different cloud providers in section 3. Section 4 is the case study of attacks. Conclusion comprises the last part of paper.

a) Characteristics, benefits, and cons of cloud computing

Cloud computing proves as a boon to its customers because of its attractive features. Its advantages catch the attention of organizations to store their data, but it nevertheless suffers from various disadvantages. The following figure depicts cloud computing paradigm mentioning its characteristics, advantages, and disadvantages.

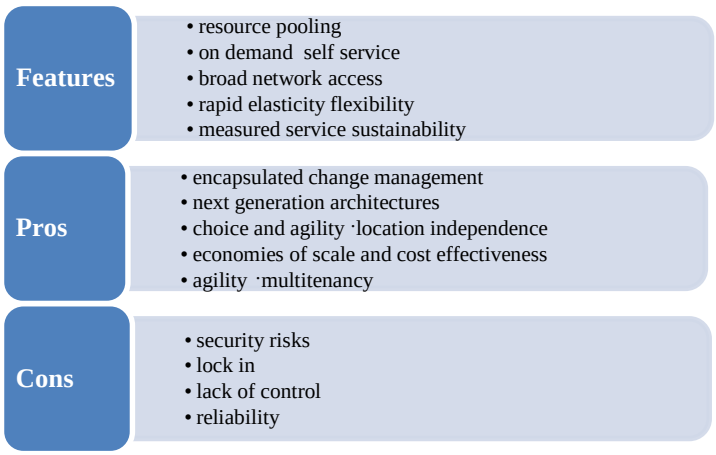

Figure 1: Cloud Computing Paradigm

b) Delivery models

Cloud services can be provided as four basic cloud delivery models which are as follows:

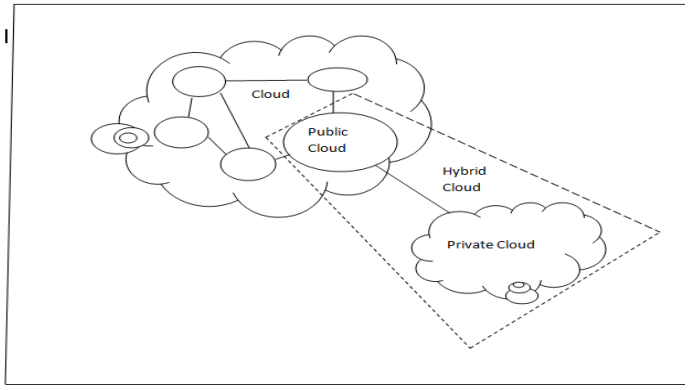

Figure 3: Cloud Delivery models

The public cloud provides the interface between the unrestricted customers & the owner group (third party), for example, an Amazon cloud service where numerous enterprises are proficient of functioning at the same instant. It is more cost effective, highly reliable & flexible and location Independent. But they are less secure & customizable. **Private cloud** affords the services merely for an organization in an exclusive manner. For example, CIO/G6. It offers high security and more control in comparison of public clouds. **Community cloud** provides the services for the specific groups instead of whole public groups. For example, Government or G-Cloud. Cost effectiveness and more security are the advantages of using community clouds. **Hybrid cloud** is formed by combining any of the public, private or community clouds. For example, CIO/G6/APC+ Amazon EC2. Enhanced scalability, security, and flexibility are the advantages of this model. But it faces networking issues and security compliance.

c) Cloud Service models

Three service models comprise the cloud architecture solutions, described beneath:

1) **Software as a service (SaaS):** It allows the customer to have an application for lease from cloud service provider instead of buying, installin and running software. For Example, Gmail Docs.

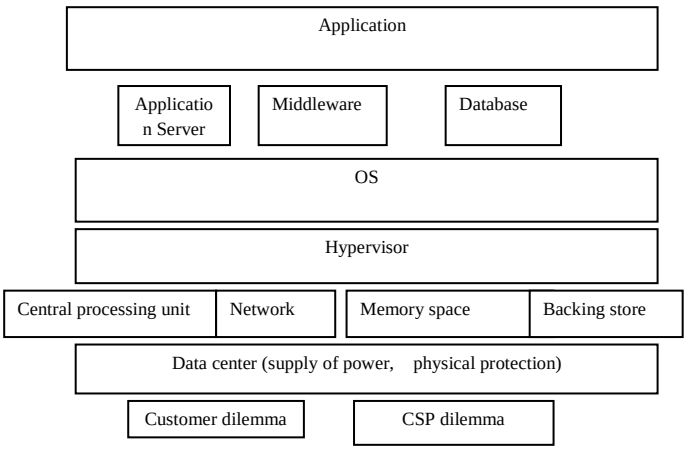

Figure 2: Software as a Service

2) **Platform as a service (PaaS)**: It provides a juncture to the clients upon which applications can be prepared and executed in the cloud. For Example, Windows Azure.

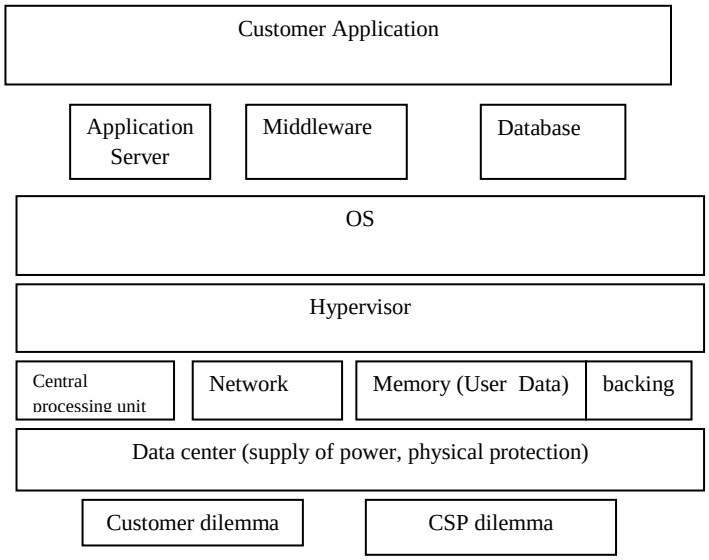

Figure 4: PaaS model

3) **Infrastructure as a service (IaaS):** Users can exploit the resources on-demand from the accessible pool of resources installed in data centers. For example, Elastic cloud Compute.

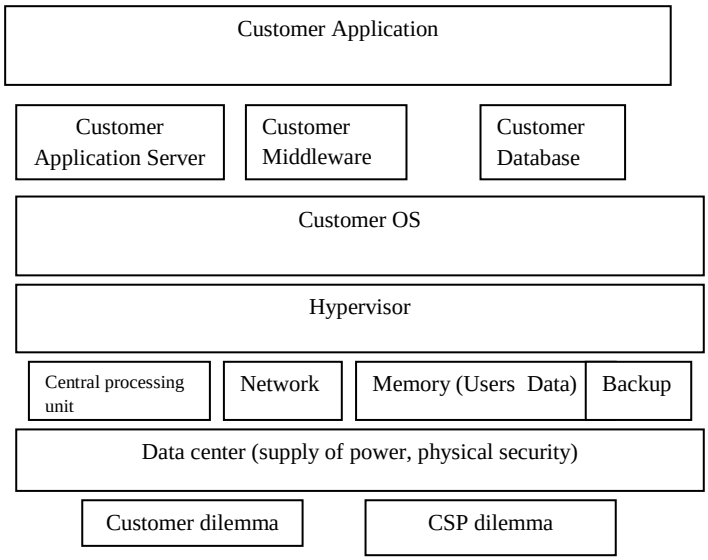

Figure 5: Infrastructure as a Service

The cloud technology reference model depicted above report that the Customer problem includes issues related to the creation, growth, failure, abort of any application along with testing, monitoring, diagnostics and verification of customer application. The cloud service provider acting as a third party has the responsibility of resource management, basic monitoring and hardware and software infrastructure management.

II. SECURITY IN CLOUD ENVIRONMENT

The implication of security is ample. Security combines Confidentiality, the preclusion of the unofficial revelation of data, Integrity, the avoidance of the illegal alteration or removal of information, and Availability, the deterrence of unauthorized custody of the data. The notion of handling important data to a third party is worrisome and the customers must be cautious in discerning the risks of information breaches. This segment introduces a comprehensive analysis of security issues, challenges, threats, the security implications in service models and delivery types along with solutions provided for security.

Why is cloud computing security considerable?

1) Escalating tradition of cloud services in non-traditional sectors.
2) The budding espousal of cloud services in administrative departments.
3) The increase in cloud service attacks.
4) The emerging practice of cloud services planned for decisive data storage.

Figure 5 illustrates the Specific customer concerns related to security whereby protecting and safeguarding the private data have been ranked topmost among all the other factors.

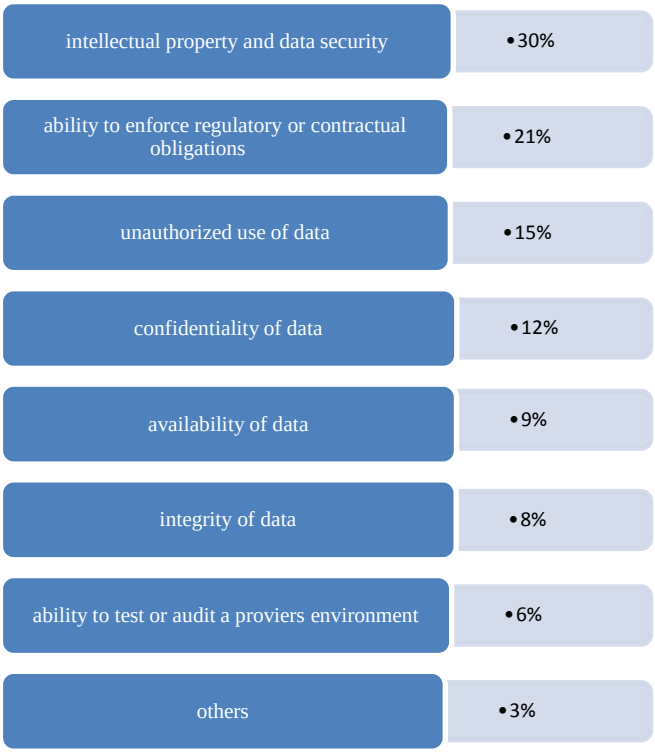

Figure 6: Customer concerns related to Security

Source: Debtite Enterprise@ Risk: Privacy and Data protection study, 2007

2.1 Challenges

The contemporary acceptance of cloud computing is unified by several challenges since the customers are still incredulous regarding its legitimacy. Following are the major challenges that crop up in the adoption of clouds:

- **Outsourcing** –Privacy violations can occur as the customers actually lose control on their data and tasks.
- **Multi-tenancy** – New vulnerabilities and security issues can occur because of the shared nature of clouds between multiple customers.
- **Massive data and Intense computation** –Traditional security mechanisms can't be applied to clouds due to large computation or communication overhead.
- **Heterogeneity:** Integration problems arise between diverse cloud providers using different security and privacy methods.
- **Service Level Agreement:** A negotiation mechanism between provider and consumer of services need to be established to ensure the consumer about the superiority, accessibility, consistency, and performance of the computing assets available for their business needs.
- **Costing charges:** Although infrastructure cost has reduced using clouds, the data communication cost still exists. The cost per unit of computing resource increases of the transfer of data, particularly in the scenario of the

hybrid cloud where company's information is scattered among public/private/community clouds.

- **Charging mode:** A deliberate and feasible charging model based on consumption of static computing, redesign and development of software, etc. for Software providers is critical for productivity and maintainability.
- **Interoperability issues:** This has become an obstacle for customers to opt from substitute offering concurrently to optimize assets at diverse stages in a group. Standardization appears to be an answer to interoperability challenges.

Security is regarded as the dominant barrier amongst the nine challenges in accordance to the survey done by IDC in August 2008 existing in clouds as publicized in Table 1.

Table 1: Challenges/Issues in the clouds [Rittinghouse, 2009]

S.No.	Challenge/Issue	%age
1.	Security	74.6
2.	Performance	63.1
3.	Availability	60.1
4.	Hard to integrate with in-house IT	61.1
5.	Not enough ability to customize	55.8
6.	Worried on demand will cost more	50.4
7.	Bringing back in-house may be difficult	50.0
8.	Regulatory requirements prohibit cloud	49.2
9.	Not enough major suppliers yet	44.3

2.2 Cloud computing security issues

There are following security issues as given below:

- **Trust:** The CSP is required to provide sufficient security policy to reduce the risk of data loss or data manipulation.
- **Confidentiality:** The confidentiality can be breached as a division or storage of information on isolated servers is done in cloud computing which is accessed through the internet.
- **Privacy***:* refers to the willingness of a user to manage the revelation of private information. An illegal admittance to user's sensitive data may bring security issues.
- **Integrity:** is to guarantee the precision and uniformity of data. Therefore, the Cloud service provider should provide security against insider attacks on data.
- **Reliability and availability:** Trustworthiness of cloud service provider decreases when a user's data get leaked.
- **Authentication and authorization:** To prevent unauthorized access, software is required outside the organization's firewall.
- **Data Loss:** Exclusion or amendment of data lacking any backup could lead to data loss.
- **Easy Accessibility of Cloud:** Cloud services are able to be applied by anybody through a straightforward registration model. This opens a chance to access services for the crafty minds.
- **Long term viability:** What happens to the information if the cloud dealer goes out of business, how are consumer records returned and in what specific arrangement?
- **Data seizure:** Company providing service may violate rules and laws, which may result in a risk of data seized by a foreign government.
- **Policy integration:** Different tools used by different cloud servers to ensure data security may cause major integration issues.
- **Audit:** is required as the cloud service provider might use the records himself while processing. Thus, all user activities must be traced. But large amounts of data are being stored in the cloud, so it is very difficult to audit everything.
- **Virtualization:** In cloud computing, the resources are requested, utilized and the relinquished on demand by the service provider. The data and application are generally controlled by a single cloud service provider which may cause various security related risks.

2.3 Cloud security threats

Cloud computing, undoubtedly represents one of the most significant shifts in the way we use the internet. Basically, the major threat for employing any efficient security scheme is created by the tasks expected from the clouds. Beneath are certain threats faced by the organizations while deploying a cloud security system.

1) **Mistreatment and despicable use of data:** Cloud computing suffers from attackers because of their relatively weak registration system which fails in providing efficient fraud detection capabilities. Thus, a suite of strong security solutions is desired.
2) **Malicious insiders:** The level of access and ability to infiltrate organizations and assets by malicious insiders decide the damage to financial and productivity losses. The consumers must recognize what the providers are doing to detect and safeguard against malicious insiders. The broad-spectrum lack of precision and the convergence of services under a single executive sphere amplify the threat to achieve entire control over cloud services or harvest confidential data from malicious users.
3) **Insecure interfaces and application programming interfaces:** A range of protection issues in an organization associated with confidentiality, integrity, and availability occur because of the weak set of interfaces and API's. Functionalities like provisioning, orchestration, management, and monitoring are performed using the interfaces. New value added services being made using the interfaces to their customers often

increase the complexity of interfaces, which increases the level of complexity of the new layered API.

4) **Shared technology issues:** Vendors utilize cloud services by fully utilizing the resources in a scalable way. The unauthorized access to data is made feasible by attackers from exploiting the shared hardware and software resources like shared disks partitions, CPU caches etc. in the storage servers. Customers should not have access permissions to access any other tenant data, network traffic etc.
5) **Lack of proper cloud security standards:** In the adoption of cloud services, unanswered questions may cause serious threats like details of internal security, storage of data and related logs and their permissions to access, what information will a vendor disclose in the occurrence of a security violation?
6) **Account or facility hijacking:** The damage and possible measures resulting from a breach to credentials can cause damage to vital areas of cloud computing services and negotiate the CIA to those services.

2.4 Security implications in delivery models

Cloud requires the primary constituent, security, which varies and is dependent on the deployment model that is used, the approach and its nature in which it is provided. Public cloud being used by multiple enterprises at the same time is comparatively less secure & customizable. Private cloud works for a private organization and thus provides high security and more control in comparison of public clouds. Community cloud provides the services for the communal concerns and has more security. Hybrid cloud is bound together by a consistent technology that allows information and application portability. Enhanced scalability, safety measures and flexibility are the advantages of this model. But it faces networking issues and security compliance.

The security endeavor of a cloud system is fundamental to guarantee accessibility of information transmitted amid or inside the participating parties, to sustain the integrity, thereby preventing data loss or amendment of data owing to illegally access and module malfunction, to authenticate the identity of communicating parties and to provide secure access to services and internetworking within the systems. According to a survey done by IBM, figure 6 mentions the security implications in delivery models.

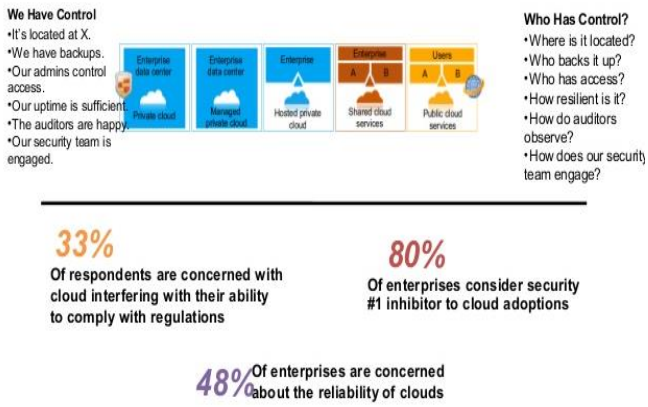

Figure 7: Security Implications in Cloud Delivery models Source: Driving Profitable Growth through Cloud Computing, IBM Study, 2008.

2.5 Security implications in service models

Internet is used to transmit data in cloud. The issues allied with safekeeping data on the internet are also obligatory by the cloud. Additionally, the three comprehensive models of cloud computing IaaS, PaaS, and SaaS acquire a diverse impact on application protection. However, when any application is hosted in a cloud environment, in a typical application, two chief security questions that occur are:

1) How protected is the data?
2) How safe is the code?

Type of service	Security provided by the cloud service provider	Extensibility
SaaS	Greatest	Least
PaaS	Least	Greatest
IaaS	Intermediate	Medium

Figure 8: Security for the Cloud Service Models

The cloud service provider becomes less responsible for providing security when moving down the stack; the security implementation and management becomes the responsibility of the customers.

a) *Security issues in SaaS:*

SaaS model provides its clients with considerable profits such as enhanced functioning effectiveness and reduced expenditure, but, suffers from the issue of providing no transparency to its users regarding storage of data. The client, thus having to rely on the provider for suitable security techniques. Security should be considered as the key element in SaaS. Following figure 9 depicts some of the key security essentials that need to be cautiously measured to guarantee security of data because it provides security related to data location, data segregation, data

confidentiality, data location, authorization and authentication, data recovery and backup, data integrity, data access, net application safety, information breaches, susceptibility in virtualization, network security and backup process.

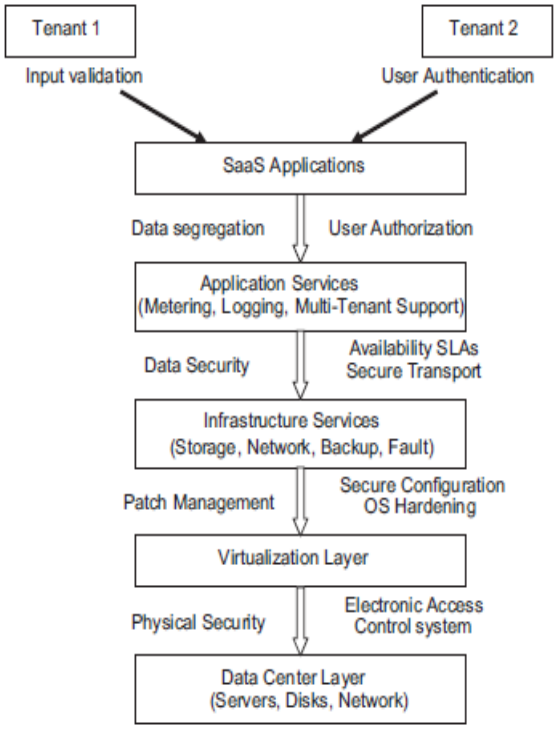

Figure 9: Security for the SaaS stack [Subashini, 2011]

In a simple scenario, For Amazon Elastic Cloud Compute (EC2) administrators, secure shell (SSH) keys are vital to achieve access control of an individual. To avoid illegal access to data, it is encrypted before uploading to Amazon S3 using a Simple Storage Service (S3) and uses SSL encrypted endpoints to secure the network in order to evade outflow of receptive information. Network security issues are also protected in AWS.

b) ***Security in PaaS:*** In PaaS, a cloud service provider gives some authority to the individuals to construct applications on the top of the platform. It is more extensive than SaaS at the cost of customer controlled features. Vulnerabilities are related to the device to device SOA, web applications and are affected by a security hole in virtualization manager.

c) ***Security issues in IaaS:*** In case of no security fissure in the virtualization manager, the developer has enhanced authority over the protection. Security issues in IaaS generally affect the visible running code, web applications and device to device SOA and affect the infrastructure by extensive blackboard testing. The complexity allied is because of the deployment models as depicted in the table 2 below where CSP is the Cloud Service Provider.

Table 2: Deployment model characteristics

Model type	Infrastructure managed by	Owner of the infrastructure	Infrastructure location	Dedicated hardware	Access and consumption
Public	CSP	CSP	Off-premise	No	Untrusted
Private (external)	CSP	CSP	Off-premise	Yes	Trusted
Private (internal)	Internal group	Internal association	On-premise	Yes	Trusted
Community	CSP	CSP	Off/On-premise	Yes	Trusted
Hybrid	Both organization and CSP	Both organization and CSP	Off/on premise	Depends on contract with CSP	Trusted and Untrusted both

A dynamic set of agreements and secure protocols are obligatory to facilitate the protected communication of information in the cloud.

2.6 Security attacks:

Although cloud service providers offers tremendous benefits to users, security attacks may still occur in cloud computing environment which may cause users to hesitate to trust on the service providers. Following are some of the most emphasized concerns related to the Cloud security.

1) **Authentication attack:** Because of the weak authentication system used in hosted and virtual machines, they are very prone attacks on any server.
2) **The Man in the middle attack:** This type of assault occurs whilst an invader tries to interfere and places himself between two users in any communication system and harms the system by modifying or intercepting data and infuses false data.
3) **Denial of service attacks:** because of shared nature of data in the cloud, it is more vulnerable to this kind of attack. We can't reach a particular site because of the overburdening of the server with the solicitations to get to a particular site. An Example of such an

attack occurred in 2009 when Twitter suffered a devasting DoS attack.

4) **Side Channel attacks:** Cloud security can be breached by inserting a malicious virtual machine in immediacy to the intended cloud server and subsequently harming through this attack.
5) **Network security:** Because of insecure SSL trust configuration and session management weakness, network security can be breached by network penetration and packet analysis.
6) **Web Application Security:** It is compromised due to insecure direct object references, cross-site scripting, insecure cryptographic storage space, unrestricted URL access, and insecure transport layer safety.

2.7 Cloud security solutions

Cloud computing is a novel style of computing theory, moving from personal computers to a "cloud" of computers providing dynamically scalable and virtualized resources over the Internet. Numerous efforts have taken place to present guidance for cloud security which is somewhat recent and has yet to achieve broad recognition. These include:

1) **McAfee Incorporation:** SaaS delivers protection to secure business to organizations by providing a comprehensive security and integrated management by delivering complete email, web protection, vulnerability management, and endpoint protection, thereby saving time, effort and cost of an organization.
2) **SWOT Analysis:** company's cloud access control provides provisions like the Single sign on (SSO), strong authentication and audit, centralized management and reporting and auto synchronization of identity data between an enterprise and cloud applications. It also provides a secure platform for email, web, etc. However, it suffers from speed limitations and market threats from other security solutions.
3) **Netfix:** it serves as a distributed system and provides capacity planning and procurement, key management and embeds new security controls.
4) **Cloud Security Alliance (CSA)** gathers and groups solutions for non-profit organizations and individuals for providing information guarantee in the cloud.
5) **Open Web Application Security Project (OWASP)** provides an updated record of cloud based vulnerabilities.
6) **Open Grid Forum** security and infrastructural specifications and information for grid computing developers and researchers are published in a document.
7) **The Trusted Computing Group (TCG)** formed the Trusted Multi-tenant Infrastructure Work Group projected to build up a security framework utilizing the existing standards for compliance and auditing.
8) **The Federal CIO Council's** planned Security Assessment and Authorization for U.S. Government Cloud Computing which adopted the NIST 800-53R3.
9) **Cloud Audit:** Cloud operators can check the security of cloud services by tools using interface and namespace.
10) **Cloud Controls Matrix:** Gives detailed understanding of security concepts and principles aligned to the CSA in 13 areas.

III. COMPARISON OF CLOUD PLATFORM

Depending on the nature and size of an enterprise, cloud services are being applied to an organization. Following table 3 provides the comparison of significant features offered by various cloud providers in the industry including IBM, Rackspace and Bluelock, Windows Azure, Google App Engine and Amazon AWS.

Table 3: Comparison between different companies

Parameter	**IBM**	**BlueLock**	**Rackspace**	**Google AppEngine**	**Amazon AWS**	**Windows Azure**
Cloud services	SaaS, PaaS, IaaS	SaaS, IaaS	IaaS,PaaS,SaaS	PaaS	Paas,IaaS	PaaS, IaaS
Data security	Encrypting and management of the keys protect the data.	NET APP virtual storage console for consistent backups with VMware virtual machine, and array based snapshots at NET APP	Antivirus, Firewall and encryption of SSL is being used to protect data against worms and Trojans	Java JVM, Go compiler and Python run in secured "sandbox" environment to isolate application for service and security	Host,guest operating system is provided with a complete firewall protection. Amazon S3 is protected with SSL encrypted endpoints. Simple DB can be protected by domain level controls by API	Well-built storage keys, SSL support are used
Physical security	Security is safeguarded by using biometrics access control and closed circuit television to protect cloud infrastructure	Biometric authentication for access control and video recordings are used for providing physical security.	Biometric scanning and security cameras for protection against unauthorized access is provided.	Electronic card access control, Alarm systems, cameras, Perimeter fences and biometrics may be used.	Two or more levels of two factor authentication, robust perimeter control, strictly controlled physical access.	Motion sensors, biometric controlled access system, video camera protection, security breach alarms. Two factor

						access controls are provided.
Application Security	Suspension and demolition of images must be done carefully	Dedicated VLANs provides isolation from all clients. Firewalls at enterprise level and application level provide security against intrusion detection and protection	Expert database administrators are hired to provide optimal performance, monitoring and troubleshooting and emergency response services	Internal traffic is monitored for suspicious behavior, monitor public mailing list, blog posts	Unix/Linux configuration, AWS Multifactor authentication, CloudWatch logs is used to collect and monitor system performance	Provided by .NET framework code, windows account with least privileges
Operational security	Security provided by encrypted passwords	Authorization log of remote access methods, firewalls, patch management and security policy auditing software are used to provide reports for managing virtual servers	Encrypted passwords and system access log files created and managed for auditing purpose	No direct access to memory, file system, protected protocols HTTPS are used.	Unique security credentials, multifactor authentication	Rigorous data handling procedures and hardware disposal methods are used
Privacy	IBM Infosphere Optim and InfoSphere Gurdium solutions are provided for data security and protection	Registration procedure, e-newsletter, cookies, service related announcements are provided for security	Portfolios of private cloud solutions are provided for private cloud and training provided to employees on documented informat	Unique user id assigned to each user using two-factor authentication mechanism like certificates, one time passwo	Root account or IAM user account, X.059 certificates, access keys is used	9 step incident response, contractual commitments are made. Focuses on containment and recovery.
			ion security and privacy	rds. Also, password policies are used like password expiration and sufficient strength, password reuse restriction mentioned.		
Network security	Deploy network security measures by implementing intrusion and anomaly detection, encryption, management and access restriction	Managed firewall, intrusion detection, VPN and network antivirus are used	Network policy enforcement controls, including unicast reverse path forwarding protocols, automatically provisioned hypervisor controls are used. Two network interfaces are used: front/public and secondary interfaces	Network firewall, ACL rules management done for peer review, automated testing and network segregation. Routing of external traffic through custom front-end servers stop malicious requests, Generate high priority alerts in event of logs of programming errors	Secure network Architecture by using firewalls, Access control lists, secure access points, SSL protocol used by HTTP/HTTPS to connect to AWS access point, the AWS ticketing system used.	Traffic limit to VMs using a host firewall, network isolation by configuring endpoints for required access and packet filters are used

IV. CASE STUDIES

Many real-world scenarios where cloud computing was compromised by attacks and their feasible prevention methods are listed below in table 2.

Table 4: Case Studies

Type of attack	Definition	Example	Solution
XML Signature Wrapping Attack	Wrapping attack inserts a fake element into the signature and then makes a web service request.	In 2011, Dr. Jorg Schwenk discovered a cryptographic hole in Amazon EC2 and S3 services.	A proposed solution is to use a redundant bit called STAMP bit in the signature in the SOAP message.
Malware Injection	Hacker attempts to insert malicious code by inserting code, scripts, etc. into a system.	In May 2009, four public websites were set offline for the BEP in which hackers introduced undetectable iFrame HTML code that redirected guests to a Ukrainian website.	Web browsers like Firefox should install NoScript and set Plugins The FAT table can be used to determine the validity and integrity of the new instance.
Social Engineering Attack	It depends on human interaction, thereby breaking normal security procedures.	On August 2012, hackers completely destroyed Mat Honan's digital life by deleting data from his iPad, iPod, and MacBook by exploiting Amazon and AppleID Account of the victim.	Apple forced its customers to use Apple's online "iForgot" system to provide stronger authentication. Various account settings like a credit card, email addresses can't be altered on phone by Amazon customer service head.
Account Hijacking	It compromises confidentiality, integrity, and availability by stealing credentials of accounts.	In July 2012, UGNazi entered CloudFare's personal Gmail account by exploiting Google's email and password recovery mechanism.	CloudFlare has stopped sending password reset and transactional messages for security purpose.

V. CONCLUSION

Certainly Cloud Computing will sustain Information systems as the profits outnumber its limitations. The Cloud can be termed as a huge pool of easily usable and reachable virtually and dynamically reconfigured resources which aim to provide optimum resource utilization by exploiting pay-per-use model. The above discussion shows that security is the prime hindrance in the adoption of cloud computing and it is obligatory to be provided by Cloud Service Providers. In this document, generic security issues, challenges, and threats along with its solutions are recognized so that security can be constructed on the trust mitigating protection of a trusted third party. Cloud computing has the latent to turn out to be a leader to grant a protected, effective and reasonably achievable IT solution in the prospect. As a prospect dimension to this work, the investigation will be conducted for creating a potent and robust tool so that information can be stored, maintained, restructured, retrieved efficiently and securely.

VI. REFERENCES

[1]. Subshini S., A Survey on security issues in service delivery models of cloud computing, J. of Network and Computer Applications 34 pp. 1-11 doi: 10.1016/j.jnca.2010.07.006 Elsevier 2011.

[2]. Esther T., A survey on secured storage of data and consequent issues in Cloud Computing, Int. J. of Computing, Communications, and Networking, Vol. 3 Issue 3 pp. 33-39 ISSN: 2319-2720 2014.

[3]. Kanwal Ayesha, Evaluation and Establishment of Trust in Cloud Federation, Int. Conference on Ubiquitous Information, Management and Communication (IMCOM) doi: 10.1145/2557977.2558023 2014 ACM.

[4]. Habib S., Towards a Trust management System for cloud computing, Trust, Security and Privacy in Computing and Communications (TrustCom) pp. 933-939 IEEE 2011.
[5]. Kumar V., Cloud Computing: Towards Case Study of Data Security Mechanism, Int. J. of Advanced Technology & Engg. Research (IJATER) ISSN: 2250-3536 Vol 2 Issue 4 2012.
[6]. Kuyoro S., Cloud Computing Security Issues and Challenges, Int. J. of Computer Network (IJCN) Vol 3 Issue 5 2011.
[7]. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 Dec, www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf 2009.
[8]. Sravani K., Effective Service Security schemes in Cloud Computing, Int. J. of Computational Engg. Research Vol. 3 Issue 3 ISSN: 2250-3005 2013.
[9]. Evaluating Cloud Security: An Information Security Framework Chapter 9 from Securing the Cloud,doi: 10.1016/B978-1-59749-592-9.00009-9 pp: 232-252 Elsevier 2011.
[10]. Ismail S., Security Issues and Solutions in cloud Computing-A Survey, Int. J. of Computer Science and Information Security, Vol.14(5) pp.309-315 2016.
[11]. Zissis Dimitrios, Addressing Cloud computing Security issues, Future Generation Computer Systems, doi:10.1016/j.future.2010.12.006 Elsevier 2010.
[12]. Rittinghouse J.: Cloud Computing: Implementation, Management, and Security. ISBN 9781439806807. CRC Press, pp.154 (2009).
[13]. Zahir T., Security and Privacy in Cloud Computing, IEEE Cloud Computing RMIT University. Vol.1 Issue 1 pp: 54-57 doi: 10.1109/MCC.2014.20 2014.
[14]. Xiao Z., Security and Privacy in Cloud Computing, IEEE Communications Surveys & Tutorials. Vol. 15 (843) 2013.
[15]. Aguiar, Z., An Overview of Issues & Recent Developments in Cloud Computing & Storage Security pp 1–31 Springer Berlin 2013.
[16]. Pearson, Privacy, Security and Trust in Cloud Computing, Privacy and Security for Cloud Computing pp: 3–42 doi: 10.1007/978-1-4471-4189-1_1. Springer 2013.
[17]. Charles N., A quantitative analysis of current security concerns and solutions for Cloud Computing, J. of Cloud Computing Advances Systems and Applications doi: 10.1186/2192.Vol. 1 Issue 11 pp: 1-11 Springer 2012.
[18]. Acklyn M., Cloud Service Security & Application Vulnerability, IEEE SoutheastCon pp: 1-8 doi: 10.1109/SECON.2015.7132979. IEEE. April (2015).
[19]. Diogo, Security issues in Cloud Environments, A Survey Int. J. of Information Security, pp: 113–170 Vol. 13 Issue 2 doi 10.1007/s10207-013-0208-7 Springer 2014.
[20]. Passent M., Security issues over some Cloud Models, Int. Conference on Communication, Management and Information Technology (ICCMIT), ScienceDirect, Procedia Computer Science Vol. 65 pp: 853-858 doi: 10.1016/j.procs.2015.09.041 ELSEVIER 2015.
[21]. Gagangeet Single Aujla, Rajat Chaudhary, Neeraj Kumar at al., "SecSVA: Secure Storage, Verification and Auditing of Big Data in the Cloud Environment", Imminent Communication Technologies for Smart Communities, IEEE Communications Magazine, doi:10.1109/MCOM.2018.1700379 pp:78-85 Jan 2018.
[22]. Ali Azhar, Malik Saif, Khan,"DASCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transactions on Cloud Computing, Vol. 5 No. 4 pp 642-655 IEEE 2017.
[23]. Hao Yan, Jiguo Li, Jinguag Han, Yichen Zhang," A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage", IEEE Transactions on Information Security, Vol. 12 Issue 1 doi:10.1109/TIFS.2016.2601070, pp:78-88 Jan 2017.
[24]. Kritikos Kyriakos, Kirkham Tom, Kryza Bartosz,"Towards a security enhanced PaaS platform for Multicloud applications", Future Generation Computing Systems, doi: http://dx.doi.org/10.1016/j.future.2016.10.008 Elsevier, 2016
[25]. Weinman Joe,"The Economics of the Hybrid Multicloud Fog", IEEE Cloud Computing, Cloud Economic Column, doi:2325-6095/17/$33.00@2017 IEEE 2017.
[26]. Dr. K. Subramanian, F. Leo John, "Secure and Reliable Unstructured Data sharing in Multi-Cloud Storage using the Hybrid cryptosystem", IJCNS, Vol. 17 No. 6 pp: 196-2016 June 2017.
[27]. Ibrahim Abaker, Hashem Targin, Gani Abdullah, Yaqab Ibrar, "The use of "Big Data" on Cloud Computing: Review and open research issues", Information Systems, Elsevier, pp:98-115, http://dx.doi.org/10.1016/j.js.201.4.07.006 2015.
[28]. Kolhar Manjur, Mosleh M., Abd El-atty ," Cloud Data Auditing techniques with a focus on Privacy and Security", doi: 1540-7993/17/$33.00@2017 IEEE , IEEE Computer and Reliability Societies,2017.
[29]. Balamurugan Balusamy at al.," A secured access control Techniques for Cloud Computing Environment using Attribute based Hierarchical Structure and Token Granting System", doi:- 10.6633/IJNS.2017.19(4).9,2017.
[30]. Srisakthi S. & Shanthi A. P., "Towards the design of a secure and fault tolerant cloud storage in a multicloud environment", Taylor & Francis, pp:-1-9, 2015.