IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, July 2015.
www.ijiset.com
ISSN 2348 – 7968

Study on Security Challenges in Cloud Computing

B.Vasumathi,
Assistant Professor,Department of Computer Science,
PGP College of Arts & Science,
Namakkal, TamilNadu, India.

Karthick
Student,Department of Information Technology
VSB College of Engineering and Technology
Karur,Tamilnadu,India

Vignesh
Student,Department of Information Technology
VSB College of Engineering and Technology
Karur,Tamilnadu,India

***Abstract*— Vendors offer a pool of shared resources to their users through the cloud network. Nowadays, shifting to cloud is a very optimal decision as it provides pay-as-you-go services to users. Cloud has boomed high in business and other industries for its advantages like multi-tenancy, resource pooling, storage capacity etc. In spite of its vitality, it exhibits various security flaws including loss of sensitive data, data leakage and few others related to cloning, resource pooling and so on. As far as security issues are concerned, a very wide study has been reviewed which signifies threats with service and deployment models of cloud. In order to comprehend these threats, this study is presented so as to effectively refine the crude security issues under various areas of cloud. This study also aims at revealing different security threats under the cloud models as well as network concerns to stagnate the threats within cloud, facilitating researchers, cloud providers and end users for noteworthy analysis of threats.**

Keywords*— *Security threats; SQL Injection; Malevolent users; Browser Security; Malicious Attacks; Data Leakage.

I. INTRODUCTION

Cloud Computing has emerged as a very well-known technique to support large and voluminous data with the help of shared pool of resources and large storage area.Cloud computing, indeed, is a wide-ranging term that transmits hosted services over the Internet. These hosted services are generally separated into three broad categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The internet is usually represented as the “Cloud”. A cloud service is generally used by the clients as and when needed, normally on the hourly basis. This “on-demand” or “pay as you go” approach makes the cloud service flexible, where end user can have a great deal or modest of a service the way they desire at any point of time and the service is entirely administered by the provider. Noteworthy improvements in each key components included virtualization, distributed computing and also the improved access to high-speed internet facility as well as weak economy have speeded up the inflate of cloud computing rigorously.

A cloud can either be a private or a public. Thus a public cloud sells services to any person residing on the Internet. At present, Amazon Web Services is the major public cloud provider. A private cloud is an authorized network or a data centre that provides hosted services to a restricted number of individuals. When a service provider uses public cloud resources to produce their private cloud, the result is called as a virtual private cloud. For a cloud computing, the main aim is to offer a scalable and a very easy admittance to computing resources and Information Technology services.

Cloud computing has spawned a very noteworthy interest in both academia and industry, but it is still a budding theory. In essence, it aims to combine the fiscal utility model with the evolutionary expansion of various existing advances and computing technologies. It even unites various distributed services, as well as applications and in¬formation infrastructures that consist of groups of com¬puters, storage resources and networks. Confusion exists in IT communities about how a cloud differs from existing models and how these differences af¬fect its adoption. Some visualize a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy and culture.

As cloud computing comprehends the idea of computing as an efficacy, providers are developing a mutual-shared group of configurable resources, which clients can vigorously condition and liberate according to their varying needs. Thus, both the group providers and the users would easily benefit from the reuse of computing resources and reduction in cost.

The cloud services that are implemented or those that will be implemented will always be accompanied by several threats. Knowledge about these threats shall prove to be the first step to prevent them. Hence security is the chief concern of several clients who desire to leverage cloud services. An easy example of this is the exercise of botnets to spread spam and malware. The other example is the application interfaces that are required to connect to cloud services especially that are developed by third parties. These interfaces must provide the user with highly protected authentication, authorization, encryption and movement monitoring mechanisms.

ISSN 2348 – 7968

Cloud computing is undeniably providing with different hosted services over the internet. These hosted services are broadly classified in three different service models, namely Infrastructure as a Service, Platform as a Service and Software as a Service which have been discussed as below:

A. Cloud Service Models:

As known, cloud computing provides with diverse hosted services. The various service models briefly discussed earlier have further been elaborated as below, to reveal their significance with a range of security threats further in the survey:

- Infrastructure as a Service (IaaS) also referred as Resource Clouds generally provide resources which are managed and can easily be scaled up, as services to a variety of users. They essentially supply superior virtualisation capabilities. Consequently, diverse resources may be offered via a service line: Data and storage clouds have to offer a dependable access to data of a potentially large size. The success rate of data access defines the quality of these cloud servers. As infrastructure can be dynamically scaled up or down based on the need of application resources, it helps to equip multiple tenants at the same time. Moreover, the resources that are used are generally billed by the providers on the basis of the computational usage by the users.

- Platform as a Service (PaaS) supply computational resources via a platform upon which applications and services can be urbanized and hosted. In other way, it supplies all the needed resources to build an application and service via the internet, without downloading or installing it. PaaS classically makes use of fanatical APIs to organize the performance of a server hosting engine which completes and replicates the execution according to consumer requests. As each supplier exposes their own API according to the individual key potentialities, applications developed for one precise cloud provider cannot be enthused to an additional cloud host; there are though attempts to make bigger broad programming models with cloud abilities.

- Software as a Service (SaaS): It is also referred to as Application or a Service Clouds. SaaS is the model which hosts the application as a service to its various cloud users via internet. The user utilizes the software out of the box without any integration or patching up with any infrastructure. Service clouds provide an implementation of explicit business functions and business processes as per the requirement. These applications are bestowed with unambiguous cloud capabilities using a cloud infrastructure or platform rather than providing a cloud for them. Repeatedly, types of standard application software functionality are obtainable within a cloud. One of the biggest benefits of SaaS is, it helps in costing less money than actually buying the application. It provides with cheaper and reliable applications to the organization.

The three cloud services described above attract some highly significant amount of threats. This includes modification of data without proper backup, leading to data breaches or unauthorized access to sensitive data. In case of proper data backup being taken, it is vulnerable if it is not encrypted properly. Unsecured access to resources over the cloud may lead to unauthorised usage of service, platform or even an infrastructure of the provider or other users due to the associated disadvantages of virtualization as discussed in later section.

As on date only few threats have been revealed but there still exists many a more threats that are yet unsolved. either service or deployment models. While this survey majorly covers the threats that are directly influencing deployment models, service models and various network security is one of the major chal¬lenges to the cloud and it is often a disturbing. There exist various researches dealing with security threats with security threats which are generally found the main cause for various security and data breaches.

The survey of related research work done on the cloud security (CS) challenges is discussed in the first half of the paper. In the second part of paper, the challenges to the CS are discussed in detail. The discussion spans the security challenges with respect to the type of deployment, service and common network issues. The next part comprises of the discussion and conclusions followed by the tables showing advantages and disadvantages of deployment models from view point of security and the vulnerabilities of different service models as appendices.

II. Challenges To Cloud Security

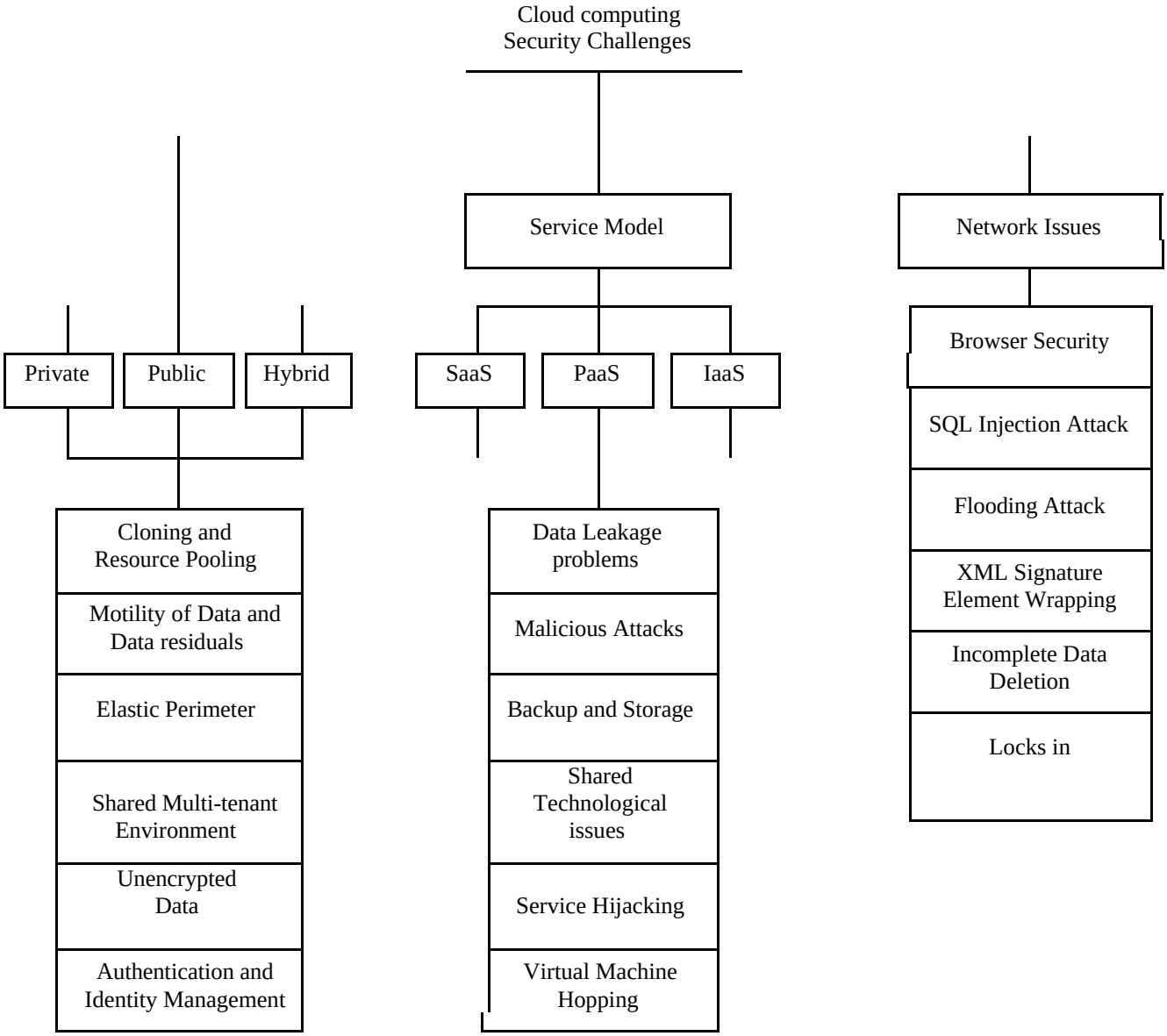
Security has been one of the most challenging issues for the IT executives particularly in cloud implementation. There exist numerous security anxieties that are preventing companies from captivating advantages of the cloud. Several studies, including the one by Amit Sangroya et al. [1] quote security as the primary level confront for cloud users. In this section taxonomy related to cloud computing security has been presented.

Fig. 1 represents the schematic diagram showing the hierarchy of the cloud computing, with security challenges on both the cloud computing models: Deployment and Service models and also the issues related to Networks.The classification provided above reveals various common challenges under cloud computing. The Deployment model is classified further as Private, Public and Hybrid Cloud and the security issues of the same have been exposed in

ISSN 2348 – 7968

common. Further, the Service model is classified into the SaaS, PaaS and IaaS briefing its security challenges in common. The security challenges with respect to network is also shown as for any internet based service, network is considered as the backbone for cloud computing.

Figure 1: Classification of Security Challenge



A. Deployment Models and its security challenges:

There exist three basic types of deployment models, namely Private, Public and Hybrid clouds. Private cloud model is generally deployed within an organization and is limited only for the internal access by individuals of that organization. Public cloud model is employed by the organization for gaining access to various resources, web applications, and services over any of internet, intranet as well as extranet. Hybrid cloud is the combination of two or more clouds (public and/or private). It is an environment providing multiple service suppliers, both internal and external.

ISSN 2348 – 7968

Various security challenges related to these deployment models are discussed below:

- Cloning and Resource Pooling: Cloning deals with replicating or duplicating the data. According to Bernd Grobauer et al. [2], cloning leads to data leakage problems revealing the machine's authenticity. While Wayne A. Resource Pooling relates to the unauthorized access due to sharing through the same network. While the study on Virtual and Cloud Computing by various researches states that a Virtual Machine can easily be provisioned, they can also be inversed to previous cases, paused, easily restarted, readily cloned and migrated between two physical servers, leading to non-auditable security threats.

- Motility of Data and Data residuals: For the best use of resources, data often is moved to cloud infrastructure. As a result the enterprise would be devoid of the location where data is put on the cloud. This is true with public cloud. With this data movement, the residuals of data is left behind which may be accessed by unauthorized users. According to Rohit Bhadauria et al. [38], data-remnant causes very less security threats in private cloud but severe security issues may evolve in public cloud donations. This again may lead to data security threats like data leakage, data remnants and inconsistent data, as stated by Hassan Takabi et al. [4]. The authors have also mentioned that in order to solve the problems with data storage the optimal solution of cryptography can be thought of effectively.

- Elastic Perimeter: A cloud infrastructure, particularly comprising of private cloud, creates an elastic perimeter. Various departments and users throughout the organization allow sharing of different resources to increase facility of access but unfortunately lead to data breach problem. In private clouds, according to Krishna Subramanian [5], the resources are centralized and distributed as per demand. The resource treatment transfers resources based on the requirements of the users thus leading to problems of data loss, where any user may try to access secure data with ease.

- Shared Multi-tenant Environment: Multitenancy as one of the very vital attribute of cloud computing, which allows multiple users to run their distinct applications concurrently on the same physical infrastructure hiding user data from each other. But the shared multi-tenant character of public cloud adds security risks such as illegal access of data by other renter using the same hardware. A multi-tenant environment might also depict some resource contention issues when any tenant consumes some unequal amount of resources. This might be either due to genuine periodic requirements or any hack attack. Hsin-Yi Tsai et al. [6], has shown that multi-tenancy makes the impact of VM Hopping attack potentially larger than conventional IT environment.

- Unencrypted Data: Data encryption is a process that helps to address various external and malicious threats. Unencrypted data is vulnerable for susceptible data, as it does not provide any security mechanism. These unencrypted data can easily be accessed by unauthorized users. Unencrypted data risks the user data leading cloud server to escape various data information to unauthorized users. For example, the famous file sharing service Dropbox was accused for using a single encryption key for all user data the company stored.

- Authentication and Identity Management: With the help of cloud, a user is facilitated to access its private data and make it available to various services across the network. Identity management helps in authenticating the users through their credentials. But a key issue, concerned with Identity Management (IDM), is the disadvantage of interoperability resulting from different identity tokens and identity negotiation protocols as well as the architectural pattern. While Jianyong Clien et al. [8] have mentioned that IDM leads to a problem of intrusion by unauthorized users. They even discussed that in order to serve authentication, apart from providing a password, a multi-factor authentication using smart card and fingerprint must be implemented for attaining higher level of security.

B. Service models and its security challenges:

Various cloud services like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are delivered and used in real time over the cloud. Bhaskar Prasad Rimal et al. [9] have mentioned SaaS as a multi tenant platform which is commonly referred to as Application Service Provider aiding distribution of services across cloud users. While the PaaS provides the developers a platform to work with all the environments and systems for the developing, testing and deploying web applications through the cloud service. The computer infrastructure needed for this application to run on a particular platform is provided by IaaS which may give more flexibility and pay-as-you-go scheme.

According to John Viegga [10], the users of SaaS have to rely heavily on the cloud provider for security purposes without any assurance to the data protection of users. In PaaS, the cloud providers offer some controls to the users building applications on their platform, without ensuring them the threats with network or intrusion prevention. While with IaaS, the developers have a better control over the application. This addresses proper security and compliance.

Various security challenges with the service models are discussed below:

- Data Leakage and consequent problems: Data deletion or alteration without backup leads to certain drastic data-related problems like security, integrity, locality, segregation and breaches. This would lead to sensitive data being

ISSN 2348 – 7968

accessed by the unauthorized users. As its measure provided by Rafael Moreno et al. [7], cloud platforms should provide new services in order to collect context information and to perform analysis and manage data privacy so as to support applications requesting the information. One solution to this data leakage problem, as provided by Danny Harnik et al. [13], is deduplication with allowing a limitation on number of user uploads per time window. The term deduplication means storing only a single copy of redundant data and providing just a link to this copy rather than storing actual copies of this data.

- Malicious Attacks: The threat of malicious attackers is augmented for customers of cloud services by the use of various IT services which lacks the lucidity between the procedure and process relating to service providers. Malicious users may gain access to certain confidential data and thus leading to data breaches. Farzad Sabahi [12] has shown malicious attacks by the unauthorized users on the victim's IP address and physical server. An access control mechanism tool can be thought of to control unauthorized user in accessing secured data. Peter Mell [41], has suggested Infrastructure as a Service as one of the models that exposes challenges with using virtualization as a frontier security protection to defend against malicious cloud users.

- Backup and Storage: The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats. As per the study carried by Intel IT center [42], more the server virtualization increases, a very difficult problem with backup and storage is created. Data de-duplication is listed as one of the solution to reduce backup and offline storage volumes. But discussing about de-duplication, Danny Harnik et al. [13], have shown that de-duplication in cloud storage is carried out with the misuse of data backup.

- Shared Technological issues: IaaS vendors transport their services in a scalable way by contributing infrastructure. But this structure does not offer strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, a virtualization hypervisor intercede the access between guest operating systems and the physical compute resources. As discussed by Perez R et al. [11], in spite of several advantages, these hypervisors have exhibited flaws that have permitted guest operating systems to expand inappropriate levels of control or authority on the underlying platform. This certainly led to security issues on the cloud. Lori M. Kaufman [14] has shown the implementation of IaaS by the customer to facilitate the infrastructure or hardware usage.

- VM Mobility: The contents of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering a hard drive. VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host. Several types of attacks might take advantage of weaknesses in VM mobility which includes man in-the-middle attacks. The severity of the attacks ranges from leaking perceptive information, to completely compromising the guest OS. Moreover, VM mobility augments the complication of security management because it offers augmented flexibility. In the IaaS model, a provider presents resources and underlying hardware as a service and a user can produce his or her possessed computing platform by importing a personalized VM representation into the infrastructure service. The huge scale of IaaS makes VM mobility's force on confidentiality and integrity in the cloud possibly outsized than in a conventional IT environment. According to B. Grobauer [2], a PaaS provider offers a variety of pre-configured computing platform and solution stacks to the service users. The users take advantage of the libraries and APIs to build up their individual applications on a permanent computing platform by importing their VM images. Although PaaS considers virtualization as a key implementation technology, it does not hold up VM mobility, therefore this service model is not having the same security challenges as a traditional IT environment. While the confidentiality, integrity and availability of PaaS, SaaS and DaaS (Database-as-a-Service) are still open to the elements, the threats rose from IaaS.

- VM Denial of Service: Virtualization lets numerous VMs split physical resources like CPU, network bandwidth and memory or disk. A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered. The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations. In cloud computing, DoS attacks could having service providers place sufficient configurations to put a ceiling on the resources owed to the VMs decreases their probability. Additionally, it is advisable to have the Service Level Agreement (SLA). This legally identifies responsibilities of the service provider and the user.

Various security threats with deployment and service models have been noticed. This makes us aware about the fact that cloud deals majorly with internet; and one need to examine various security threats with network as well. Thus certain basic issues related to network of cloud has been shown below.

C. Network issues on Cloud:

Cloud computing mainly depends upon internet and remote computers or servers in maintaining data for running various applications. The network is used to upload all the information. With the same aspect, H.B. Tabakki et al. [3] have stated security issues with network on cloud as a prime focus. It provides virtual resources, high bandwidth

and software to the consumers on demand. But in reality, the network structure of this cloud faces various attacks and security issues like cloud malware injection attack, browser security issues, flooding attacks, locks-in, incomplete data deletion, data protection and XML signature element wrapping, which are explained further below.

- Browser Security: Every client uses browser to send the information on network. The browser uses SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host. Steve Kirsch [16] states that in order to overcome this, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally.Web Services security (WS-security) concept on browsers work with XML encrypted messages which does not need to be decrypted at intermediated hosts.

- SQL Injection Attack: These attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information. Uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker is misread by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to easily access and modify the functioning of a website.

- Flooding Attacks: In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests. Cloud has a property to expand on the basis of large amount of request. It will expand in order to fulfill the requests of invader making the resources inaccessible for the normal users.

- XML Signature Element Wrapping: It is found to be a very renowned web service attack. According to Jamil [20], it protects identity value and host name from illegal party but cannot protect the position in the documents. The attacker simply targets the host computer by sending the SOAP messages and putting any scrambled data which the user of the host computer cannot understand. This would not let the user to understand the twisted data, thus misguiding and misleading the user.

- Incomplete Data Deletion: Incomplete data deletion is treated as hazardous one in cloud computing.when data is deleted, it does not remove the replicated data placed on a dedicated backup server. The operating system of that server will not delete data unless it is specifically commanded by network service provider. Precise data deletion is majorly impossible because copies of data are saved in replica but are not available for usage.

- Locks in: Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on data, application and service portability, not leading to facilitate the customer in transferring from one cloud provider to another or transferring the services back to home IT location.

In order to effectively utilize the cloud computing technology, the research community needs to take practical and positive measures to guarantee security. An association exists to assume universal standards to ensure inter-operability amongst service providers. The attempts to expand security standards to warrant data's Confidentiality, Integrity and Availability, together known as CIA, are incorporated in this effort. The network must be correctly trained to efficiently detect intrusions. Hence, one should count the network related issues and try to avoid them.

III.DISCUSSION

In Table – 1 of Appendix, the security issues with the deployment models of cloud computing that is private, public and hybrid cloud are shown. Even the pros and cons of the usage of these deployed models have been listed for reference.

In Table-2 of the Appendix, the threats and the impacts of cloud service model, in terms of virtualization attacks have been compared and revealed. As discussed earlier, various virtualization vulnerabilities exist and they have a huge impact on cloud services. These virtualization vulnerabilities are discussed with respect to four types of service models basically, Software as a Service (SaaS), Database as a Service (DaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The major security challenges are bifurcated on the basis of conventional environment falling into Confidentiality, Integrity and Availability (CIA).

As indicated in III. A., cloud computing security challenges with deployment models, viz., private cloud, public and hybrid cloud have been shown along with their advantages and disadvantages at a distant, from where the security issues can be gasped at a glance. It states the advantages and disadvantages of cloud computing deployment models differentiated in three types. In accordance to their pros and cons, various security issues were concluded, showing how and which model is more secured.

From Table – 2, it is concluded that, the threats associated with VM mobility reduces with the service model PaaS. There is no direct impact of virtual mobility on SaaS, but DaaS does get affected with security challenges mainly confidentiality and integrity. Thus, although virtualization still pretences cloud computing security threats

ISSN 2348 – 7968

some of the description of cloud service models can hold back definite virtualization vulnerabilities.

V. Conclusion And Future Work

Cloud computing has made end users both thrilled and edgy. They are excited by various opportunities provided by the cloud and are anxious as well on the questions related to the security it offers. As users migrate their data on cloud they would be alarmed with the security flaws inherent to the cloud environment. Thus security threats with cloud computing has emerged as one of the very plausible topics. This study has analyzed almost every security threat found across both the cloud models and the network and has also revealed solutions to some of them. This work will further be extended for creating a structured approach for conducting risk analysis in order to uncover security threats lying with the cloud deployed.

References

[1] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments", Springer-Verlag Berlin Heidelberg 2010, pp. 255-265.
[2] Bernd Grobauer, Tobias Walloschek, and Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities", IEEE, 1540-7993/11, 2011, pp: 50-57.
[3] H. Takabi, J.B.D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," Proc. 1st IEEE Int'l Workshop Emerging Applications for Cloud Computing (CloudApp 2010), IEEE CS Press, 2010, pp. 393– 398.
[4] Hassan Takabi and James B.D. Joshi, University of Pittsburgh, Gail – Joon and Ahn Arizona State University, "Security and Privacy Challenges in Cloud Computing Environments", IEEE security and privacy, www.computer.org/security, 2010, pp. 24 – 31.
[5] Krishnan Subramanian, "Private, Public and Hybrid Clouds", whitepaper: Trend Micro, 2011.
[6] Hsin-Yi Tsai, Melanie Siebenhaar and André Miede, Yu-Lun Huang, Ralf Steinmetz, "Threat as a Service? Virtualization's impact on Cloud Security", IEEE, IT Pro, 2012, pp: 32- 37.
[7] Rafael Moreno-Vozmediano, Rubén S. Montero, and Ignacio M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services", IEEE, Digital Object Indentifier 10.1109/MIC.2012.69.
[8] Jianyong Chen, Yang Wang, Xiaomin Wang, "On demand Security Architecture for Cloud Computing", IEEE, 0018-9162, Digital Object Indentifier 10.1109/MC.2012.120, pp: 1 -12.
[9] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing Systems", 978-0-7695-3769-6/09, IEEE, pp: 44 – 51.
[10] John Viega, "Cloud Computing and the Common Man", IEEE, 0018-9162/09, pp: 106 – 108.
[11] Perez R, van Doorn L, Sailer R. "Virtualization and hardware-based security". IEEE Security and Privacy 2008;6(5):24–31.
[12] Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486-2, IEEE, 2011, pp: 245 – 249.
[13] Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage", 540-7993/10, IEEE, 2010, pp: 40 – 47.
[14] Lori M. Kaufman, Bruce Potter, "Monitoring Cloud Computing by Layer, Part 1", 1540-7993/11, IEEE, pp: 66 – 68.
[15] Thomas Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199–212.

APPENDIX

TABLE I. Pros And Cons Of Deployment Models With Their Level Of Security

	Advantages and Disadvantages
Private Cloud	• Most control over data and platform • Latent for multi-tenancy of business units to cause fulfilment and defence risk • May not have convulsive abilities when added performance or capacity is required
Public Cloud	• Likely for better cost savings if infrastructure owned and controlled by public providers • Failure of control and data loss and platform • Possible for multi-tenancy with former organizations to reason security risk • Third party safety controls possibly not clear and may cause unidentified risks.
Hybrid Cloud	• Potential for difficulty to cause unfamiliar vulnerabilities and indefinite risks

ISSN 2348 – 7968

TABLE II. VIRTUALIZATION VULNERABILITIES WITH SERVICE MODELS OF CLOUD

Cloud Computing Environment and Security Conventional Environment		Virtualization (VM) Vulnerabilities		
		VM Hopping	VM Mobility	VM Denial-of-Service attacks
Software as a Service	Confidentiality	o	×	×
	Integrity	O	×	×
	Availability	o	×	×
Database as a Service	Confidentiality	✓	×	×
	Integrity	✓	×	×
	Availability	×	×	×
Infrastructure as a Service	Confidentiality	✓	✓	×
	Integrity	✓	✓	×
	Availability	✓	✓	×
Platform as a Service	Confidentiality	✓	×	×
	Integrity	✓	×	×
	Availability	✓	×	×

O → Indicates optional. Direct impacts are not possible, but indirect impacts may cause vulnerability.

× → Indicates reduced occurrence of the vulnerability.

✓ → Indicates presence of vulnerability.