An Analysis of Security Threats in Cloud Computing.

Muhammad Sadiq

Reg. No. F11C04G05006

RIPHAH INTERNATIONAL UNIVERSITY

Faculty of Computing

Islamabad

2015

An Analysis of Security Threats in Cloud Computing.

Muhammad Sadiq

Faculty of Computing
RIPHAH International University Islamabad, Pakistan

Thesis submitted in partial fulfillment of the requirements
for the award of degree of

Master of Science in Computer Science

Research Supervisor: ***Dr. Sheheryar Malik*** ***June, 2015***

DECLARATION

I, **Muhammad Sadiq** S/O **Muhammad Amin**, **Reg. No. F11C04G05006**, a student of MS in Computer Science at the Riphah International University do hereby solemnly declare that the thesis entitled "Cloud Computing Security Threats: and Guidelines. submitted by me in partial fulfillment of MS degree in Computer Science, is my original work, except where otherwise acknowledged in the text, and has not been submitted or published earlier and shall not, in future, be submitted by me for obtaining any degree from this or any other University or institution.

Date: **Student's Signature: _____**

ACCEPTANCE BY THE VIVA VOCE COMMITTEE

Title of Thesis: An Analysis of Security Threats in Cloud Computing.

Name of Student: Muhammad Sadiq

Dated : June 18, 2015

Accepted by the Faculty of Computing, Riphah International University, in partial fulfillment of the requirements for the award of Degree of Master of Science in Computer Science

Viva Voce Committee

External Examiner		_____
Supervisor	**Dr. Sheheryar Malik** Assistant Professor Faculty of Computing Riphah International University, Islamabad	_____
Incharge Graduate Programs – FC	**Dr. Sheheryar Malik** Incharge Graduate Programs Faculty of Computing Riphah International University, Islamabad	_____
Dean – FC	**Dr. Saad Naeem Zafar** Dean Faculty of Computing Riphah International University, Islamabad	_____

ACKNOWLEDGEMENT

First of all, I would like to express my sincere gratitude in the domain of Almighty Allah and then to the Riphah International University for letting me to fulfill my dream of being a student here. I would also like to thanks the Computer Science Department and Faculty Members for giving me the opportunity to complete my honorable MS degree. My deepest gratitude goes to my thesis supervisor Dr. Sheheryar Malik for being an extraordinary the best researcher who showed me the direction and helped to get me started on the path to complete my thesis. The enthusiasm, encouragement and faith in me throughout have been extremely helpful. He was always available for my questions; he was positive and gave generously of his time and vast knowledge. He always knew where to look for the answers to obstacles while leading me to the right source, theory and perspective. He has been actively interested and involved in my work and introduced different methodologies in different perspective which made me to think in broad minded. He has always been available to advise me. I am very grateful for his patience, motivation, enthusiasm, and immense knowledge. I would also like to thanks to Dr. Muhammad Yousuf for his kind support and i feel proud to work under his kind supervision also, my family and my friends who provided me support and encouragement throughout this study. I would also like to thank to my honorable teachers and guiders, without whom none of my success would be possible.

Declaration of Authorship

I, Muhammad Sadiq , declare that this thesis titled, 'An Analysis of Security Threats in Cloud Computing.' and the all work presented in it are done by myself . I also confirm that:

- This work was done complectly for the research degree at this University.
- Where work of this thesis partially or completely has previously been submitted for a degree or publication or any other qualification in this University or any other academia , the work has been clearly stated.
- Where I have consulted other published work, is always clearly attributed.
- Where I have mentioned from the work of other researchers and resources , the reference is always given. With the exception of such as mentioned quotations, this complete work completely my own.
- I have acknowledged and mentioned all main sources of help.

Signed:

Date:

Abstract

Cloud computing has become a widespread choice for the enterprises and individuals to fulfill their computing requirements. It offers variety of service types over the internet and enables its customer to have on demand, scalable resources available 24/7. Despite its many great advantages, a cloud computing environment possesses many security threats and trust related issues due to its shared (generally) nature.

Cloud computing faces similar threats as traditional computing. Contingent upon the administration and sending model embraced, tending to security hazards in the cloud may turn into an additionally difficult and complex undertaking. This circumstance subsequently speaks to the cloud suppliers the need to execute their key obligations of making a savvy as well as a protected distributed computing administration. Security is crucial for critical cloud computing services – one flaw can impact a wide range of organizations directly. From a logical perspective the cloud computing service is a single point of failure. .

In this study, we identify threats and security attributes applicable in cloud computing. We also identified the financial impact and reported incidents due to relevant threat and find out the weaknesses of system.

We conducted a literature Survey (LS) to identify studies focusing on information security threats in the cloud computing. We also identified the relevant threats with respect to Cloud Service model, Cloud deployment models and cloud computing components We used Engineering Village, Google Scholars and Scopus online citation databases as primary sources of data for literature Survey. In this study, we help both cloud supplier and clients on the security issues that are to be considered.

Keywords: cloud computing, security threats, literature Survey. ...

Acknowledgements

We would like to express our gratitude to our thesis supervisor,Sheheryar Malik, Ph.D whose expertise, guidance and support enabled us to develop understanding of the study. We would also like to thanks to Dr. Yousuf for his kind support and, our families and friends who provided us support and encouragement throughout this study. Without them we would not have been able to complete this thesis.. . .

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Cloud computing has become a widespread choice for the enterprises and individuals to fulfill their computing requirements. It offers variety of service types over the internet and enables its customer to have on demand, scalable resources available 24/7.Despite its many great advantages, a cloud computing environment possesses many security threats and trust related issues due to its shared (generally) nature. Security is very important for all cloud computing services because resource sharing is from central point, so one security flaw can fail whole system.

1.2 Motivation

The increasing demands of cloud computing added the new characteristic which is heterogeneity (Multi-tenancy) which implies use of same resources or applications by multiple consumer although they belong from same domain or from different domain [1].

Due to wide features cloud computing is going to be popular in industry. The increasing demands of cloud computing added the new characteristic which is

heterogeneity (Multi-tenancy) which implies use of same resources or applications by multiple consumer although they belong from same domain or from different domain [1].

Due to wide features cloud computing is going to be popular in industry. we can estimate its popularity with just few figures like just EC2 (cloud service provider) have more then half million blade servers [2]. As per IDC estimation for western Europe cloud computing marke will grow upto 15 billion US$ in 2015 which was just 3.3 billion US$ in 2010. If we observe just this figure it estimates 35% growth rate [2].

Verizon Business in their 'Verizon Business 2008 Data Breach Investigation Report' (Wade et al., 2008) reported 59% of the breaches involve hacking[3].

A Credit card processor Global Payments said in 2012 about a security breach which exposes data of one and half million customers information icluding credit card number insurance number etc. The estemated cost of financial lost is 84 million US$.

In 2012 Zapos reported its data breach which effects about 24 million customers [2].

An organization's security depends upon the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented by the organization [1]. These controls can be implemented in one or more layer by implementing from facilities(physical security), including network Infrastructure (Infrastructure security) to abstract resources (Virtualization security),Platforms(Platform Security) for Data(Data Security), all the way Information and application (Application Security).

As per information security breaches survey 2013 | technical report (Department for Business, Innovation and Skills) www.pwc.co.uk Ninety-three percent (93%) of large corporations reported at least one security breach in the last year [2].

An organization's security depends upon the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented by the organization [1]. These controls can be implemented in one or more layer by implementing from facilities(physical security), including network Infrastructure (Infrastructure security) to abstract resources (Virtualization security),Platforms(Platform Security) for Data(Data Security), all the way Information and application (Application Security).

As per information security breaches survey 2013 | technical report (Department for Business, Innovation and Skills) www.pwc.co.uk Ninety-three percent (93%) of large corporations reported at least one security breach in the last year.

The overall aim of this study is to identify cloud computing security threats and threats impact on all cloud computing aspects.

1.3 Problem Description

Cloud computing has gained more attention from academic as-well-as from industry.cloud security is high barrier to its adaptation.Rapid elasticity and resource pooling is basic cloud computing feature which is possible to resource sharing and mostly

in cloud computing cloud service provider have mainly focus to scale up their resources in secure way. service providers are using security practices but due to its complex model threat landscape is changed. It varies according to cloud service models, cloud deployment models etc. [2].

Threat landscape data is scattered in literature. There is lack of overall threat map with all cloud computing aspects.

1.4 Research Goal

The overall aim of this study is to identify cloud computing security threats and threats impact on all cloud computing aspects.

1.4.1 Objectives

The set objectives of the study which will direct towards achieving our aim are to:

1. Identify relevant information security attributes(Threats, Vulnerabilities, Attacks) for cloud computing.
2. Identify information security threats for cloud computing.
3. Identify threats for different cloud deployment model, cloud service model and cloud components..
4. Identify impact level of threats for cloud service model, cloud deployment model and components as well.

1.5 Research Methodology

We conducted a literature review (LR) to identify studies focusing on information security threats in the cloud computing. We identified the relevant threats with respect to Cloud Service model, Cloud deployment models and cloud computing components.

We are following the qualitative methodology for our research to formulate guidelines to address security issues in cloud computing on the basis of comprehensive analysis of existing work and identification of common security threats.

We have been used secondary source for the collection of data, i.e documents analysis, artifact analysis and the research study. We used Engineering Village,

Google Scholars and Scopus online citation databases as primary sources of data for literature review. Artifact analysis is useful for identifying the problem for the future research.Here we will be used research mixed-method, as the combination of both qualitative and quantitative research approaches.

1.6 Thesis Outline

The structure of the thesis is planned in the form of separate chapters. The chapters are organized as follows.

- Chapter 2 Describes the context, in which we brief about the basic knowledge of cloud and also introduce the terminology of cloud computing security because our thesis based upon that.
- In chapter 3 we conclude the related work to our thesis. We identified the works which have been done on cloud computing security. At the end we summarize all the efforts of researcher and the comparison of their work.
- In chapter 4 we defined selected threats and their reported financial impacts .
- In Chapter 5 we analyze our thesis and draw the results and also presents the recommendation for the new researcher; in the last we propose an idea on basis of our research study results.
- In the last chapter we conclude our work and describe the guideline for future research and improvement. ...

Chapter 2

Context

this section gives over view of the concepts using in this study.

2.1 Cloud Computing

Cloud computing is the deliverance of computing services in excess of the Internet. Cloud services permit individuals and enterprises to utilize software and hardware which are managed by third parties at remote location. Online file storage, social networking sites, webmail, and online business applications are examples of cloud services. Cloud computing is future of next generation, computing provides its customers with a virtualized network right of entry to applications and / or services. No issue from wherever the customers are accessing a service, they are automatically directed to the accessible and offered resources. The cloud computing model permits access to information as well as computer resources from everywhere that a network link i.e. internet is accessible. Cloud computing provides a shared group of resources, together with data storage space, PC processing power, networks, particular corporate and client applications. It has been defined by the U.S. National Institute of Standards and Technology (NIST) as following.

"Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

Cloud computing is emerging and recent trend towards distributed computing. It's a new business model to deliver computing. [4] Although it is fruitful for both consumer and provider. User needs computational resources at low price and provider get specific domain customers for their business. Industry's big players like Amazon, Google, Microsoft, Apple,....etc are developing large scale applications on cloud computing model. According to Gartner the financial investment on CC in 2016 will have a Global Compounded Annual Growth Rate of: IaaS: 41%, PaaS: 26.6% and SaaS: 17.4% in 2016.[5].

Cloud computing is one of the popular computing models for both local users and enterprises. Cloud computing popularity has improved as the time goes because most of the enterprises now use the services of cloud computing infrastructure. The cloud computing services are mainly differentiated into three main categories, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). A cloud system is a new resource provisioning infrastructure and various computing opportunities can be provided to its users. Users of the cloud can access many types of applications. The characteristics of cloud computing differentiate it from the accessing and management of resources. Cloud computing has a high scalability; it is economical and provides an efficient data backup facility etc.

Cloud computing services provide the easiest accessible means for the enterprises. Any enterprise can outsource large parts of their IT infrastructure and their maintenance. Cloud computing can actually be attractive for an enterprise due to reduction of the upfront charges for their computing infrastructure.

"Cloud Computing" term originated as a marketing effort to fix financial gaps associated with Internet Bubble at the beginning of this century.A five centuries old question "To Be or Not To Be?" in our information overloaded world can be rephrased as "To Share or Not To Share?". It has been inevitably resolved to an unequivocal "To Share" the information. In our case, it is Personal Information (PI) and the way that sharing is realized raises a lot of concerns and is still in discussion.

The first problem is the legal protection of PI, as current laws do not reflect continuously evolving situation. The second problem is the environment to share PI. Centralized sharing may work in some very limited cases, and even medical information cannot be organized in one "center" for such unions . Internet has been invented as an information sharing resource and has been used since for that purpose. However, it has not been designed to serve non-public information such as PI.

The third problem is the implementation of sharing services within Internet. What is currently available as so-called Cloud Computing Services (CCS) is not ready to handle PI neither from legal nor from technology standpoints.

A survey conducted by International Data Corporation (IDC) group between 2008 and 2009, proves that cloud computing is cost effective for users[6][7]. It's human nature to do better and much better. In the MIT Centennial talk in 1961, John McCarthy said that " The computer utility could become the basis of a new and important industry"[8]. In 1960s researchers introduced time-sharing utilities and later on it's for network computers in 1990s which resulted the term Grid computing[9][10][11].

Grid computing is defined as "a hardware and software infrastructure that provides dependable consistent, pervasive, and inexpensive access to high-end computational capabilities". [9] And Grid Computing is advance form of Distributed computing and Cloud Computing convergence form of Grid Computing. The "cloud computing" term as a whole probably first introduced by Eric Schmidt in his talk on Search Engine Strategies Conferences in 2006[8].

The first technology which was similar to cloud technology was “Cloud 1.0”. it was abstraction of TCP/IP layers and network devices communicate by complying the TCP/IP protocol and devices don’t have information about each other locations. The recent “Cloud 2.0” is abstraction of World Wide Web where the data and files can be stored and share without the user information. And the current model is “Cloud 3.0”which is abstraction of large scale infrastructure, complexity of data, servers, and heterogeneous platforms [9].

The big reason behind the popularity of cloud computing is its advantages which are reduced cost since services are provided on demand with pay-as-you-use model, high abstraction of resources, compute instance scalability and its flexibility, resource sharing, management through API’s and increasing mobility and heterogeneity.[4] according to a survey 91 % of the organizations in US and Europe agreed that reduction in cost is a major reason for them to migrate to Cloud environment.

Cloud computing is the delivery of computational services over the internet. Cloud computing is not a technological model it’s a business model to deliver computing. Essential characteristics of Cloud computing [12],[1].

And the biggest one is cost. As per Giles Hogben 2013 50,000 Machines for 1 Minute cost the same as 1 machine for 1 year.

- On-demand self-services
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured services ...

2.1.1 Cloud Computing Characteristics

2.1.1.1 On-demand Self-Service

The human interaction to the equipment of the cloud service's provider includes the management of network storage and computing power, can be done automatically. User can use the computing power on demand like a local machine by self-oriented.

Through the global network facility user can use the resources as he wish to use it, at any time and from any place of the world. The resources can be server time and also network space i.e. space on storage devices; all these resources can be accessed without any interference from the user side or from the service provider.

2.1.1.2 Broad Network Access

Broad network access permits services to be offered over the Internet / private networks. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Systems are available to the user through network. That can be accessed and used through different devices like personnel computers, smartphones, tablets and simple mobile phones. Systems performs like a personnel computer, customers can not differentiate the accessing delay while using.

2.1.1.3 Resource Pooling

Resources are virtualized and assigned dynamically and then according to the user demand it can be reassigned. Via a multi-tenant model resources are pooled by the provider's which can be serve to multiple user. The locations of the resources are hide from the user or customer who use the resources, so the location

is independence. The customer only knows about the abstraction level location like country, state or datacenter.

Resources are available from the provider to the multiple customers. This can be assigned and reassigned as per demand of the customer. In general, customer don't need to know about the physically location of the resource but he is interested about the availability and security of the resources.

2.1.1.4 Rapid Elasticity

Flexibility in the system done automatically and can be expanded or released very quickly and automatically like demanding for more CPU power or expanded a system to handle the supplementary users. On the behalf of user it would be done on a single click but on that you have to be paid for such quantity. Any private server can be stop working if there increase the load on it like any site hosted on a private server, by any reason the traffic boost to the dramatic value it may be go down or stop working. But in cloud resources are allocated dynamically in order to ensure the system operation smoothly, when such a condition occurs the resources are automatically assign to overcome the issue of load and after decreasing the traffic load resources are restored to its original condition.

2.1.1.5 Measured Service

According to the user needs and requirements of services types (i.e disk space, bandwidth, processor power and so on) cloud system automatically manage and control the resources. The services which are available for the user and provider are transparent on the behalf of their usage and measurable. Charges can be made by customers according to the services with the amounts they used. There is automatic metering check which calculates the resource usage of the customer and controlled with the transparency report for both the provider and customer.

2.1.2 Cloud Computing Service Models

Cloud computing service can be provided in 3 different manners, called cloud computing service models.1st one is SaaS (Software as a Service) second is called PaaS (Platform as a Service) and third one is IaaS(Infrastructure as a Service)

2.1.2.1 Software-as-a-Service (SaaS)

Software-as-a-Service is a service model which outsourcing the software or applications. All of the software's are available to the user or customer through pay as you go model. Most of the services of SaaS are available without any charge. Internet is mandatory to the user to access the application. SaaS can be defined as a methodology to deliver licensed software accessed through the services of web.

2.1.2.2 Platform-as-a-Service (PaaS)

Platform-as-a-Service is a service model which outsourcing the platform like windows, Unix etc. Platform as a service provide the services to deploy application with minimum cost and without any complication to manage and buy any kind of software and hardware. Customer or user can host their application on requested platform. In other word platform as a service provide the facilities which are required for building and deploying any web application services through internet. But it is to be ensure that application which you want to developed mush be compatible with the selected platform. PaaS is has a multi tenant environment with high scalability, one of the multi tier architecture.

2.1.2.3 Infrastructure-as-a-Service (IaaS)

t is a service model in which the infrastructure equipment owned by service provider and available for usage. Through this model the basic infrastructure can be outsource like storage, hardware, networking components and servers. As the service provider own all these equipment so the service provider is responsible for

maintaining and running it. The use or customer only pays as per use criteria. Infrastructure-as-a-service deliver the technology as per demand, all the service are scalable usually based on billing with the usage,

2.1.3 Cloud Computing Deployment Models

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location. Four deployment models are usually distinguished, namely public, private, community and hybrid cloud service usage.

2.1.3.1 Public Cloud

Public cloud express the cloud computing in terms of dynamically resources provisioned as per demand, it is a self service based on the internet, resources provisioned through web application and also owned by third party they charges on the basis of pay as you go model.

2.1.3.2 Private Cloud

For any corporation, a private cloud environment is the first choice to adopt it rather than adopting the plan for the public cloud. Primary datacenter deployed the virtualized hardware for the serving of local and remote users, any corporation use the virtualized hardware according to their requirements because consolidation of shared services is very beneficial for the corporations. Corporations have a full control on it and the security tracking privacy is very high.

2.1.3.3 Community Cloud

For any corporation, a private cloud environment is the first choice to adopt it rather than adopting the plan for the public cloud. Primary datacenter deployed

the virtualized hardware for the serving of local and remote users, any corporation use the virtualized hardware according to their requirements because consolidation of shared services is very beneficial for the corporations. Corporations have a full control on it and the security tracking privacy is very high.

2.1.3.4 Hybrid Cloud

Hybrid cloud is the combination of both public cloud and private cloud. Partially use of private cloud and partially use of public cloud make a full hybrid cloud. Any corporation can use a hybrid cloud according a proper plan, partitioned the data, secure data confidential experiment can be stored and done on private cloud and for the general purpose like backups, and conducting general development environments can be established on the public cloud.

2.2 Advantages and Disadvantages of Cloud Computing

2.2.1 Advantages of Cloud Computing

- Cloud computing is very cheap as compared to buy software and hardware from market.
- If the user have an internet connection then it can be used from anywhere in the world.
- Any device have a limited storage but storage system in cloud computing is unlimited.
- If user need to run cloud computing application available through web based, doesn't require high power or high priced computer.
- As the application run on the cloud, they do not utilize the power and disk space of the desktop PC of the user.

- The customer mostly used web based application, web based application doesn't depend upon the processor power, disk size.
- In cloud computing the scenario is different from the traditional installation of software there is no need a CD or DVD drive to install any kind of software programs. Software can be installed automatically through the web.
- The computers in cloud computing run faster because fewer programs loaded into the main memory.
- Cloud computing save the customer cost for purchasing expensive software because most of the software available for free in cloud computing.
- In cloud computing the application which is run through web based, can be updated automatically, latest version of the software available easily through web based.
- Cloud computing is compatible with the documents format, documents created on any machine is compatible with all other machine in cloud.
- Documents sharing is very quick and easy in cloud computing.
- Cloud computing offers massive storage and the limit of storage capacity are extendable. Expansion of Storage capacity is easiest as compared to traditional home based computer.
- Cloud computing provide the facility of data reliability i.e when hard disk crashed in desktop PC then all of your important data is lost, but in cloud computing you can save again your data from cloud archive.

2.2.2 Disadvantages of Cloud Computing

- Cloud computing big drawback is security issue, not trustful environment for classified data.
- Different privacy policies which is not acceptable to most of the customers.

- In cloud computing without internet connection you are not able to access your application and storage documents placed in cloud.
- Without internet connection you cannot access anything, means you become at zero level.
- In cloud computing you need an internet connection with best speed, otherwise with dead connection you still in problem with no work.
- In cloud computing most of the web based applications require much bandwidth to download and the same is done for any large documents.
- In cloud computing you may face the limitation of feature when you compared the web based applications with the full featured of desktop based applications.
- Some time in cloud computing even with a fast connection accessing of web based application is slower as compared with the software program on your desktop PC.
- In cloud computing unauthorized user can access to your data.
- In cloud computing each cloud systems uses different API's.
- The protocols are also different for each cloud systems in cloud.

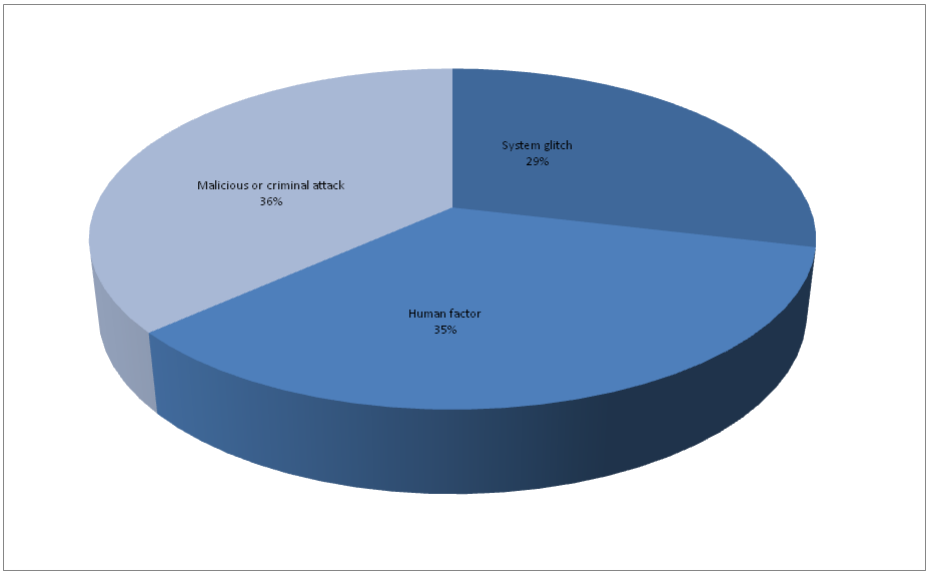
2.3 Cloud computing Security

Security is the safeguarding of assets from unwanted, illegitimate, unauthorized access. In simple words Security is the quality or state of being secure – to be free from danger.

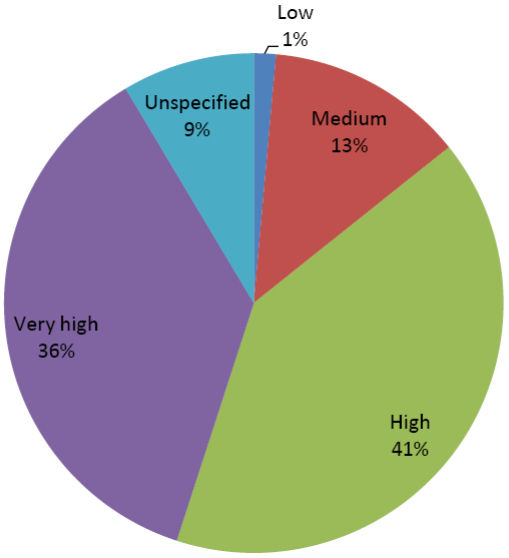
As we are aware about wide adoption of cloud computing. Clod computing provide resources via internet . Cyber attacks are increasing day by day. Technological use is increasing in both positive and negative direction . Bad user have

focus to access data [4]. The major focus during attack is access of data. In 2013 a survey conducted by ponemon Institute the major causes of data breaches are.[15]

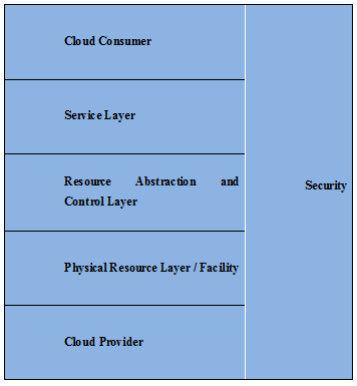
- Malicious or criminal attack.
- Human Factor.
- System Glitches.....



A survey conducted by ENISA 2011 the cloud security is high barrier to its adaptation so Security is crucial for all cloud computing services the main reason is that one flaw can impact a wide range of organizations directly due to wide range of usage of cloud computing services. In simple words we can define it as that Cloud computing have single point of failure [2].



choi et al. [13]in paper title "Advanced Security Framework Model for Cloud Computing Environment" explicitly refers a survey of IDC that 74% of IT executives and and CEO,s are reelected to adopt Cloud Computing model due to security issues.



The increasing demands of cloud computing added the new characteristic which is heterogeneity (Multi-tenancy) which implies use of same resources or applications by multiple consumer although they belong from same domain or from different domain [1].

Due to wide features cloud computing is going to be popular in industry. we can estimate its popularity with just few figures like just EC2 (cloud service provider) have more then half million blade servers [2]. As per IDC estimation for western Europe cloud computing marke will grow upto 15 billion US$ in 2015

which was just 3.3 billion US$ in 2010. If we observe just this figure it estimates 35% growth rate [2].

Verizon Business in their 'Verizon Business 2008 Data Breach Investigation Report' (Wade et al., 2008) reported 59% of the breaches involve hacking[3].

A Credit card processor Global Payments said in 2012 about a security breach which exposes data of one and half million customers information icluding credit card number insurance number etc. The estemated cost of financial lost is 84 million US$.

In 2012 Zapos reported its data breach which effects about 24 million customers [2].

An organization's security depends upon the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented by the organization [1]. These controls can be implemented in one or more layer by implementing from facilities(physical security), including network Infrastructure (Infrastructure security) to abstract resources (Virtualization security),Platforms(Platform Security) for Data(Data Security), all the way Information and application (Application Security).

As per information security breaches survey 2013 | technical report (Department for Business, Innovation and Skills) www.pwc.co.uk Ninety-three percent (93%) of large corporations reported at least one security breach in the last year.

Chapter 3

Related Work

3.1 Literature Review

In 2009 Ling Qian et al. [8] describes the history of Cloud Computing and refers this term towards Eric Schmidt which introduced the term of Cloud Computing in his talk on search engine strategies. Ling Qian et al. describes its characteristics, advantages and its architecture with the explanation of some associated risks like Privacy and Security, The continuity of service, service migration etc.

Yildiz et al. [14] offers a horizontally and vertically configurable and policy based security approach and focuses on the infrastructure scope. This approach covers within the domains of physical networks, servers, storage mediums and systems management. All these domains can be protected by using both horizontal and vertical policies but in this paper Application security is not handled. There is no security mechanism for application in this technique which is a big disadvantage of this technique because application security has an important role in cloud security.

In 2009 reddy et al.[15] Title: "Cloud Security Issues" describes the importance of SLAs (Service level agreement) because SLA is only way as per author to get the trust of client, the necessary contents of SLA are Definition of

Service, Performance management, Problem management, Customers duties and responsibilities, Warranties and remedies, Security, Disaster recovery and business continuity and Termination. All SLAs must guarantees SLA credit claim, SLA Claim fault, Public network, private network, Hardware update and Redundant infrastructure.

Almorsy et al. [16] work title "An analysis of the cloud computing security problem" highlights the security issues in different service delivery models like SaaS,IaaS,PaaS. For IaaS (infrastructure as a Service) have issues like VM security, Virtual network security, Hypervisor security, Virtual machine boundaries etc. For PaaS (Platform as a Service), he mentioned the issues related to DOS attacks, man in the middle attack, Dictionary attack, Injection attacks and input validation related attacks and focuses the importance of API security. SaaS (Software as a Service) inherits all security issues from IaaS and PaaS because it built on top of them.

Takabi et al. [17] in paper Title "Security and Privacy Challenges in Cloud Computing Environments." Describes the security and privacy as biggest challenge for cloud computing and highlight some security issues like authentication and identity management, access control and accounting, trust management and policy integration, secure service management, privacy and data protection and organizational security management. Author suggests some approaches like access control, secure interoperation, secure service provisioning and composition, data centric security and privacy.

Sahoo et al. [11] in 2010 describes the types of virtualization as full virtualization, OS-layer virtualization, para virtualization, Application virtualization, Resource virtualization and storage virtualization. After discussing the advantages and disadvantages of virtualization, author highlights the security issues related to virtualization because cloud computing depends on virtualization. The security vulnerabilities related to virtualization are communication between VMs, communication between VM and host, VM Escape, VM monitoring from the

host, VM monitoring from other VM, Denial of Service, Guest-to-Guest attack, External modification of VM etc.

In 2010 Julisch et al. [18] Title: "Security and control in the cloud" highlights the security concerns of CIOs and CSOs from cloud computing. ISO 27001 controls implementation in cloud environment and focuses that cloud security is not just responsibility of cloud provider its responsibility of both parties. Providers have to offer regular audit of data location etc. A key message for cloud client in this paper is that they have to be realistic about what they are purchasing from cloud services. what they do not purchase is risk transfer . Cloud client also have need to follow risk management process.

Ramgovind et al. [6] Title:" The management of security in cloud computing" declares security as biggest challenge to implementing cloud computing security model. Cloud stakeholders have to ensure security as much as possible and authors have suggested information security controls for cloud deployment models i.e Public cloud, Private Cloud, Hybrid cloud and Service models i.e IaaS, PaaS and SaaS. Information security controls are Availability, Non-rapudiation, Integrity, Confidentiality, Authorization, Identification and Authorization.

Wu et al. [7] describes One of biggest challenges of security virtual machine instance interconnectivity to implement Cloud computing platform. Author highlights the security issues in VM security are The break of isolation, Remote management vulnerabilities, Denial of service (DOS) vulnerabilities, Virtual machine based Root kits, Revert to snapshots problem and network virtualization security problem as bridging, route and propose a novel virtual network model which have separate routing layer, firewall layer and shared network layer.

In 2011 Velev et al. [4]emphasis the advantages of cloud computing over traditional business model and point out risks and security concerns with cloud computing like Abuse and Unallowed use of cloud computing, Insecure application programming interface, Malicious insiders, Shared technologies vulnerabilities, Data loss and leakages, Account hijacking, Service hijacking, Internet

traffic hijacking and Unknown risk profile, and describes the importance of Infrastructure security and divides Infrastructure into three sub categories with respect to security implementation i.e The network level infrastructure, The host level infrastructure and The application level infrastructure.

Subashin et al. [3] performed a security survey with respect to cloud service delivery models and point out the security components for PaaS, SaaS, IaaS, main focus was PaaS and highlighted some key security elements like Data security, Network security, Data locality, Data integrity, Data segregation, Data access, Authentication and authorization, Data confidentiality, Web allocation security, Data breaches, Virtualization vulnerabilities, Availability, Backup and Identity management etc. Authors also highlighted the weaknesses related to each element and possible attacks like Data security can be breached through Cross-site scripting, Access control weaknesses, OS and SQL injection flaws, Cross-site request forgery, cookies manipulation, Hidden field manipulation, insecure storage and insecure confirmations.

Bhadauria et al. in 2011 published a survey with title" A survey on security issues in cloud computing" [19] and the focus of author was to point out the barriers to adoption of cloud computing and found the security and privacy is the biggest barrier towards adoption of cloud computing model and other barriers like Performance , Latency and reliability, Portability and interoperability, Data storage over IP network and Data breach through optical fiber etc have low priority then security. Authors highlights the possible security breaches at different security level like basic level security, Application level security, Network level security, and possible breaches like for network level security can be breached by DNS attacks, Sniffer attacks, By reused IP addresses, Denial of service and distributed denial of service attacks etc, where application level security can be breached through denial of service attacks, cookie poisoning, hidden field manipulation, Backdoor and debug options, distributed denial of service attacks, Captcha breaking, Google hacking etc and provides some sort of guidelines to overcome these issues.

Akhil behl in 2011 [20] pointed some threats which breaks the customer trust over cloud provider like Insider threats, Outside malicious attacks, Data loss, Service disruption, Multitenancy issues and loss of control, and suggests some key characteristics during implementation of cloud computing security like Availability and performance, Malicious insiders, Outside attacks, Loss of control and Multitenancy to overcome the level of threats. Chaves et al. [21] highlighted the customer security concers in cloud computing like Cloud provider are implementing standard security practices , How much cloud is vulnerable for attack , Privileged user access, regulatory and compliance, Data location, data segregation, Recovery, Investigative support, Long-term viability etc.

Jamil et al. [22] title "Security issues in cloud computing and countermeasures" point out some cloud computing security issues and explore the issues in depth to provide the counter solution. Although authors discussed just few issues like XML signature element wrapping, etc but define complete attack vector.

Sabahi in his paper [?] "Virtualization-level security in cloud computing" describes the three approaches of virtualization i.e. Operating system based virtualization, Application based virtualization and hypervisor based virtualization, and highlights the virtualization level threats and attacks like VM level attacks, Cloud provider vulnerabilities, Expended network attack surface, Authentication and authorization, Lock-in, Data control in cloud and communication in virtualization level.

David [23] describes the cloud security issues and threats separately . according to David the security issues for cloud computing are like Privileged user access, regulatory compliance, data location, data segregation, investigation support and long term viability else ware the security threats are like threats to information privacy and confidentiality, threats of shared technology and threats to data loss and leakages, and provides some mitigation technique to overcome the impact of threats.

In 2011 Cloud Security Alliance (CSA) [1] presents "Security guidance for critical areas of focus in cloud computing v3. 0" in this guide CSA categories

Cloud security into two parts architectural and non-architectural, and non architectural categories in further two sub categories governance and operational and discussed both with respect to following domain Governance and risk management, Legal issues: contracts and legal discovery, compliance and audit management, information management and data security, interoperability and portability, traditional security, business continuity and disaster recovery, data center operation, incident response, Application security, encryption and key management, Identity, entitlement and access management, virtualization and Security as a Service.

As per Marnix et al. [24] "Survey and analysis of security parameters in cloud SLAs across the European public sector" which is an report of ENISA (European Network and Information Security Agency) the SLA have very important role in Cloud computing security. As per ENISA customer should define security requirements in form of parameters, monitoring methodology. In this survey 36 percent people declare security is very high risk 41 percent declares it as high and 13 percent declare security as medium risk.

NIST(National Institute of Science and Technology) releases "NIST cloud computing reference architecture , Special Publication 500-292" [25] in 2011. In this reference architecture NIST introduces new cloud characteristics like Cloud consumer, Cloud Provider, Cloud broker, Cloud carrier and Cloud auditor and describes security implementation as per its responsibility and describes cloud conceptual model with respect to all these parties.

Mell et al. [12] "The NIST definition of cloud computing, Special Publication 800-145" 1st time defines properly Cloud computing its proper definition, its deployment models and its service models. This definition is now commonly used in literature. NIST also defines the important characteristics of cloud computing like On-demand Self-services, Broad network access, resource pooling, rapid elasticity, Measured services.

Modi et al. [26] in 2012 did a detail survey and find vulnerabilities, threats, and attacks on cloud computing separately like vulnerabilities are vulnerabilities in cloud environment, vulnerabilities in internet protocol, unauthorized

access to management interface, injection vulnerabilities, vulnerabilities in browser and APIs , and Threats as change to business model, Abusive use of cloud computing, Insecure interface and API, malicious insiders, shared technologies/multi-tenancy nature, data loss and leakages, service hijacking, risk profiling, identity theft, and possible attacks as zombie attacks, service injection attacks, Attacks on virtualization, Man-in-the middle attack, Metadata spoofing attack, phishing attack and back door channel attack. Modi et al. also highlights the security issues at different layers of cloud computing like Application level security issues, Service availability, Integrity of workload state, Data storage level security issues, virtualization level security issues, authentication and access control level security issues, trust level security issues and security issues related to auditing, regulatory compliance and Law.

Chen et al. [?] in paper title "Data security and privacy protection issues in cloud computing" describes a data life Cycle. as per Chen data security and privacy protection is necessary at every level like Data generation level, Data transfer level, Data use level, Data share level, Data storage level, Data archival level and Data destruction level. All these levels have its own importance because data can be breached from any level so security must be implemented at all levels.

Zissis et al. [9] have focus on trust because trust is the major element between Cloud provider and Cloud consumer and believes that Cloud computing have challenges of confidentiality and privacy, integrity and availability. Due to third party trust is mandatory and trust on third parties relies upon for low and high level confidentiality, server and client authentication, creation of security domains, cryptographic separation of data, certificate-based authentication.

Parekh et al. [27] in 2013 highlights some security issues with respect to cloud service models i.e. Private, Public, Hybrid, and service models i.e. SaaS, PaaS, IaaS, and Network issues. Security issues for service model are Data leakage problem, Malicious attacks, Backup and storage, Shared Technology issues, Service Hijacking and virtual machine hooping, and issues for deployment models are Cloning and resource pooling, Motility of Data and Data residuals, Elastic

Perimeter, Shared Multi-tenant environment, Unencrypted Data, Authentication and Identity management, and Network issues are Browser security, SQL injection attacks, Flooding attacks, XML signature Element Wrapping, Incomplete Data deletion, Locks-in etc, Authors mapped Confidentiality, Integrity, Availability with respect to Service delivery model like Software as a Service, Database as a Service, Infrastructure as a Service and Platform as a service at different virtualization vulnerabilities like VM hooping, VM mobility, VM Denial of service attack.

Da silva et al. [5] Title: "Systematic Mapping Study on Security Threats in Cloud Computing" take 7 most common security threats i.e. Abuse and Nefarious use of cloud computing, Insecure Interface and API, Malicious Insider, Shared Technology Issues, Data Loss or Leakage, Account or Service Hijacking, unknown Risk Profile, and 15 security domains like Access Control, Accountability, Anonymity, Applied Cryptography, Authentication, Data or Database Protection, Digital Forensics, Identity management, Integrity, Intrusion Detection, Formal Security models, Network security, Privacy, Risk analysis and Management, Trust Model and management, and mapped the number of publication as per threat and domain further more authors categories publications as per year, as per publisher and tries to find the total number of publication in this field.

CSA (Cloud Security Alliance) [28] with title "The Notorious nine: cloud computing top threats in 2013" presents top 9 security threats and their controls with respect to service model of cloud computing i.e. Data Breaches, Data Loss, Account Hijacking, Insecure API, Denial of Service, Malicious Insider, Abuse of Cloud Services, Insufficient Due Diligence, Shared technology issues, and its risk matrix on the basis of experts expertise.

Ko et al. [29] in 2013 identifies some new threats with the help of CSA survey titled "Cloud computing vulnerability incidents: A statistical overview" i.e. Hardware failure, Natural disaster, Closure of Cloud Services, Cloud Related Malwares and Inadequate Infrastructure Design and Planning, and explains with the help of examples of reported incident.

ENISA [30] published a report of survey regarding top 16 threats of 2013 . the report title is "ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats." The highlighted threats are Drive-by Download, Malicious code: Worms/Trojans, Code injections, Botnets, Physical Damage/Theft/Loss of Media, Identity Theft/Fraud, Denial of Service, Phishing, Spam, Reguware/Ransomware/Scareware, Data Breaches(Compromising Confidential Information), Information Leakage, Targeted attacks, Watering hole attacks, and categorize all threats with respect to its trends for Critical Infrastructure, Mobile Computing, Social Networks, Cloud computing, Trust Infrastructure, Big Data and Interconnected devices.

In start of 2014 OWASP (Oper Web Application Security Project) [31] Releases its top 10 web application threats with impacts and mitigation techniques. OWASP also have compared its 2013 threats survey with its previous threats survey, conducting in 2010. as per OWASP the top 10 threats for web applications are, Injections (SQL, OS, etc), Broken Authentication and session management(Compromise passwords, sessions, etc), Cross Site Scripting(Session hijacking, defacing web sites, etc), Insecure Direct Object References, Security misconfigurations(configurations of different Servers, Platforms, etc), Sensitive data exposure, missing function level access control, Cross-Site request Forgery,Vulnerable components, Unvalidated Redirects and forwords. Cloud Computing based on web so thats why we have to include all this threats as Cloud Computing Threats.

Chapter 4

Security Threats in Cloud Computing

4.1 Vulnerability, Threat, Attack

Vulnerability is defined as “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” [32].

"weakness in a system, application, or network that is subject to exploitation or misuse” [32].

"Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source” [32].

“A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy"[33].

In simple words we can explain that vulnerability is a weakness of the system which can be exploited to gain system unauthorized access or misuse. As per RFC 4949 the definition of threat is "A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm" [33].

As per NIST "Glossary of Key Information Security Terms “Threat is defined as " Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." or " The potential source of an adverse event." "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability" [32].

As we discussed that vulnerability is a weakness of the system which can be exploited to gain system unauthorized access or misuse. If vulnerability has potential of danger then it can be threat for system. Some time systems have such type of vulnerabilities which don't have potential of danger for system in that case that vulnerability is not potential threat for that system. “An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity”[32].

“Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself” [32].

“An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat” [33].

Vulnerability is a weakness of the system which can be exploited to gain system unauthorized access or misuse. If vulnerability has potential of danger then it can be threat for system and the methods used to exploit that vulnerability is called attack. Some time systems have such type of vulnerabilities which don't have potential of danger for system in that case that vulnerability is not potential

threat for that system. All these terms are related to each other and have very close relation with each other.

4.2 Identification of Cloud Security Threats

In this section we identify the threats and their potential reported losses.

4.2.1 Data Breach:

As Wikipedia "A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." it can be any personal information like credit card no, national insurance no, personal information, Bank account information, account passwords etc. Incidentally breached or stolen both will be treated as breached.

As per Verizon research report, reported data breaches costs 12 billion US $ in 2013. [34] as per OTA (Online Trust Alliance) in 2013 110 million Credit card or Debit Card Accounts has been breached.[35] as per Pokémon Institute report published in 2013 the cost of data breach for Germany and US in 2012 is 4.8 Million US$ and 5.4 million US$, it is cost of reported breaches. The average cost per record of data breach for Germany and US is 214$ and 277$ respectively[36]. As per CNN news Home Department confirmed that the data of approximate 56 million people has been exposed in a cyber attack [37] .

In February 2015, Anthem endured an information rupture of about 80 million records, including individual data, for example, names, government managed savings numbers, dates of conception, and other touchy subtle elements. [38]

4.2.2 Data Loss:

Data loss is an error condition, by which consumer losses its data. It can be error in system, system failure, negligence, backup failure, disaster etc. it's different from data breach. In data breach data goes to wrong hands but in data loss customer do not have access to its data.

As per KPMG report in last 5 years 1 billion people have faced Data Loss, in Data Loss the last 2 years was very critical because the reported cases have been increased 40 % the previous year's this thing make it very critical, Technology sector is most effected sector of Data loss due to its highest %age of reported cases which is 26% of total reported cases all other sectors are also infected by this threat.[39]

4.2.3 Account or Service Traffic Hijacking:

Hijacking refers to is primarily described as unauthorized change. However as per With respect to cloud data travels from source to destination via internet. During this transmission it passes through many channels and can be hijacked at any channel The type of hijackings includes like Browser hijacking, DNS hijacking, IP hijacking, page hijacking, session hijacking etc.

As per OTA (Online Trust alliance) just in 2013, 110 million people have lost the credentials of Credit Cards, Debit Cards, Social Security numbers etc. which is a big loss of customers and place a big role towards customer's lack of trust. Among 110 million [35] KPMG also reported that 1 billion people lost Data in last five years, among 1 billion 668 million lost due to the hacking which is 60 % of total data loss which shows its criticality of this threat.[39]

4.2.4 Denial of Service (DOS) ,Distributed Denial of Service (DDOS):

In cloud computing model Services are accessible via internet . Services can be infrastructure (Computational power) Software (any type of application) and Platform for both legitimate and malicious user. Service provider do-not have any distinguish between good and bad user. So hackers also can gain more computational power on very low expense. In 2013 a spamhaus project faced an attack of 300 GB/s. this attack was wake up call for security professionals [40]. As per survey of Ponemon Institute Denial of Service (DOS) is one of most critical threat for online business, and are 17 % of total attacks. The average Cost of Business loss per attack is 187,506 $ [41] [42].

4.2.5 Botnets:

In cloud computing model Services are accessible via internet . Services can be infrastructure (Computational power) Software (any type of application) and Platform for both legitimate and malicious user. Service provider do-not have any distinguish between good and bad user. So hackers also can gain more computational power on very low expense. In Cloud Computing resources are shared and inter connected via internet, so any malicious user can gain access and control remotely and perform malicious activity like DoS,DDos attack, Spyware, Adware etc.

Botnet based network attacks are difficult to detect and their numbers are increasing. In addition in network attacks, the fraction of botnet based network attacks are more than any other attacks[40]. Huawei Cloud Security Center forecast predict in the coming years there will be an increase in mobile botnets, larger point-to-point botnets, and more widespread use of evasion techniques like Fast-Flux etc. as per ENISA the annual economic loss due to malicious software is 10 billion US$. The famous examples of Botnet based attacks are, against Estonia in 2007, against Georgia in 2008 and against Iran in 2009 [43].

4.2.6 Insecure API,s and Interfaces:

Cloud computing service providers use APIs to permit clients to connect with the administrations. These interfaces are utilized to perform capacities, for example, provisioning, administration, verification, observing, access control, and others, and they must be outlined with insurance from both unintentional and malevolent bargain. Furthermore, outsiders frequently fabricate quality included administrations upon APIs, which they then offer to their clients. This makes a layered API with expanded unpredictability and can build hazard.

Examples: Clear text authentication or transmission of data, anonymous access, reusable passwords, improper authorizations, and API dependencies are some examples of this threat.

4.2.7 Malicious insider:

Malicious insider to an entity or organization have legal access to organizations data or resources but using for individual benefits or compromising organizations security parameters like integrity, availability or confidentiality .This person may be a regular employee; X-employee, contractor, Sub contractor. It can be by physical presence or by some spy software.A report distributed in July 2012 on the insider risk in the U.S. money related area gives a few measurements on insider danger episodes 80% of the malignant demonstrations were conferred at work during working hours, 81% of the culprits arranged their activities in advance; 33% of the culprits were depicted right now 17% at this very moment. The insider was distinguished in 74% of cases. Monetary benefit was a thought process in 81% of cases, retribution in 23% of cases, and 27% of the individuals doing noxious acts were in money related challenges at the time[44].

4.2.8 Abuse of Cloud Computing:

As rapid elasticity and scalability are key attributes of cloud computing. These services are also available for legitimate users as well as negative users. User can utilize these resources for nefarious purposes like DOS attacks, Brute force attacks etc. Symantec, long a voice for security in cloud computing platforms for business, has issued another cautioning to organizations. In developing so dependent on distributed computing, it appears the security titan is concerned that it is turning out to be dreadfully simple to utilize unapproved cloud benefits inside an association without taking the best possible safety measures [45].

Gravity of circumstance revels when in a security monster Symantec directed a review among IT and IS (Information Security) laborers, found that numerous representatives are setting up what it terms "maverick mists". These "maverick mists" are unapproved employments of cloud stages and administrations to do organization business. Frequently, these errands are so little they aren't even seen by administration or the IT and IS offices. Notwithstanding when they will be, they are regularly not appropriately assessed at this very moment risk, because of the developing simplicity and acknowledgment of cloud administrations in regular life [45].

4.2.9 Insufficient Due Diligence:

Many organizations are adopting Cloud computing for the reason that it has cost reductions, operational efficiencies and improved security. Due to this reason number of organizations adopted the cloud are on large scale however many organizations implement the cloud without understanding the complete range of the responsibility with respect to their environmet[32].

4.2.10 Code Injection:

There are some bugs in application caused by invalid data processing. Malicious person can exploit such bugs. The technique by which unauthorized person exploit such sort of bugs are known as Code injection like SQL inject injection, Script injection, Shell injection etc.

4.2.11 Targeted Attacks:

Business is somewhat like war, with the exception of that there are legitimate limitations that oversee what should be possible and what isn't possible. Rivals in the same business intend to vanquish comparative regions through distinctive ways and means. Examination is a significant resource and a few associations may fall back on treachery and store modern secret activities to get up to speed with a focused firm. Ordinarily, taking research just expenses a small amount of the a great many $ that were put into innovative work for a given item or administration. A focused on assault is considerably more viable and harming for the casualty since the activities performed by the malignant programmer are customized. This implies that it is significantly more hard to stop a focused on assault than a crafty one essentially on the grounds that the assaults themselves are not broad.

4.2.12 Physical Theft/Loss/Damage:

Protected areas should have a range of Physical Infrastructure and facilities. A physical security boundary should be in place to avoid unofficial right of entry, allied t o physical entry controls to ensure that only authorized personnel have access to areas containing sensitive infrastructure .Suitable physical security should be in place for all places of work, rooms and amenities which surround physical infrastructure pertinent to the provision of cloud services.

Equipment security controls. Should be set up to forestall misfortune, robbery, harm or trade off of advantages. Legitimate hardware support. Should be preformed to guarantee that administrations are not upset through predictable hardware disappointments. Control of evacuation of benefits. Needed to keep away from robbery of significant and delicate resources. Secure transfer or reuse of hardware. Especially any gadgets which may contain information, for example, stockpiling media. HR security. Suitable controls should be set up for the staff working at the offices of a cloud supplier, including any interim or contract staff[46].

4.2.13 Compliance Risks:

There are dangers which accompany global capacity and these ought to be evaluated and alleviated through SLAs and contracts. There are likewise regulations that require the divulgence of private information to government organizations. Regulations which oblige protection in one nation are regularly conflicting to regulations which oblige revelation in another. Geographic contemplations for the most part influence information stockpiling, however might likewise influence information preparing[47].

Cloud service providers make data backups at different geographical site to avoid natural disasters and deploy data centers at low cast areas to maintain low price for consumers. So different rules and regulations apply on data according to Law of land. Company sales its assets including customers data etc.

Right now have diverse laws for instance, in the United States of America the Federal Rules of Civil Procedure takes into consideration disclosure demand which would break both European and Canadian law. In the United States the Federal Rules of Civil Procedure has been received in just 35 states, whilst in Europe you may need to consider government, national, and European law[47], [48].

Auditing, compliance and data privacy issues are considered to be the top cloud security challenges facing organizations, according to a global survey

from Cipher Cloud. The results of a survey of Global 2000 organizations from North America, Europe, APAC and Latin America shows that 64% identify audit/compliance/privacy as the top challenge [49].

4.2.14 Hardware Failure:

Data centers are equipped with hundreds or Thousands of Hard Disks, Network routers, Hardwired connectors etc. All equipment communicate with each other to perform tasks and make high availability to deliver high compute power or services in cloud computing . In private clouds all these networks are designed to run services locally .It is obvious that designing of servers are not done keeping in view of local networks thus servers and other hardware is at risk. The servers consist of multiple hard disks, memory modules, network cards; processors etc., each of which while carefully engineered are capable of failing. Obviously Hardware failure can effect performance which effects providers reputation and business.[50].

4.2.15 Natural Disasters:

Data centers can be damaged by expected/unexpected natural disasters.. Government is taking keen interest in familiarizing cloud computing while many agencies are reluctant to do so This is dangerous – as any user who has spilled a drink on a computer knows, flooding can easily ruin data which has not been properly backed up.

IT experts are doing much to expand their endeavors in calamity readiness, yet the work needs to rise considerably all the more rapidly. Information is developing at exponential rates, and a few laborers are experiencing difficulty keeping up. Of those surveyed, 46 % accepted that the organization's present fiasco recuperation arrangement would be tasteful for the following year. Furthermore, of those, a quarter suspected that the present operation would get them as the year progressed, yet no more than those 12 months.

Despite the fact that calamities could strike abruptly, a large portion of these offices are not trying the crisis arrangements almost enough. Over the previous years, those surveyed have found the middle value of 2.5 tests altogether. Yet when asked what might be an ideal number of yearly tests, these same government representatives addressed more than twice that at 5.3 tests for every year. Financial plan, absence of backing from higher-ups and essentially missing arrangements were referred to presently the deficiency.As the consequences of the study are examined, governments will make certain to build the wellbeing of the cloud. The cloud has itself expanded information wellbeing and may soon be a considerably more thorough arrangement [51].

Offsite and inside threats may affect the overall buildings and infrastructure during emergencies. While selecting a cloud providers reliability and consistency factors must be under consideration[52].

4.2.16 Cloud-related Malware:

Malware distributors are receiving distributed computing, either by purchasing administrations specifically or by bargaining real records, right now and practical approach to bring their malware web, as indicated by another report. Significant facilitating suppliers, for example, Amazon and GoDaddy (which have 16 percent and a 14 percent of malware, individually) can likewise help malware abstain from blacklisting by holing up behind these providers' reputations [53].

This action brings about the accompanying dangers being distinguished by Cisco for 2014 [54].

- 4.5 billion emails are blocked every day
- 80 million web requests are blocked every day
- 6450 endpoint file detections occur every day in FireAMP
- 3186 endpoint network detections occur every day in FireAMP

- 50,000 network intrusions are detected every day

[55].

4.2.17 Lock-In:

cloud computing may be deleting the additions we've made as far as seller reliance lock-in. Running with a cloud arrangement means becoming tied up with the particular conventions, guidelines and apparatuses of the cloud merchant, making future movement exorbitant and troublesome. How is this so? Since norms are as yet being framed, and distributed computing is still excessively juvenile, making it impossible to achieve the point where clients are requesting seller freedom. The issue is, when organizations take a seat to figure the expense of utilizing distributed computing administrations, they don't calculate the expenses of moving off the framework – costs which could be restrictive and unexpected[56].

Lock-in can be an issue right now imposing business models for suppliers with specific clients and as being what is indicated limits the weight to advance, Global cloud suppliers frequently give private application programming interfaces to empower organizations to utilize their worth included administrations.

At the point when beginning to utilize these APIs inside of your code, the seller really restricts its capacity to move to another cloud supplier since they may not utilize the same administrations or API, Keidar clarified. "This, basically, is the fundamental driver for cloud lock-in[57].

vendor lock-in is seen as one of the potential drawbacks of cloud computing. One of Gartner's research analysts recently published a scenario where lock-in and standards even surpass security as the biggest objection to cloud computing [58].

4.2.18 Unknown Risk Profile:

Cloud computing offers significant potential for reduced cost, rearranged IT foundations, and enhanced IT proficiency. Programming adaptations, overhauls, security hones, powerlessness profiles, interruption endeavors, and security outline are all elements for assessing your organization's security stance. In some of these ranges, distributed computing arrangements may offer diverse levels of perceivability contrasted with their on-reason partners. This can add to making it harder to "figure" a danger profile. As a general rule, all bases have some obscure dangers.

Chapter 5

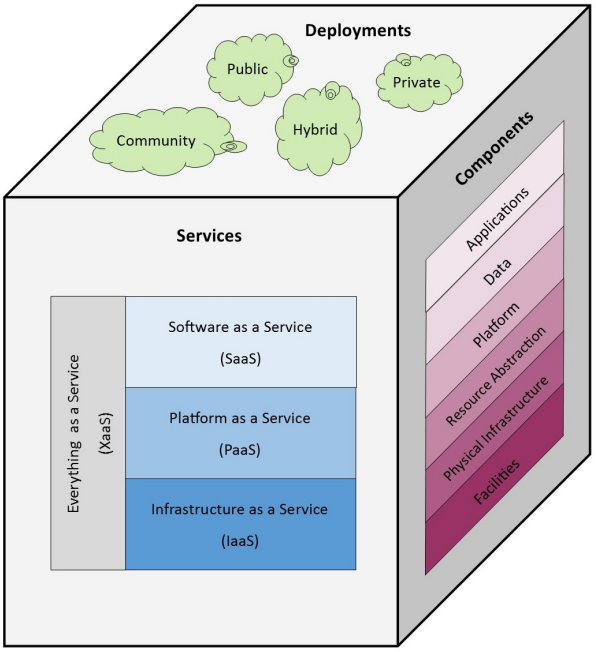
Analysis of Cloud Security Threats

5.1 Identification of Cloud Security Threats

TABLE 5.1: Threats discussed in literature

Threats,Vulnerabilities, Attacks	**References**
Data Breaches	[9],[3], [4], [26], [28], [9],[10], [59], [60] , [1], [5]
Data Loss	[9], [3],[1],[21], [4],[20],[28], [26], [21],[5], [61],[59],[60], [20],[61]
Account or Service Traffic Hijacking	[9],[3], [4],[26],[5], [20],[28], [20],[61],[60], [31]
Insecure Interfaces and API	[9],[3], [4],[26],[5], [20],[61],[28],[10],
Denial of Service	[9],[10],[22], [26],[20],[28], [62], [60], [31], [3], [62], [18]
Malicious Insiders	[4],[26],[10],[20], [61],[28],[9], [5],[61],[59],[60], [3]
Abuse of Cloud Services	[4],[5], [61], [26],[28], [60]
Insufficient Due Diligence	[61],[28],[60]
Shared Technology Vulnerabilities/Issues	[3],[4], [17],[28], [26],[5],[20],[61], [20],[60], [9]
Drive-by exploits	[30]
Worms/Trojans	[30],[31]
Code Injection	[3],[22],[26], [22], [31]
Exploit Kits	[30]
Botnets	[30], [28]
Phishing	[30]
Compromising Confidential Information	[9],[3],[1]
Rogueware/ Scareware	[30]
Targeted Attacks	[28], [9]
Physical Theft/Loss/Damage	[9], [3]
Identity Theft	[9]
Abuse of Information Leakage	[30]
Search Engine Poisoning	[31]
Rogue Certificates	[31]
Hardware Failure	[3],[61], [9]
Natural Disasters	[3], [61], [9]
Closure of Cloud Service	[61]
Cloud-related Malware	[61]

Injection	[9],[22]
Broken Authentication and Session Management	[9],[3], [22]
Cross-Site Scripting (XSS)	[3], [9]
Insecure Direct Object References	[3], [31]
Security Reconfiguration	[9]
Sensitive Data Exposure	[9], [31], [3]
Missing Function Level Access Control	[3], [31]
Cross-Site Request Forgery (CSRF)	[3], [31]
Using Known Vulnerable Components	[9], [31]
Unvalidated Redirects and Forwards	[3], [31]
Access control verification	[3]
cookies manipulation	[3]
hidden field manipulation	[3]
Inter VM Attacks	[10],[62], [26]
XML signature element wrapping attack	[22]
Unknown Risk Profile	[5],[61],[28]
Loss Of Governance	[59]
Lock-IN	[59]
Isolation Failure	[59]
Compliance Risks	[59]
Management Interface & Compromise	[59]
Data Protection	[59]



Model Picture2.jpg Model Picture2.jpg

FIGURE 5.1: Proposed Model

5.2 Proposed Model

we will analyze the selected cloud computing security issues for all cloud service models. i.e. PaaS (platform as a service), IaaS (infrastructure as a service) , SaaS (software as a service) and for all cloud deployment models and cloud components.

5.3 Threat analysis at Cloud Component level

TABLE 5.2: Threats at Component level (clearly discussed in literature)

Components						
Threat	Application	Data	Platform	Resource Abstrection	Physical Infrastrectur	Facility
Data Breaches	[9],[3]	[9],[3],[1],[4],[5]	-	-	-	-
Data Loss	[9],[3]	[9],[3],[1],[21], [5],[20],[61]				
Account or Service Traffic Hijacking	[9],[3],[31]	[9],[3]		[9]	-	
Insecure Interfaces and API	[9],[3]	[9]	-	[20]		
Denial of Service	[9],[22][31]	[9],[3]	[22]	[9],[62]	[9]	
Malicious Insiders	[9],[3],[4]	[9],[3]	[9]	-	[9]	-
Abuse of Cloud Services	[4]	-	-	-	-	-
Insufficient Due Diligence	-	-	-	-	-	-
Shared Technology Vulnerabilities/Issues	[3],[4]	[3]	-	[9],[17],[20],[61]	[3]	-
Drive-by exploits	V[31]	-	-	-	-	-
Worms/Trojans						

Code Injection	[3],[22],[31]	[3]	-	-	-	-
Compromising Confidential Information	[9],[3]	[9],[3]	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	[9]	[9],[3]	-
Identity Theft	[9]	[9]	-	[9]	-	-
Rogue Certificates	[31]	-	-	-	-	-
Hardware Failure					[9],[3]	-
Natural Disasters					[9],[3]	-
Injection	[9],[22]	[9],[22]				
Broken Authentication and Session Management	[9],[3]	[9],[3]	[22]	[9]	-	[22]
Cross-Site Scripting (XSS)	[3],[31]	[3]	-	-	-	-
Insecure Direct Object References	[31]	-	-	-	-	-
Security Misconfiguration	[31]	-	-	-	-	-

Sensitive Data Exposure	[9],[31]	[9],[3]	-	-	-	-
Missing Function Level Access Control	V[31]	-	-	-	-	-
Cross-Site Request Forgery (CSRF)	[31]	[3]	-	-	-	-
Using Known Vulnerable Components	[31]	[3]	-	-	-	-
Unvalidated Redirects and Forwards	[31]	[3]	-	-	-	-
Access control verification	-	[3]	-	-	-	-
cookies manuplation	-	[3]	-	-	-	-
hidden field manuplation	-	[3]	-	-	-	-
Inter VM Attacks	[10]	[10]	[10]	[10],[62]	[10]	[10]
XML signature element wrapping attack	[22]	-	-	-	-	-

This table elaborates the actual no of references, of Cloud computing security threats for cloud components. This table describes the original no of references of threats for cloud components i.e. Application, data, platform, resource abstraction, physical infrastructure and facility. In this table there is just no of references for all threats, these threats are taken from literature although by threat definition there is some ambiguity between these threats because some of these threats are actually attacks and some are vulnerabilities . but in 1st phase we are taking all threats as discussed in literature .We have included just those papers which have discussed the given threat with respect to cloud components. In this table we have just count of total references of threats.

By this table approximate 50 threats are addressed in literature. If we observe this table data and application is much vulnerable then other cloud components and facility is ignored or missing.

TABLE 5.3: Threats at Component level (Indirectly discussed in literature)

	Components					
Threat	Application	Data	Platform	Resource Abstrection	Physical Infrastrectur	Facility
Data Breaches	[4],[26],[61], [28]	[4],[26],[20], [61],[28]	[4],[26],[61], [28]	[61],[28]	[4],[26],[61], [28]	[4],[9],[61]
Data Loss	[26],[61],[28]	[63], [26],[61],[32]	[26],[61],[28]	[21],L[61],[32]	[26],[61],[28]	[26],[61]
Account or Service Traffic Hijacking	[4],[26],[20], [61], [28]	[63], [4],[61],[28]	[4],[26],[20], [61], [28]	[4],[26], [20], [61],[28]	[20],[61]	[4],[26],[61]
Insecure Interfaces and API	[22],[4],[26], 10],[20],[61],[28]	[22],[4],[26], [5],[20],[61], [28],[60]	[22],[4],[26], [5],[20], [61], [28]	[22],[4], [26], [10],[20],[61],[28]	[28]	[22],[4], [26], [5]
Denial of Service	[22],[20],[28]	[22],[4],[26], [5],[20], [61], [28], [60]	[22],[20],[28]	[62], [20], [28]	[28]	[22]
Malicious Insiders	[?],[26],[5], [20],[61],[28]	[4],[26],[5] [20],[61],[28]	[4],[26],[5], [20],[61],[28]	[4],[26],[5], [20].[61],[28]	[4],[26],[5], [20], [61]	[?], [26],[5],[20], [61]
Abuse of Cloud Services	[?],[26],[5], [61],[28]	[?],[26],[5], [61]	[4],[26],[5], [61],[28]	[26],[5],[28]	[26],[5],[61]	[4], [26],[5]
Insufficient Due Diligence	[61],[28]	[61]	[61],[32]	[61]	[61]	[61]

Shared Technology Vulnerabilities/Issues	[4],[26],[5], [62],[61],[28]	[4],[5],[62], [61],[28]	[4],[62],[20], [61],[28]	[4],[26], [5],[28]	[20],,[61]	[26],[61]
Code Injection	[22]	[22]	[22],[31]	[22]	-	[22]
Hardware Failure	[61]	[61]	[61]	[61]	[61]	
Natural Disasters	[61]	[61]	[61]	[61]	[61]	
Closure of Cloud Service	-	[61]	-	-	-	
Cloud-related Malware	[61]	[61]	[61]	[61]	[61]	[61]
XML signature element wrapping attack	[22]	[22]	-	[22]	-	
Unknown Risk Profile	[61]	[61]	[61]	[61]	[61]	[61]
LOSS OF GOVERNANCE:	-	[59]	-	-	-	-
COMPLIANCE RISKS	-	[59]	-	-	-	-
MANAGEMENT INTERFACE COMPROMISE:	-	[59]	-	-	-	-

DATA PROTECTION:	-	[59]	-	-	-	-

This table elaborates the actual no of references, of Cloud computing security threats for cloud components. This table describes the original no of references of threats for cloud components i.e. Application, data, platform, resource abstraction, physical infrastructure and facility. This table describes the references of threats which are by our understanding targeting the threats for cloud components. Author doesn't have clear description about components but by his disruption it can be understand that author is addressing these cloud components.

In this table there is just no of references for all threats, these threats are taken from literature; there is some ambiguity between these threats because some of these threats are actually attacks and some are vulnerabilities. But in 1st phase we are taking all threats as discussed in literature .We have included just those papers which have discussed the given threat with respect to cloud components. In this table we have just count of total references of threats.

By this table approximate 50 threats are addressed in literature. If we observe this table the threats data loss, data breaches, account or service traffic hijacking, insecure interfaces, denial of services, malicious insiders, abuse of cloud services, insufficient due diligence, shared technology issues have more impact on Application, data, platform, resource abstraction, physical infrastructure, and facility then other threats .

TABLE 5.4: Threats at Cloud deployment models level (clearly discussed in literature)

Deployment Model				
Threat	Public	Private	Community	Hybrid
Data Breaches	[9],[?],[10],[59],[60]	[9]	[9]	[9], [59]
Data Loss	[9],[21],[?],[5], [61],[?],[60]	[9]	[9]	[9],[59]
Account or Service Traffic Hijacking	[9],[?],[5], [20],[61],[60]	[9],[5]	[9]	[9]
Insecure Interfaces and API	[9],[4],[10], [20],[61]	[9]	[9]	[9]
Denial of Service	[9], [22],[20],[60]	[9]	[9],[22]	[9]
Malicious Insiders	[9],[4],[10], [20],[61],[59],[60]	[9],	[9]	[9],[?]
Abuse of Cloud Services	[4],[5], [61],[60]	-	-	-
Insufficient Due Diligence	H[61],V[60]	-	-	-
Shared Technology Vulnerabilities/Issues	[4],[20],[60]	-	-	-
Drive-by exploits	[30]	-	-	-
Worms/Trojans	[30]	-	-	-
Code Injection	[22]	-	-	-
Exploit Kits	[30]	-	-	-
Botnets	[30]	-	-	-
Phishing	[30]	-	-	-

Compromising Confidential Information	[9]	[9]	[9]	[9]
Rogueware/ Scareware	[30]	-	-	-
Identity Theft	[9]	[9]	[9]	[9]
Abuse of Information Leakage	[30]	-	-	-
Hardware Failure	[61]	-	-	-
Natural Disasters	[61]	-	-	-
Closure of Cloud Service	[61]	-	-	-
Cloud-related Malware	[61]	-	-	-
Injection	[9],[22]	[9]	[9],[22]	[9],[22]
Broken Authentication and Session Management	[9]	[9]	[9]	[9]
Security Misconfiguration	-	-	-	[3]
Sensitive Data Exposure	[9]	[9]	[9]	[9]
Cross-Site Request Forgery (CSRF)	-	-	-	[3]
Using Known Vulnerable Components	-	-	-	[3]

Unvalidated Redirects and Forwards	-	-	-	[3]
Access control verification	-	-	-	[3]
cookies manuplation	-	-	-	[3]
hidden field manuplation	-	-	-	[3]
Inter VM Attacks	[10]	[10]	[10]	[10]
XML signature element wrapping attack	[22]	-	-	-
Unknown Risk Profile	[5],[61]	-	-	-
LOSS OF GOVERNANCE:	[59]	-	-	[59]
LOCK-IN	[59]	-	-	[59]
ISOLATION FAILURE	[59]	-	-	[59]
COMPLIANCE RISKS	[59]	-	-	[59]
MANAGEMENT INTERFACE COMPROMISE:	[59]	-	-	[59]
DATA PROTECTION:	[59]	-	-	[59]

This table elaborates the actual no of references, of Cloud computing security threats for cloud deployment models i.e. Public cloud, Private cloud, community cloud, hybrid cloud. This table describes the original no of references of threats for cloud deployment models.. In this table there is just no of references for all threats, these threats are taken from literature, although by threat definition there is some ambiguity between these threats because some of these threats are actually attacks and some are vulnerabilities . But in 1st phase we are taking all threats as discussed in literature .We have included just those papers which have discussed the given threat with respect to cloud components. In this table we have just count of total references of threats.

If we observe this table public cloud in more vulnerable then other cloud deployment models for all threats.

TABLE 5.5: Threats at Cloud deployment models level (Indirectly discussed in literature)

	Deployment Model			
Threat	Public	Private	Community	Hybrid
Data Breaches	V[26],[61],[28]	[4],[26],[18],[61],[28]	[4],[26],[18],[61],[28]	[4],[26],[20], [61],[28],[60]
Data Loss	[26],[61],[28]	[26],[61],[28]	[9],[21], [26],[61],[28]	[9],[21],[26],[61],[28]
Account or Service Traffic Hijacking	[26],[31],[28]	[4],[26],[20], [61],[28]	[9],[4],[26], [10],[20],[61],[28]	[9],[4],[26],[5],[20], [61],[28],[60]
Insecure Interfaces and API	[22],[26],[61],[28]	[22],[4],[26],[10], [20],[61],[28]	[9],[22],[?], [26],[10],[20],[61],[28]	[9],[22],[4], [26],[10],[20],[61],[28],[60]
Denial of Service	[22],[28]	[22],[20],[28]	[9],[22],[20],[28]	[9],[22],[20], [28],[60]
Malicious Insiders	[?],[26],[28]	[4],[26],[5], [20],[61],[28]	[9],[?],[26], [5],[20],[61],[28]	[9],[4],[26], [5],[20],[61],[28],[60]
Abuse of Cloud Services	[26],[28]	[4],[26],[5],[61],[28]	[9],[4],[26], [5].[61],[28]	[9],[4],[26], [5],[61],[28],[60]
Insufficient Due Diligence	[28]	[61],[28]	[61],[32]	[61],[28],[60]
Shared Technology Vulnerabilities/Issues	[26],[5],[17], [61],[28]	[4],[26],[5],[62],[61], [28]	[4],[26],[5], [62],[61],[28]	[4],[26],[5],[17],[61],[28],[60]
Code Injection	[22],[31]	[22]	[22]	[22]
Rogueware/ Scareware	-	-	[9]	[9]

Abuse of Information Leakage	-	-	[9]	[9]
Hardware Failure	-	[61]	[61]	[61]
Natural Disasters	-	[61]	[61]	[61]
Cloud-related Malware	-	[61]	[61]	[61]
Injection	[31]	-	-	
Broken Authentication and Session Management	[31]	-	[9]	[9]
Cross-Site Scripting (XSS)	[31]	-	[9]	[9]
Sensitive Data Exposure	-	-	-	[3]
Missing Function Level Access Control	-	-	[9]	[9]
Using Known Vulnerable Components	-	-	-	[3]
Unvalidated Redirects and Forwards	-	-	-	[3]

Access control verification	-	-	-	[3]
cookies manuplation	-	-	-	[3]
hidden field manuplation	-	-	-	[3]
Inter VM Attacks	-	-	-	[3]
XML signature element wrapping attack	-	[22]	[22]	[22]
Unknown Risk Profile	-	[61]	,[61]	,[61]
LOSS OF GOVERNANCE:	-	-	[59]	-
LOCK-IN	-	-	[59]	-
ISOLATION FAILURE	-	-	[59]	-
COMPLIANCE RISKS	-	-	[59]	-
MANAGEMENT INTERFACE COMPROMISE:	-	-	[59]	-

DATA PROTECTION:	-	-	[59]	-

This table elaborates the actual no of references, of Cloud computing security threats for cloud deployment models i.e. Public cloud, Private cloud, community cloud, hybrid cloud. This table describes the original no of references of threats for cloud deployment models. This table describes the references of threats which are by our understanding targeting the threats for cloud service models.

Author doesn't have clear description about service model but by his disruption it can be understand that author is addressing this deployment model. In this table there is just no of references for all threats, these threats are taken from literature, although by threat definition there is some ambiguity between these threats because some of these threats are actually attacks and some are vulnerabilities . But in 1st phase we are taking all threats as discussed in literature. We have included just those papers which have discussed the given threat with respect to cloud components. In this table we have just count of total references of threats.

If we observe this table we can see all cloud deployment models have some important threats like Data breach, data loss, account or service traffic hijacking, insecure interfaces, Denial of services, malicious insiders, abuse of cloud services, share technology issues etc.

TABLE 5.6: Threats at Cloud service models level (clearly discussed in literature)

Service Model			
Threat	**SaaS**	**Paas**	**IaaS**
Data Breaches	[9],[3],[4], [26],[28]	[26],[28]	[26],[28]
Data Loss	[9],[3], [1],H[21],[4],[20],[28]	[26],[28]	[26],[28]
Account or Service Traffic Hijacking	[9],[3], [4],[26],[5], [20],[28]	[26],[5],[28]	[26],[5],[28]
Insecure Interfaces and API	[9],[3],[4], [26],[5],[20], [61],[28]	[26],[5],[28]	[26],[5],[28]
Denial of Service	[9],[10],[22],[26],[20],[28]	[9],[22],[26],[28]	[9],[22],[26],[62],[28]
Malicious Insiders	[?],[26],[10],[20],[61],[28]	[9],[26],[5], [20],[28]	[9],[26],[5], [20],[28]
Abuse of Cloud Services	[4],[5],[61]	[26],[5],[28]	[26],[5],[28]
Insufficient Due Diligence	[61],[28]	[28]	[28]
Shared Technology Vulnerabilities/Issues	[3],[4],[17],[28]	[28]	[3],[26],[5], [20],[61],[28]
Drive-by exploits	[30]	-	-
Worms/Trojans	[30]	-	-
Code Injection	[3],[22]	[26]	
Exploit Kits	[30]	-	-
Botnets	[30]	-	-
Phishing	[30]	-	-
Compromising Confidential Information	[9],[3],[1]	-	-

Rogueware/ Scareware	[30]	-	-
Physical Theft/Loss/Damage	-	[9]	[9],[3]
Identity Theft	[9]	-	-
Abuse of Information Leakage	[30]	-	-
Hardware Failure	-	-	[3]
Natural Disasters	-	-	[3]
Closure of Cloud Service	[61]	-	-
Cloud-related Malware	[61]	[61]	[61]
Injection	[9],[22]	-	-
Broken Authentication and Session Management	[9],[3]	-	-
Cross-Site Scripting (XSS)	[3]	-	
Insecure Direct Object References	[3]	-	
Security Misconfiguration	[9]	[9]	[9]
Sensitive Data Exposure	[9]	-	-
Missing Function Level Access Control	[3]	-	-
Cross-Site Request Forgery (CSRF)	[3]	-	-
Using Known Vulnerable Components	[9]	[9]	[9]
Access control verification	[3]	-	-

cookies manuplation	[3]	-	-
hidden field manuplation	[3]	-	-
Inter VM Attacks	[10], [62]	[10]	V[10],[26],[62]
XML signature element wrapping attack	[22]	-	

This table elaborates the actual no of references, of Cloud computing security threats for cloud service models i.e. Software as a service SaaS, Platform as a Service PaaS, Infrastrecture as a Service IaaS. This table describes the original no of references of threats for cloud service models.. In this table there is just no of references for all threats, these threats are taken from literature, although by threat definition there is some ambiguity between these threats because some of these threats are actually attacks and some are vulnerabilities . but in 1st phase we are taking all threats as discussed in literature .We have included just those papers which have discussed the given threat with respect to cloud components. In this table we have just count of total references of threats.

If we observe this table SaaS service model have more threats then other service models and data breaches, data loss, account or service traffic hijacking, insecure interfaces, denial of services, malicious insiders, abuse of cloud services, shared technology vulnerabilities are the common threats for cloud service models.

TABLE 5.7: Threats at Cloud service models level (Indirectly discussed in literature)

	Service Model		
	SaaS	Paas	IaaS
Data Breaches	[?],[61]	[4],[20],[61]	[?],[61]
Data Loss	H[61]	[21],[61]	[61]
Account or Service Traffic Hijacking	[20],[61]	[4],[20],[61]	[?],[20],[61]
Insecure Interfaces and API	[22],[31]	[22],[4],[20],[61]	[22],[4],[20],[61]
Denial of Service	[22],[18]	[22],[20]	[22],[20]
Malicious Insiders	-	[4],[20],[61]	[4],[20],[61]
Abuse of Cloud Services	[26],[5]	[?],[5],[61]	[?],[5],[61]
Insufficient Due Diligence	-	[61]	[61]
Shared Technology Vulnerabilities/Issues	[26],[20],[61]	[4],[26],[62], [20],[61]	[4],[62],[20]
Code Injection	[22],[31]	[22],[20],[31]	[22],[31]
Hardware Failure	[61]	[61]	[61]
Natural Disasters	[61]	[61]	[61]
Cloud-related Malware	[61]	[61]	[61]
Injection	[31]	[31]	[31]
Broken Authentication and Session Management	H[26]	-	-

Cross-Site Scripting (XSS)	[31]	-	-
XML signature element wrapping attack	-	[22]	[22]
Unknown Risk Profile	[61]	,[61]	,[61]
LOSS OF GOVERNANCE:	[59]	[59]	[59]
LOCK-IN	[59]	[59]	[59]
ISOLATION FAILURE	-	-	[59]

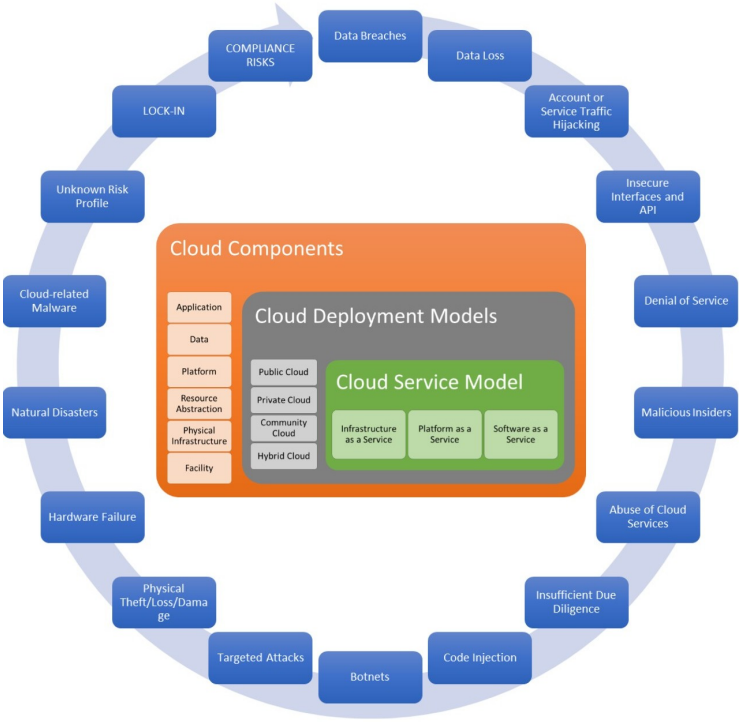
This table elaborates the actual no of references, of Cloud computing security threats for cloud service models i.e. Software as a service SaaS, Platform as a Service PaaS, Infrastructure as a Service IaaS. This table describes the references of threats which are by our understanding targeting the threats for cloud service models. Author doesn't have clear description about service model but by his disruption it can be understand that author is addressing this service model. In this table there is just no of references for all threats, these threats are taken from literature, although by threat definition there is some ambiguity between these threats because some of these threats are actually attacks and some are vulnerabilities . But in 1st phase we are taking all threats as discussed in literature .We have included just those papers which have discussed the given threat with respect to cloud components. In this table we have just count of total references of threats.

If we observe this table PaaS and IaaS service model have also threats like SaaS. The difference is just the target of auther is most probably Saas but in description he is also addressing PaaS and IaaS. Data breaches, data loss, account or service traffic hijacking, insecure interfaces, denial of services, malicious insiders, abuse of cloud services, shared technology vulnerabilities are the common threats for cloud service models.

5.4 Proposed Cloud Reference Model

we will analyze the selected cloud computing security threats for all cloud service models. i.e. PaaS (platform as a service), IaaS (infrastructure as a service) , SaaS (software as a service) and for all cloud deployment models and cloud components.

5.5 Analysis of Security Threats at Cloud Component Level



Model Picture.jpg Model Picture.jpg

FIGURE 5.2: Proposed Model

TABLE 5.8: Severity level of threats for Cloud components (directly discussed in literature)

	Components					
Threat	Application	Data	Platform	Resource Abstrection	Physical Infrastrectur	Facility
Data Breaches	H[9],H[3]	H[9],H[3],H[1],H[4], V[5]	-	-	-	-
Data Loss	H[9],H[3]	H[9],H[3],H[1],H[21], V[5],V[20], H[61]	-	-	-	-
Account or Service Traffic Hijacking	H[9],H[3],V[31]	H[9],H[3]		H[9]	-	-
Insecure Interfaces and API	H[9],H[3]	H[9]	-	H[20]		
Denial of Service	H[9],H[22], V[31]	H[9], H[3]	H[22]	H[9],H[62]	H[9]	
Malicious Insiders	H[9],H[3],V[?]	H[9],H[3]	H[9]	-	H[9]	-
Abuse of Cloud Services	V[4]	-	-	-	-	-
Insufficient Due Diligence	-	-	-	-	-	-
Code Injection	H[3],H[22],V[31], H[9]	H[3],H[9],H[22]	-	-	-	-
Targeted Attacks	-	-	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	H[9]	H[9],H[3]	-
Hardware Failure	-	-	-	-	H[9],H[3]	-
Natural Disasters	-	-	-	-	H[9],H[3]	-

Cloud-related Malware	-	-	-	-	-	-
Unknown Risk Profile	-	-	-	-	-	-
LOSS OF GOVERNANCE:	-	-	-	-	-	-
LOCK-IN	-	-	-	-	-	-
COMPLIANCE RISKS	-	-	-	-	-	-

This table elaborates the actual no of references and the impact of Cloud computing security threats for cloud components. If we observe this table we will find that Data loss is high threat for data. As per literature 5 times it has been found high threat and 2 times it has been found very high threats. Data breaches for data is also important, 4 times it's high and once it's very high. Data loss and data breaches are also high threat for applications. Denial of services and malicious insiders are high level threats for application. Code injections are also high level threats for applications.

Hardware failure and natural disasters are also high level threats for physical infrastecture. Physical security is also important for physical infrastructure. Abuse of Cloud Services is also very high threats as per some researchers. Insecure interfaces are also high threats for applications.

TABLE 5.9: Average Severity level of threats for Cloud Components (clearly discussed in literature)

Components						
Threat	Application	Data	Platform	Resource Abstrection	Physical Infrastrectur	Facility
Data Breaches	3	3	-	-	-	-
Data Loss	3	3.29	-	-	-	-
Account or Service Traffic Hijacking	3.33	3	-	3	-	-
Insecure Interfaces and API	3	3	-	3	-	-
Denial of Service	3.33	3	3	3	3	-
Malicious Insiders	3.33	3	3	-	3	-
Abuse of Cloud Services	4	-	-	-	-	-
Insufficient Due Diligence	-	-	-	-	-	-
Code Injection	3.33	3	-	-	-	-
Botnets	-	-	-	-	-	-
Targeted Attacks	-	-	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	3	3	-
Hardware Failure	-	-	-	-	3	-
Natural Disasters	-	-	-	-	3	-
Cloud-related Malware	-	-	-	-	-	-
Unknown Risk Profile	-	-	-	-	-	-
LOCK-IN	-	-	-	-	-	-

COMPLIANCE RISKS	-	-	-	-	-	-

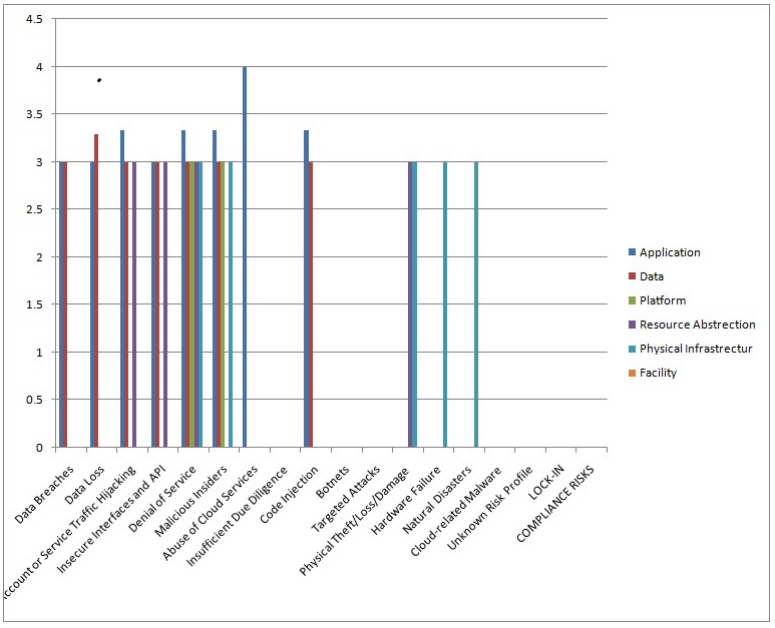


FIGURE 5.3: Average Severity level of threats for Cloud Components (clearly discussed in literature)

This table elaborates average of references and the impact of Cloud computing security threats for cloud components. This average has been taken by reviewing the author's emphasis regarding threat. We took the values as 1 for Low, 2 for medium, 3 high, 4 for very high. 0 is by default for no discussion but 0 doesn't mean the threat don't have any impact. It means the author donot have discussed about threat or the threat has very low impact with this regard which is negligible. The average has been taken by adding the values and dividing by no of references. This average helps us to determine the overall impact of threat. This average for this table is between 3 to 4, it can be explained if it is 4 this threat have very high impact and if it is 3 it have high impact overall. If it is more then 3 and less then 4 then it have more then high impact. If we look this table abuse of cloud services is very high level threat for applications and malicious insider is high level threat for application, data, platform and physical infrastructure.

Most of the threats are high level threats for application like data loss, data breach, account or service traffic hijacking, denial of services, malicious insiders, code injections etc

TABLE 5.10: Severity level of threats for Cloud components (Indirectly discussed in literature)

Threat	**Components**					
	Application	Data	Platform	Resource Abstrection	Physical Infrastrectur	Facility
Data Breaches	H[4],H[26],M[61], H[28]	V[4],V[26],V[20], V[61],V[28]	H[4],M[26],M[61], M[28]	L[61],L[28]	H[4],H[26],H[61], H[28]	H[?],H9],H[61]
Data Loss	H[26],M[61], H[28]	H[63],V[26], V[61],V32]	M[26],M[61],M[28]	H[21],L[61],L32]	H[26],H[61],H[28]	H[26],H[61]
Account or Service Traffic Hijacking	H[?],L[26],L[20], H[61],V[28]	H[63],H[?],H[61], L[28]	H[4],M[26],M[20], H[61],M[28]	L[4],M[26],L[20], M[61],L[28]	L[20],H[61]	H[4],L[26],H[61]
Insecure Interfaces and API	V[22],H[?],M[26], H10],V[20],H[61],H[28]	V[22],H[4],V[26], H[5],V[20],H[61], H[28],H[60]	H[22],H[4],V[26], H[5],V[20],H[61], H[28]	V[22],H[4],V[26], H10],V[20],H[61],M[28]	L[28]	V[22],H[?],H[26], H[5]
Denial of Service	V[22],H[20], H[28]	V[22],H[4],V[26], H[5],V[20],H[61], H[28],H[60]	H[22],H[20],H[28]	V[62],H[20], M[28]	L[28]	H[22]
Malicious Insiders	V[?],V[26],H[5], V[20],H[61],H[28]	V[4],V[26],V[5], V[20],H[61],H[28]	V[4],V[26],M[5], V[20],H[61],H[28]	V[4],V[26],L[5], V[20].H[61],M[28]	V[4],V[26],V[5], V[20],H[61]	V[4],V[26],H[5], V[20],H[61]
Abuse of Cloud Services	V[4],L[26],M[5], H[61],L[28]	V[4],L[26],M[5], H[61]	V[4],V[26],M[5], H[61],H[28]	L[26],L[5],L[28]	M[26],M[5],H[61]	V[4],L[26],M[5]
Insufficient Due Diligence	L[61],L[28]	H[61]	M[61],L32]	H[61]	H[61]	M[61]
Code Injection	H[22]	V[22]	H[22],H[31]	H[22]	-	H[22]

Botnets	-	-	-	-	-	-
Targeted Attacks	-	-	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	-	-	-
Hardware Failure	M[61]	H[61]	L[61]	L[61]	H[61]	
Natural Disasters	M[61]	H[61]	L[61]	L[61]	H[61]	
Cloud-related Malware	H[61]	H[61]	H[61]	H[61]	L[61]	L[61]
Unknown Risk Profile	L[61]	M[61]	H[61]	M[61]	M[61]	L[61]
LOCK-IN	-	-	-	-	-	-
COMPLIANCE RISKS	-	H[59]	-	-	-	-

This tales describes the references and the impact of Threats with respect to cloud computing components, like L for low, M for medium, H for high, V for very high. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low, if authors have discussed some how its severity then we took it as medium, if by authors point of view the threat have high impact we assigned H because it have high impact, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat If we observe the table Insecure Interfaces are the major threat for applications, data, platform and malicious insider is common for all components like application, data, platform, resource abstraction, physical infrastructure and facilities.

This table describes the no of references of threats for cloud components i.e. Application, data, platform, resource abstraction, physical infrastructure and facility and describes the references of threats which are by our understanding targeting the threats for cloud components. Author doesn't have clear description about components but by his disruption it can be understand that author is addressing these cloud components.

Other threats like compliance risks, vender lock-in, unknown risks, malwares, disasters, hardware failure, physical theft, targeted and code injections are addressed by very few researchers. It doesn't mean these threats are not serious threats; these threats also can be very dangerous.

TABLE 5.11: Average Severity level of threats for Cloud Components (Indirectly discussed in literature)

	Components					
Threat	Application	Data	Platform	Resource Abstrection	Physical Infrastrectur	Facility
Data Breaches	2.75	4	2.25	1	3	3
Data Loss	2.67	3.75	2	1.33	3	3
Account or Service Traffic Hijacking	2.4	2.5	2.4	1.4	2	2.33
Insecure Interfaces and API	3.14	3.38	3.29	3.71	1	3.25
Denial of Service	3.33	3.37	3	3	1	3
Malicious Insiders	3	3.67	3.33	3	3.8	3.6
Abuse of Cloud Services	2.2	2.5	3.2	1	2.33	2
Insufficient Due Diligence	1	3	1.5	3	3	2
Code Injection	3	3	3	3		3
Botnets	-	-	-	-	-	
Targeted Attacks	-	-	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	-	-	-
Hardware Failure	2	3	1	1	3	-
Natural Disasters	2	3	1	1	3	-
Cloud-related Malware	3	3	3	3	1	1
Unknown Risk Profile	1	2	3	2	2	1
LOCK-IN	-	-	-	-	-	-

COMPLIANCE RISKS	-	3	-	-	-	-

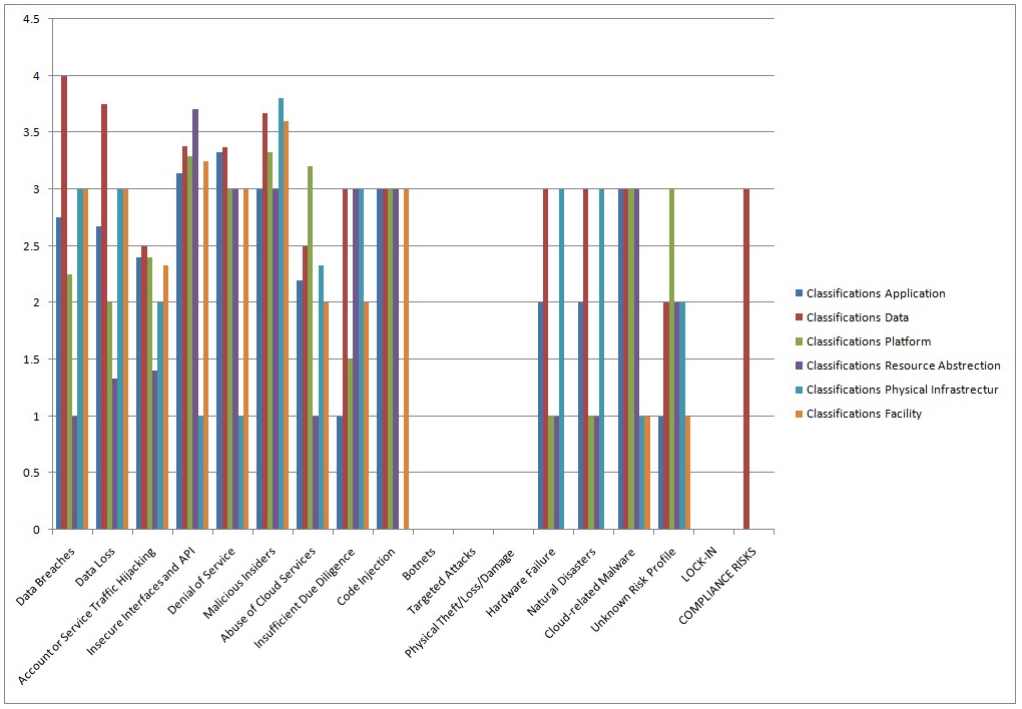


FIGURE 5.4: Average Severity level of threats for Cloud Components (Indirectly discussed in literature)

This table elaborates average of references and the impact of Cloud computing security threats for cloud components. This average has been taken by reviewing the author's emphasis regarding threat. We took the values as 1 for Low, 2 for medium, 3 high, 4 for very high. 0 is by default for no discussion but 0 doesn't mean the threat don't have any impact. It means the author doesn't have discussed about threat or the threat has very low impact with this regard which is negligible. The average has been taken by adding the values and dividing by no of references. This average helps us to determine the overall impact of threat.

If we observe these averages. These averages vary from 1 to 4. For application data loss and data breach is approximately 3 it means these are high level threats for application. Insecure interfaces and denial of services have value more then 3 which show these threats are more then high level threat for application. Malicious insider is also high level threat for application, more then high for data and platform, resource abstraction, physical infrastructure as well as facility. Insecure interface are also more then high level threat for data, platform and resource abstraction.

5.6 Analysis of Security Threats at Cloud Deployment Level

TABLE 5.12: Severity level of threats for Cloud deployment models (clearly discussed in literature)

Threat	**Deployment Model**			
	Public	Private	Community	Hybrid
Data Breaches	V[9],V[4],V10], H[?],V[60]	H[9]	H[9]	H[9],H[?]
Data Loss	V[9],V[21], V[4],V[5],H[61], H[?],V[60]	H[9]	H[9]	H[9],H[?]
Account or Service Traffic Hijacking	V[9],[?],V[5], V[20],V[61],V[60]	H[9],L[5]	H[9]	H[9]
Insecure Interfaces and API	V[9],V[4],V[10], V[20],H[61]	H[9]	H[9]	H[9]
Denial of Service	V[9],V[22],H[20], V[60]	H[9]	H[9],H[22]	H[9]
Malicious Insiders	V[9],V[4],V10], V[20],H[61],H[?], V[60]	H[9],	H[9]	H[9],H[?]
Abuse of Cloud Services	V[?],M[5],H[61], V[60]	-	-	-
Insufficient Due Diligence	H[61],V[60]	-	-	-
Code Injection	H[22],H[9]	H[9]	H[9],H[22]	H[9],H[22]
Botnets	H[30]	-	-	-
Targeted Attacks	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	-

Hardware Failure	H[61]	-	-	-
Natural Disasters	H[61]	-	-	-
Cloud-related Malware	V[61]	-	-	-
Unknown Risk Profile	V[5],H[61]	-	-	-
LOCK-IN	H[59]	-	-	H[59]
COMPLIANCE RISKS	H[59]	-	-	H[59]

This table describes the original no of references and what is the impact of threats for deployment model. In this table there is just no of references, and level of impact like L for low, M for medium, H for high, V for very high. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low, if authors have discussed some how its severity then we took it as medium, if by authors point of view the threat have high impact we assigned H because it have high impact, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat.

We have included just those papers which have discussed the given threat with respect to cloud deployment models like public cloud, private cloud, community cloud, hybrid cloud. Just those papers are included which have directly discussed the threats with respect to cloud deployment model. In this table we have just count of total references of threats for cloud deployment model. If we notice the pattern of this table we can see the most focus target of literature is public cloud.

For public cloud most of the threats have high impact or very high impact like data breach 3 authors declared it very high threat for public cloud and 1 declared it high, data loss 4 declared it very high and 2 declared it high threat for public cloud, account or service traffic hijacking all 4 authors declared it very high threat for public cloud, insecure interfaces 4 declared it very high and 1 declared it as high level threat, malicious insider 4 declared it as very high and 2 declared it as high threat etc. most of research has focus on public cloud other deployment models like private, community , hybrid are less addressed in literature. The reason can be public cloud is available anywhere without any geographical boundary and domain.

TABLE 5.13: Average Severity level of threats for Cloud Deployment models (clearly discussed in literature)

	Deployment Model			
Threat	Public	Private	Community	Hybrid
Data Breaches	4	3	3	3
Data Loss	3.71	3	3	3
Account or Service Traffic Hijacking	4	2	3	3
Insecure Interfaces and API	3.8	3	3	3
Denial of Service	3.75	3	3	3
Malicious Insiders	3.71	3	3	3
Abuse of Cloud Services	3.25	-	-	-
Insufficient Due Diligence	3.5	-	-	-
Code Injection	3.5	3	3	3
Botnets	3	-	-	-
Targeted Attacks	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	-
Hardware Failure	3	-	-	-
Natural Disasters	3	-	-	-
Cloud-related Malware	4	-	-	-
Unknown Risk Profile	3.5	-	-	-
LOCK-IN	3	-	-	3
COMPLIANCE RISKS	3	-	-	3

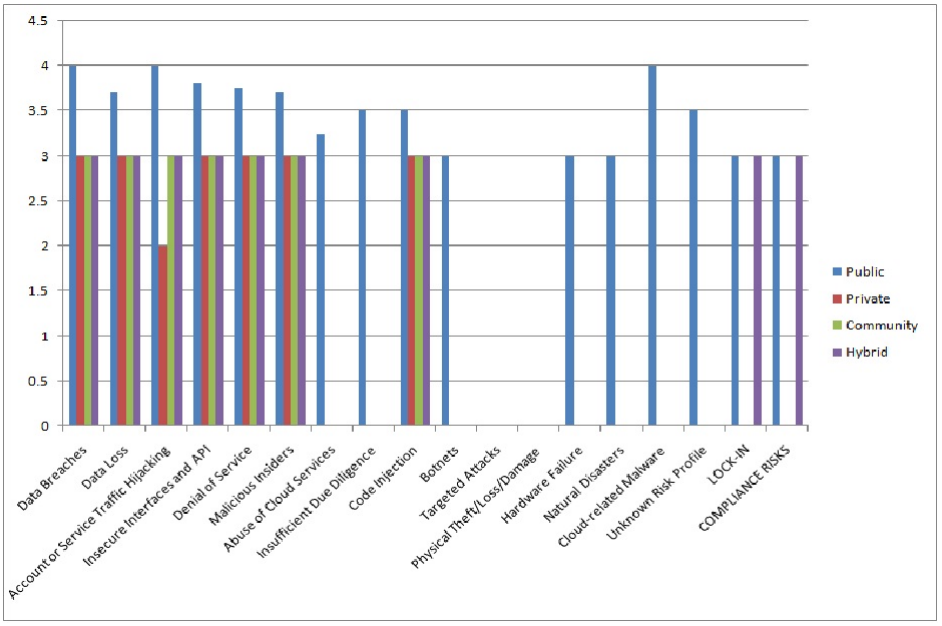


FIGURE 5.5: Average Severity level of threats for Cloud Deployment models (Clearly discussed in literature)

This table describes the average impact of threats for cloud deployment models i.e. Public cloud, private cloud, community cloud, Hybrid cloud. In this table level of impact like L for low, M for medium, H for high, V for very high and values are assigned as 1 for low, 2 for medium, 3 for high, 4 for very high, 0 or no value is assigned if authors don't have discussed relevant threat. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low and value of low is 1, if authors have discussed some how its severity then we took it as medium and value of medium is 2, if by authors point of view the threat have high impact we assigned H because it have high impact value assigned for high is 3, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat the assigned value is 4. The average is taken by adding all vales and dividing by no of referred papers.

We have included just those papers which have discussed the given threat with respect to cloud deployment models like public cloud, private cloud, community cloud, hybrid cloud. Just those papers are included which have directly discussed the threats with respect to cloud deployment model. In this table we have just count of total references of threats for cloud deployment model. If we notice the pattern of this table we can see the most focus target of literature is public cloud.

The average varies from 2 to 4. For data breaches, account, service traffic hijacking, malwares it 4 for public cloud which shows these are very high level threats for public cloud. Insecure interfaces, data loss, denial of services, malicious insiders, insufficient due diligence and code injections have average of approximate 4, this shows these are also more then high threats for public cloud. Private cloud have less average values then public cloud which shows private cloud

in somehow secure then public cloud. This table also shows the researcher focus is on public cloud rather then other cloud deployment models.

TABLE 5.14: Severity level of threats for Cloud deployment models (Indirectly discussed in literature)

Threat	**Deployment Model**			
	Public	Private	Community	Hybrid
Data Breaches	V[26],V[61],V[28]	L[4],H[26],H18], H[61],H[28]	H[4],H[26],H[18], H[61],H[28]	H[4],H[26],H[20], H[61],H[28],H[60]
Data Loss	V[26],V[61],V[28]	H[26],H[61],H[28]	H[9],H[21],H[26], H[61],H[28]	H[9],H[21],H[26], H[61],H[28]
Account or Service Traffic Hijacking	V[26],V[31],V[28]	L[?],M[26],M[20], H[61],H[28]	H[9],H[4],M[26], M[10],M[20],H[61], H[28]	H[9],H[4],H[26], M[5],M[20],H[61], H[28],H[60]
Insecure Interfaces and API	V[22],V[26],V[61], V[28]	H[22],V[?],H[26], H[10],V[20],H[61],H[28]	H[9],V[22],H[?], H[26],H[10],V[20],H[61],H[28]	H[9],V[22],H[?], H[26],H10],V[20],H[61], H[28],H[60]
Denial of Service	V[22],V[28]	L[22],M[20],H[28]	H[9],H[22],H[20], H[28]	H[9],V[22],H[20], H[28],H[60]
Malicious Insiders	V[4],V[26], H[28]	V[4],V[26],V[5], V[20],H[61],H[28]	H[9],V[?],V[26], V[5],V[20],H[61], H[28]	H[9],V[4],V[26], V[5],V[20],H[61], H[28],H[60]
Abuse of Cloud Services	V[26],H[28]	V[4],H[26],L[5] ,H[61],L[28]	H[9],V[?],H[26], M[5].H[61],L[28]	H[9],V[4],H[26], M[5],H[61],M[28], H[60]
Insufficient Due Diligence	H[28]	M[61],L[28]	H[61],L[32]	H[61],M[28],H[60]
Code Injection	V[22],V[31], V[31]	H[22]	H[22]	H[22]
Botnets	-	-	-	-
Targeted Attacks	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	-

Hardware Failure	-	H[61]	H[61]	H[61]
Natural Disasters	-	H[61]	H[61]	H[61]
Cloud-related Malware	-	H[61]	H[61]	H[61]
Unknown Risk Profile	-	H[61]	,H[61]	,H[61]
LOCK-IN	-	-	M[59]	
COMPLIANCE RISKS	-	-	M[59]	-

This table describes the references and what is the impact of threats for deployment model. In this table there are just references, and level of impact like L for low, M for medium, H for high, V for very high. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low, if authors have discussed some how its severity then we took it as medium, if by authors point of view the threat have high impact we assigned H because it have high impact, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat.

We have included just those papers which have discussed the given threat with respect to cloud deployment models like public cloud, private cloud, community cloud, hybrid cloud. Just those papers are included which are by our understanding targeting the threats for cloud components. Author doesn't have clear description about components but by his disruption it can be understand that author is addressing these cloud deployment models.

If we observe this table we can see that the given threat data breach . for public cloud 3 authors discusses it as very high level threat, for private 1 author discussed it as low and other 4 discussed it as high level threat, for community cloud all 6 authors discussed it as high level threat. For hybrid cloud 5 authors discussed it as high level threat because hybrid cloud is very close to public cloud.

Data loss is also discussed as very high level threat for public cloud, for private its discussed it as high level threat, for community and hybrid its also as high level threat. Most of the threat for public cloud are high or very high level threat.

TABLE 5.15: Average Severity level of threats for Cloud Deployment Models (Indirectly discussed in literature)

	Deployment Model			
Threat	Public	Private	Community	Hybrid
Data Breaches	4	3.2	3	3
Data Loss	4	3	3	3
Account or Service Traffic Hijacking	4	2.2	2.57	2.75
Insecure Interfaces and API	4	3.28	3.25	3.22
Denial of Service	4	2	3	3.2
Malicious Insiders	3.67	3.67	3.57	3.5
Abuse of Cloud Services	3.5	2.4	2.67	2.86
Insufficient Due Diligence	3	1.5	2	2.67
Code Injection	4	3	3	3
Botnets	-	-	-	-
Targeted Attacks	-	-	-	-
Physical Theft/Loss/Damage	-	-	-	-
Hardware Failure	-	3	3	3
Natural Disasters	-	3	3	3
Cloud-related Malware	-	3	3	3
Unknown Risk Profile	-	3	3	3
LOCK-IN	-	-	2	-
COMPLIANCE RISKS	-	-	2	-

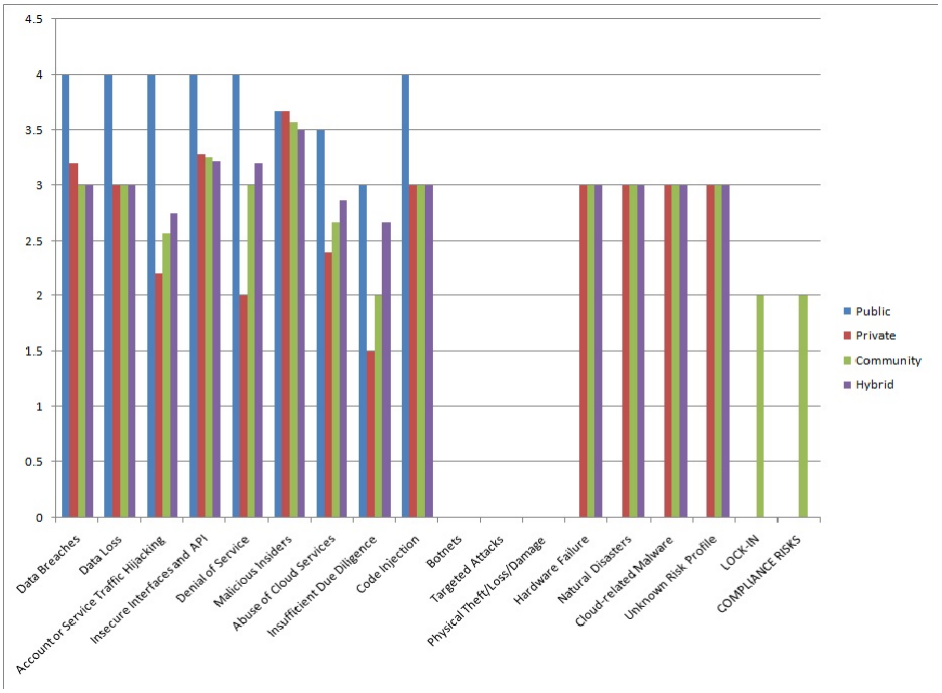


FIGURE 5.6: Average Severity level of threats for Cloud Deployment models (Indirectly discussed in literature)

This table describes the average impact of threats for cloud deployment models i.e. Public cloud, private cloud, community cloud, Hybrid cloud. In this table level of impact like L for low, M for medium, H for high, V for very high and values are assigned as 1 for low, 2 for medium, 3 for high, 4 for very high, 0 or no value is assigned if authors don't have discussed relevant threat. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low and value of low is 1, if authors have discussed some how its severity then we took it as medium and value of medium is 2, if by authors point of view the threat have high impact we assigned H because it have high impact value assigned for high is 3, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat the assigned value is 4. The average is taken by adding all vales and dividing by no of referred papers.

We have included just those papers which have discussed the given threat with respect to cloud deployment models like public cloud, private cloud, community cloud, hybrid cloud. If we observe these averages these averages varies from 1.5 to 4. For public cloud data loss,data breaches, account or service traffic hijacking, insecure interfaces, denial of services, code injections, abuse of cloud services and malicious insiders are very high level threats because the average impact of these threats for public cloud is approximately 4.

5.7 Analysis of Security Threats at Cloud Service Model Level

TABLE 5.16: Severity level of threats for Cloud service models (clearly discussed in literature)

	Service Model		
Threat	SaaS	Paas	IaaS
Data Breaches	H[9],H[3],V[?], V[26],V[28]	V[26],V[28]	V[26],V[28]
Data Loss	H[9],H[3],V[1], H[21],V[?],H[20], V[28]	V[26],V[28]	V[26], V[28]
Account or Service Traffic Hijacking	H[9],H[3],V[?], V[26],H[5],H[20], V[28]	V[26],M[5],V[28]	V[26],M[5],V[28]
Insecure Interfaces and API	H[9],H[3],V[4], V[26],H[5],H[20],H[61],V[28]	V[26],V[5],V[28]	V[26],V[5],V[28]
Denial of Service	H[9],H[10],V[22], H[26],M[20],H[28]	H[9],V[22],H[26], H[28]	H[9],V[22],H[26], V[62],H[28]
Malicious Insiders	V[4],V[26], V[10],V[20], V[61],H[28]	H[9],V[26],V[5], V[20],H[28]	H[9],V[26],V[5], V[20],H[28]
Abuse of Cloud Services	V[4],M[5], H[61]	H[26],M[5],H[28]	H[26],M[5],H[28]
Insufficient Due Diligence	H[61],M[28]	M[28]	M[28]
Code Injection	H[3],H[22], H[9]	V[26]	
Botnets	-	-	-
Targeted Attacks	-	-	-
Physical Theft/Loss/Damage	-	H[9]	H[9],H[3]
Hardware Failure	-	-	H[3]
Natural Disasters	-	-	H[3]
Cloud-related Malware	H[61]	H[61]	H[61]

Unknown Risk Profile	-	-	-
LOCK-IN	-	-	-
COMPLIANCE RISKS	-	-	-

This table describes the original no of references and what is the impact of threats for cloud service model. In this table there is just no of references, and level of impact like L for low, M for medium, H for high, V for very high. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low, if authors have discussed some how its severity then we took it as medium, if by authors point of view the threat have high impact we assigned H because it have high impact, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat.

We have included just those papers which have discussed the given threat with respect to cloud service models i.e. Software as a Service , Platform as a Service, Infrastructure as a Service. Just those papers are included which have directly discussed the threats with respect to cloud deployment model. In this table we have just count of total references of threats for cloud deployment model. If we notice the pattern of this table we can see the most focus target of literature is public cloud.

If we observe this table we can see that software as service have more threats then platform as a service and infrastructure as a service, like for data breaches 5 papers discussed it 2 declared it as high threat and other 3 discussed it as very high threat., for data loss 7 papers discussed it among 7, 4 declared it as high and other by other 3 its very high level threat., account or service traffic hijacking 7 papers discussed it 4 declared it high and remaining 3 discussed it as very high, insecure interfaces reoffered by 8 authors 5 declared high and other 3 as very high, denial of service and malicious insiders referred by 6 authors etc. There is another important finding in this table i.e. denial of service and malicious insider are commonly discussed for all service models. Some threats have very few references like malwares, naural disasters, Bonnets, code injections etc.

Although threats are discussed in less no of papers for Platform as a service and Infrastructure as a service but data breach and data loss is very high level threat for both PaaS and IaaS. Malicious insiders and denial of service is also discussed is high level threat for all cloud service models.

TABLE 5.17: Average Severity level of threats for Cloud Service models (clearly discussed in literature)

	Service Model		
Threat	SaaS	Paas	IaaS
Data Breaches	3.6	4	4
Data Loss	3.43	4	4
Account or Service Traffic Hijacking	3.43	3.33	3.33
Insecure Interfaces and API	3.37	4	4
Denial of Service	3	3.25	3.4
Malicious Insiders	3.83	3.6	3.6
Abuse of Cloud Services	3	2.67	2.67
Insufficient Due Diligence	3	2	2
Code Injection	3.5	4	-
Botnets	3	-	
Targeted Attacks	-	-	-
Physical Theft/Loss/Damage	-	3	3
Hardware Failure	-	-	3
Natural Disasters	-	-	3
Cloud-related Malware	3	3	3
Unknown Risk Profile	-	-	-
LOCK-IN	-	-	-
COMPLIANCE RISKS	-	-	-

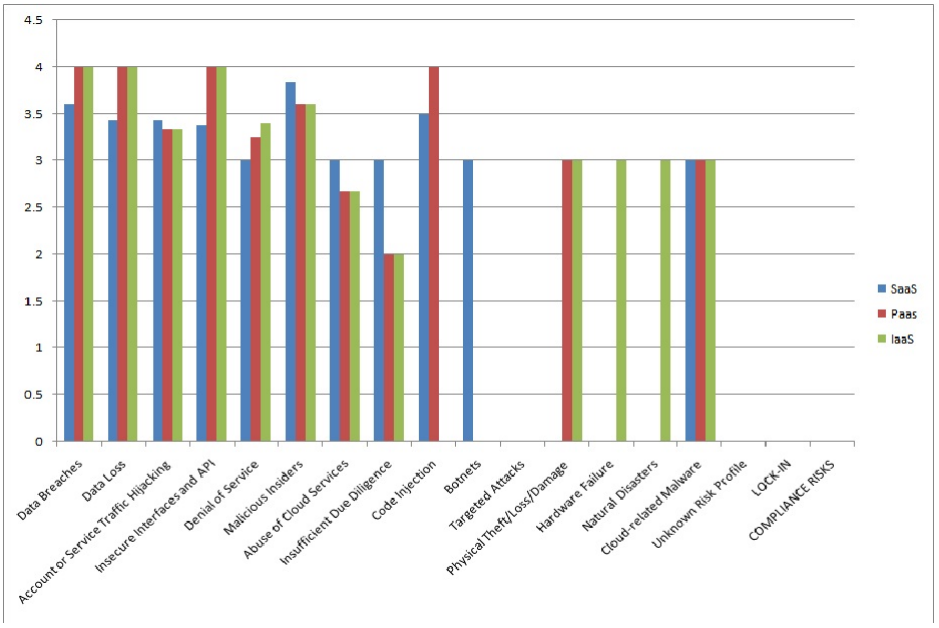


FIGURE 5.7: Average Severity level of threats for Cloud Service models (clearly discussed in literature)

This table describes the average impact of threats for cloud service models i.e. Software as a Service SaaS, Platform as a Service PaaS, Infrastructure as a Service IaaS. . In this table level of impact like L for low, M for medium, H for high, V for very high and values are assigned as 1 for low, 2 for medium, 3 for high, 4 for very high, 0 or no value is assigned if authors don't have discussed relevant threat. The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low and value of low is 1, if authors have discussed some how its severity then we took it as medium and value of medium is 2, if by authors point of view the threat have high impact we assigned H because it have high impact value assigned for high is 3, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat the assigned value is 4. The average is taken by adding all vales and dividing by no of referred papers.

We have included just those papers which have discussed the given threat with respect to cloud services. In this table we have just count of total references of threats for cloud deployment model. If we notice the pattern of this table we can see the most focus target of literature is SaaS which is Software as a Service.

If we observe the derived averages we can see the data loss and data breach both have average approximately 4 for SaaS and 4 for PaaS and IaaS, which shows these 2 threats have very high level impact for all cloud service models. Malicious insider also has average impact of more then 3 for all service models which indicates it importance for all service models.

TABLE 5.18: Severity level of threats for Cloud Service models (Indirectly discussed in literature)

Threat	**Service Model**		
	SaaS	Paas	IaaS
Data Breaches	V[4],H[61]	H[4],H[20],H[61]	L[4],H[61]
Data Loss	H[61]	H[21],H[61]	H[61]
Account or Service Traffic Hijacking	H[20],H[61]	H[4],H[20],H[61]	H[4],M[20],H[61]
Insecure Interfaces and API	V[22],V[31]	V[22],H[4],V[20],H[61]	V[22],H[4],V[20],H[61]
Denial of Service	V[22],H[18]	H[22],H[20]	H[22],H[20]
Malicious Insiders		V[4],V[20], H[61]	V[4],V[20],H[61]
Abuse of Cloud Services	L[26],M[5]	V[?],M[5],H[61]	V[4],M[5],H[61]
Insufficient Due Diligence		H[61]	H[61]
Code Injection	V[22],V[31]	H[22],H[20],V[31]	H[22],V[31]
Botnets	-	-	-
Targeted Attacks	-	-	-
Physical Theft/Loss/Damage	-	-	-
Hardware Failure	H[61]	H[61]	V[61]
Natural Disasters	H[61]	H[61]	V[61]
Cloud-related Malware	H[61]	H[61]	H[61]
Unknown Risk Profile	H[61]	,H[61]	,H[61]
LOCK-IN	M[59]	M[59]	M[59]
COMPLIANCE RISKS	M[59]	M[59]	M[59]

This table describes the references and what is the impact of threats for cloud service model. In this table there is just no of references, and level of impact like L for low, M for medium, H for high, V for very high.

The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low, if authors have discussed some how its severity then we took it as medium, if by authors point of view the threat have high impact we assigned H because it have high impact, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat.

We have included just those papers which have discussed the given threat with respect to cloud service models i.e. Software as a Service, Platform as a Service, Infrastructure as a Service. The references of threats which are by our understanding targeting the threats for cloud service model. Author doesn't have clear description about service model but by his disruption it can be understand that author is addressing these cloud service models.

TABLE 5.19: Average Severity level of threats for Cloud Service models (Indirectly discussed in literature)

	Service Model		
Threat	SaaS	Paas	IaaS
Data Breaches	3.5	3	2
Data Loss	3	3	3
Account or Service Traffic Hijacking	3	3	2.67
Insecure Interfaces and API	4	3.5	3.5
Denial of Service	3.5	3	3
Malicious Insiders		3.67	3.67
Abuse of Cloud Services	1.5	3	3
Insufficient Due Diligence		3	3
Code Injection	4	4	4
Botnets	-	-	-
Targeted Attacks	-	-	-
Physical Theft/Loss/Damage	-	-	-
Hardware Failure	3	3	4
Natural Disasters	3	3	4
Cloud-related Malware	3	3	3
Unknown Risk Profile	3	3	3
LOCK-IN	2	2	2
COMPLIANCE RISKS	-	-	-

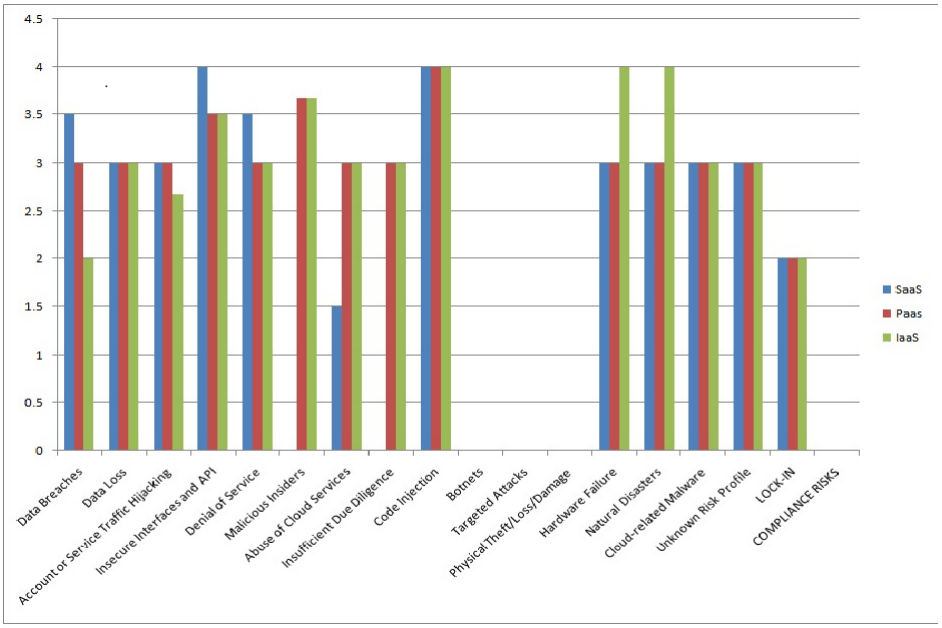


FIGURE 5.8: Average Severity level of threats for Cloud Service models (Indirectly discussed in literature)

This table describes the average impact of threats for cloud service models i.e. Software as a Service SaaS, Platform as a Service PaaS, Infrastructure as a Service IaaS. . In this table level of impact like L for low, M for medium, H for high, V for very high and values are assigned as 1 for low, 2 for medium, 3 for high, 4 for very high, 0 or no value is assigned if authors don't have discussed relevant threat.

The values are taken by detailed study of referred papers. If the authors just discussed that this threat can be effected on this deployment model we have assigned him low and value of low is 1, if authors have discussed some how its severity then we took it as medium and value of medium is 2, if by authors point of view the threat have high impact we assigned H because it have high impact value assigned for high is 3, if author have much focus on given threat and taking it as top threat then its given value is V because it very high level threat the assigned value is 4. The average is taken by adding all vales and dividing by no of referred papers.

We have included just those papers which have discussed the given threat with respect to cloud services. In this table we have just count of total references of threats for cloud deployment model. If we notice the pattern of this table we can see the most focus target of literature is SaaS which is Software as a Service.

If we observe these averages we will find these averages between 2 to 4. Data loss have average of 3 for all service model it means data loss is high level threat for all cloud service models. Account or service traffic hijacking has average value of 3 approximately which is also high level

threat for all service models. Insecure interfaces have average of 4 approximately which shows its very high level threat for all service models.

Composite View of Threats

Threat	Weakness	Service Model		Deployment model		Components	
		Model	Impact	Model	Impact	Model	Impact
Data Breaches	• Insecure configuration. • Access control weaknesses • Insecure storage. • Insecure configuration. • Data Validation. • Insufficient transport layer protection. • Authentication weaknesses. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Insufficient Vulnerability management. • Non comprehensive SLAs.	SaaS PaaS IaaS	Very High Very High High	Public Private Community Hybrid	Very High Very High High High	Application Data Platform Resource Abstraction Physical Infrastructure Facility	High Very High Medium Low Medium Medium
Data Loss	• Insecure configuration. • Access control weaknesses • Insecure storage. • Data Validation. • Insufficient transport layer protection. • Authentication weaknesses. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Insufficient Vulnerability management. • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures • Insufficient Risk assessment and data recovery.	SaaS PaaS IaaS	Very High Very High Very High	Public Private Community Hybrid	Very high High High High	Application Data Platform Resource Abstraction Physical Infrastructure Facility	High High Low Low Medium Medium
Account or Service Traffic Hijacking	• Insecure configuration. • Access control weaknesses •Insufficient Network and packet analysis. • Insecure configuration. • Insufficient Network and packet analysis. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. •Insufficient backdoor channel monitoring. • Failure to restrict URL access • Insufficient transport layer protection. • Invalidated redirect sand forwards. • Authentication weaknesses. • Insufficient network traffic monitoring and management.	SaaS PaaS IaaS	Very High Very High High	Public Private Community Hybrid	Very high High High High	Application Data Platform Resource Abstraction Physical Infrastructure Facility	High High Medium Low Low Medium

	• Insecure browser credentials. • Invalid service authenticatation and authorization. • Insufficient Vulnerability management. • Insecure service provisioning.						
Insecure Interfaces and API	• Insecure configuration. • Access control weaknesses • Insecure browser credentials. • Access control weaknesses. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. • Insecure backdoor channel. • Failure to restrict URL access • Invalidated redirect sand forwards. • Authentication weaknesses. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management.	SaaS PaaS IaaS	Very High Very High Very High	Public Private Community Hybrid	Very High Very High Very High Very High	Application Data Platform Resource Abstraction Physical Infrastructure Facility	High Very High Medium Very high Low Medium
Denial of Service	• Access control weaknesses • Session management weaknesses. • Insecure SSL trust configuration. • Insufficient Data Validation and verification. • Insufficient transport layer protection. • Invalidated redirect sand forwards. • Authentication weaknesses • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. • Invalidated redirect sand forwards. • Authentication weaknesses. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management. • Insecure service provisioning.	SaaS PaaS IaaS	Very High Very High Very High	Public Private Community Hybrid	Very High High High Very High	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Very High Very High High High Low Medium
Malicious Insiders	• Insecure storage Medium. • Insecure cryptographic storage • Authentication & Authorization weaknesses. • Invalid service management. • Invalidated services. • Insufficient Physical Security.	SaaS PaaS IaaS	Medium Very High Very High	Public Private Community Hybrid	Very High Very high Very High Very High	Application Data Platform Resource Abstraction Physical Infrastructure	Very high Very high Very High Medium Low

	• Physical access control management. • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures. • Access control weaknesses					Facility	Low
Abuse of Cloud Services	• Cross-site scripting [XSS]. • Access control weaknesses. • Insecure configuration. • Insufficient Network and packet analysis. • Session management weaknesses. • Data Validation. • Authentication weaknesses. • Insufficient network traffic monitoring and management. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management. • Insecure service provisioning. • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures.	SaaS PaaS IaaS	High High High	Public Private Community Hybrid	Very high Medium Medium Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Very High Medium Medium Low Medium Low
Insufficient Due Diligence	• Access control weaknesses. • Insecure communication channel between VMs. • Insufficient network traffic monitoring and management. • Invalid service authenticatation and authorization. • Insufficient Vulnerability management. • Insecure service provisioning. • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures. • Insufficient Risk assessment and data recovery.	SaaS PaaS IaaS	Medium High High	Public Private Community Hybrid	Very High Low Low Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Low Medium Low Medium Medium Low
Code Injection	• Access control weaknesses. • Insecure storage. • Insecure configuration. • Insufficient Network and packet analysis. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. • Invalidated redirect sand forwards. • Authentication weaknesses. • Insufficient VM Monitoring. • Insecure communication channel between VMs. • Insufficient network traffic monitoring and management. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management.	SaaS PaaS IaaS	Very High Very high Medium	Public Private Community Hybrid	Very High High High High	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Very High High Medium Medium - Medium

	• Insecure service provisioning.						
Botnets	• Access control weaknesses. • Insecure configuration. • Insufficient Network and packet analysis. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. • Insecure backdoor Channels. • Failure to restrict URL access • Authentication weaknesses. • Insufficient VM Monitoring. • Insecure communication channel between VMs. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Insufficient Vulnerability management. • Insecure service provisioning. • Non comprehensive SLAs.	SaaS PaaS IaaS	Medium	Public Private Community Hybrid	Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	
Targeted Attacks	• Access control weaknesses. • Hidden field manipulation • Insecure storage. • Insecure configuration. • Authentication & Authorization weaknesses. • Insufficient Network and packet analysis. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. •Insecure backdoor Channels. • Insecure cryptographic storage • Failure to restrict URL access. • Insufficient transport layer protection. • Invalidated redirect sand forwards. • Insufficient VM Monitoring. • Insecure communication channel between VMs. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management. • Insecure service provisioning. • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures.	SaaS PaaS IaaS		Public Private Community Hybrid		Application Data Platform Resource Abstraction Physical Infrastructure Facility	

	• Insufficient Risk assessment and data recovery.						
Physical Theft/Loss/Damage	• Authentication & Authorization weaknesses. • Insufficient comprehensive policies and procedures • Insufficient Risk assessment and data recovery. • Flaws in Facilities.	SaaS PaaS IaaS	Medium Medium			Application Data Platform Resource Abstraction Physical Infrastructure Facility	Medium Medium
Hardware Failure	• Authentication & Authorization weaknesses. • Insufficient comprehensive policies and procedures • Insufficient Risk assessment and data recovery. • Flaws in Facilities. • Natural disaster. • Inappropriate Hardware Configuration. • Unknown Reasons.	SaaS PaaS IaaS	Medium Medium Medium	Public Private Community Hybrid	Medium Medium Medium Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Low Medium Low Low High
Natural Disasters	• Insufficient comprehensive policies and procedures • Insufficient Risk assessment and data recovery. • Flaws in Facilities.	SaaS PaaS IaaS	Medium Medium Very high	Public Private Community Hybrid	Medium Medium Medium Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Low Medium Low Low Medium

Cloud-related Malware	• Access control weaknesses. • Insecure storage. • Insecure configuration. • Insufficient Network and packet analysis. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. • Use of backdoor. • Insecure cryptographic storage • Failure to restrict URL access • Insufficient transport layer protection. • Invalidated redirect sand forwards. • Authentication weaknesses. • Insufficient VM Monitoring. • Insecure communication channel between VMs. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management. • Insecure service provisioning.	SaaS PaaS IaaS	High High High	Public Private Community Hybrid	Medium Medium Medium Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Medium Medium Medium Medium Low Low
LOCK-IN	• Insecure storage. • Insecure configuration. • Insufficient Risk assessment and data recovery.	SaaS PaaS IaaS	Low Low Low	Public Private Community Hybrid	Medium Low Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	
COMPLIANCE RISKS	• Insecure cryptographic storage • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures. • Insufficient Risk assessment and data recovery.	SaaS PaaS IaaS		Public Private Community Hybrid	Medium Medium Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Medium

Unknown Risk Profile	• Access control weaknesses. • Cookie manipulation. • Hidden field manipulation • Insecure storage. • Insecure configuration. • Insufficient Network and packet analysis. • Session management weaknesses. • Insecure SSL trust configuration. • Data Validation. • Use of backdoor. • Insecure cryptographic storage • Failure to restrict URL access • Insufficient transport layer protection. • Unvalidated redirect sand forwards. • Authentication weaknesses. • Insufficient VM Monitoring. • Insecure communication channel between VMs. • Insufficient network traffic monitoring and management. • Insufficient data traffic authentication. • Insecure browser credentials. • Invalid service authenticatation and authorization. • Invalidated services. • Insufficient Vulnerability management. • Insecure service provisioning. • Non comprehensive SLAs. • Insufficient comprehensive policies and procedures. • Insufficient Risk assessment and data recovery.	SaaS PaaS IaaS	Medium Medium Medium	Public Private Community Hybrid	Medium Medium Medium Medium	Application Data Platform Resource Abstraction Physical Infrastructure Facility	Low Low Medium Low Low Low

This table describes the over all picture of threats, for Cloud service models, cloud deployment models, cloud components. We also have identified the basic weaknesses in system which causes the relevant threat. This table is outcome of all previous work. We took aggregate average of severity level of threat for cloud components, cloud service model, cloud deployment model by adding average of clearly discussed and indirectly discussed and divided the sum of averages by 2.

Our assigned severity level is 0-4. 0 for very low impact. If aggregated average lies 0.1 to 1.0 we assigned it Low. If aggregated value is 1.1 to 2.0 then severity level is medium. If aggregated average is 2.1 to 3.0 it shows High level of severity. Value 3.1 - 4.0 represents Very high level impact.

If we observe one by one threat for service model, deployment model, components and notice the weaknesses in the system. We can see the threat Data breaches have causes due to the Insecure configuration, Access control weaknesses, Insecure storage., Insecure configuration, Data Validation, Insufficient transport layer protection, Authentication weaknesses, Insufficient network traffic monitoring and management, Insufficient data traffic authentication, Insecure browser credentials, Invalid service authenticatation and authorization, Insufficient Vulnerability management and Non comprehensive SLAs. Data Breach is very high level threat for SaaS , PaaS and high level threat for IaaS cloud service model. For cloud deployment model its very high for both public and private and high for community and hybrid. For cloud components its very high for data, high for application and medium for platform, physical infrastructure and facility.

If we observe this table we can see different trends of severity for different cloud service models , cloud deployment model and cloud components. Data breaches have severity level "very high" for SaaS and PaaS cloud service model, and "high" for IaaS . For cloud deployment model in private and public data breaches have very high severity level because the target of unauthorized attempt is ultimately data. Among all components data is critical with respect to data breaches. It causes due to following reported weaknesses like , Insecure configuration, Access control weaknesses , Insecure storage, Insecure configuration, Data Validation, Insufficient transport layer protection, Authentication weaknesses, Insufficient network traffic monitoring and management, Insufficient data traffic authentication, Insecure browser credentials, Invalid service authenticatation and authorization, Insufficient Vulnerability management, Non comprehensive SLAs.

If we observe data loss also have weaknesses like , Insecure configuration, Access control weaknesses , Insecure storage, Insecure configuration, Data Validation, Insufficient transport layer protection, Authentication weaknesses, Insufficient network traffic monitoring and management, Insufficient data traffic authentication, Insecure browser credentials, Invalid

service authenticatation and authorization, Insufficient Vulnerability management, Non comprehensive SLAs and it has very high severity level for all cloud service models and for public cloud deployment model because in public cloud mostly customers donot have information about storage location etc. at application and data its high for cloud components.

Account or service traffic hijacking have severity level "very high " for SaaS, PaaS cloud service model and public cloud deployment model due to weaknesses like Insecure configuration, Access control weaknesses, Insufficient Network and packet analysis, Insecure configuration, Insufficient Network and packet analysis, Session management weaknesses, Insecure SSL trust configuration, Data Validation, Insufficient backdoor channel monitoring, Failure to restrict URL access, Insufficient transport layer protection, Invalidated redirect sand forwards, Authentication weaknesses, Insufficient network traffic monitoring and management.

Due to web based services interfaces and API are very critical for all service models, deployment models due to following weaknesses like Insecure configuration, Access control weaknesses ,Insecure browser credentials ,Access control weaknesses,Session management weaknesses,Insecure SSL trust configuration, Data Validation, Insecure backdoor channel, Failure to restrict URL access, Invalidated redirect sand forwards, Authentication weaknesses,Insufficient network traffic monitoring and management, Insufficient data traffic authentication, Insecure browser credentials, Invalid service authenticatation and authorization, Invalidated services,Insufficient Vulnerability management.

Denial of service and distributed denial of services is very common threat for cloud computing . It has very high severity level for all cloud service models and public and hybrid cloud deployment model. It causes due to following weaknesses i.e Access control weaknesses,Session management weaknesses,Insecure SSL trust configuration, Data Validation, insufficient transport layer protection, invalidated redirects and forwards, Insecure backdoor channel, Failure to restrict URL access, Invalidated redirect sand forwards, Authentication weaknesses,Insufficient network traffic monitoring and management, Insufficient data traffic authentication, Insecure browser credentials, Invalid service authenticatation and authorization, Invalidated services,Insufficient Vulnerability management.

Malicious insiders is very high level threat for all cloud deployment model and IaaS and PaaS cloud service model due to following weaknesses in system . Access control weaknesses, Insecure storage Medium, Insecure cryptographic storage ,Authentication and Authorization weaknesses, Invalid service management ,Invalidated services, Insufficient Physical Security, Physical access control management, Non comprehensive SLAs, Insufficient comprehensive policies and procedures.

In cloud computing abuse of cloud services is high level threat for all cloud service model because services are available for both good and bad users. Bad users have access of very high compute power at very low cost. For public cloud its very high level threat. Insufficient due diligence is also a common and high level threat for Platform as a Service and Infrastructure as a Service because mostly user adopts cloud service model without complete study and compatibility of providers services.

Code injections is also a very high level threat at application level and for public cloud and high level threat for all other cloud deployment models becauses users are connected with web interfaces and fetching data from services via queries.

we can easily conclude that in cloud deployment model Public cloud have much severe level threats then other cloud deployment models. PaaS and IaaS have much threats then SaaS. in components applications have much threats then other cloud components.

Chapter 6

Conclusion and Future Work

Cloud computing has become a widespread choice for the enterprises and individuals to fulfill their computing requirements. It offers variety of service types over the internet and enables its customer to have on demand, scalable resources available round the Clock.Despite its many great advantages, a cloud computing environment possesses many security threats and trust related issues due to its shared (generally) nature.

Cloud computing faces similar threats as traditional computing. Contingent upon the administration and sending model embraced, tending to security hazards in the cloud may turn into an additionally difficult and complex undertaking. This circumstance subsequently speaks to the cloud suppliers the need to execute their key obligations of making a savvy as well as a protected distributed computing administration. Security is crucial for critical cloud computing services – one flaw can impact a wide range of organizations directly. From a logical perspective the cloud computing service is a single point of failure. .

In this study, we identify threats and security attributes applicable in cloud computing. We also identified the financial impact and reported incidents due to relevant threat and find out the weaknesses of system.

Cloud security is very serious concern for both cloud provider and cloud consumers. 1st both parties have to know potential security threats and the level of danger of that threat. If cloud consumer and cloud provider both are aware from threats then both have to know causes of that threats then threats can be mitigated.

we have identified threats and severity level of threat and mapped of threat with respect to cloud service model , cloud deployment model, cloud computing components. in future we will verify this severity level from industry . after verifying our indentified threats from industry

we will do a detail analysis of each threat to identify causes of threat and mitigation techniques and then we will propose security guidelines for cloud computing service model, cloud computing deployment model, cloud computing components. we will implement these guidelines in industry and propose some solid framework .

Bibliography

[1] C Alliance. Security guidance for critical areas of focus in cloud computing v3. 0. *Cloud Security Alliance*, 2011.

[2] Dr. M.A.C. Dekker. Critical cloud computing, a ciip perspective on cloud computing services version 1,0, december 2012. Technical report, ENISA, 2012.

[3] Subashini Subashini and V Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11, 2011.

[4] Dimiter Velev and Plamena Zlateva. Cloud infrastructure security. In *Open Research Problems in Network Security*, pages 140–148. Springer, 2011.

[5] Carlo Marcelo Revoredo da Silva, Jose Lutiano Costa da Silva, Ricardo Batista Rodrigues, Leandro Marques do Nascimento, and Vinicius Cardoso Garcia. Systematic mapping study on security threats in cloud computing. *arXiv preprint arXiv:1303.6782*, 2013.

[6] S Ramgovind, Mariki M Eloff, and E Smith. The management of security in cloud computing. In *Information Security for South Africa (ISSA), 2010*, pages 1–7. IEEE, 2010.

[7] Hanqian Wu, Yi Ding, Chuck Winer, and Li Yao. Network security for virtual machine in cloud computing. In *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, pages 18–21. IEEE, 2010.

[8] Ling Qian, Zhiguo Luo, Yujian Du, and Leitao Guo. Cloud computing: An overview. In *Cloud computing*, pages 626–631. Springer, 2009.

[9] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592, 2012.

[10] Ankur Mishra, Ruchita Mathur, Shishir Jain, and Jitendra Singh Rathore. Cloud computing security. *International Journal on Recent and Innovation Trends in Computing and Communication*, 1(1):36–39, 2013.

[11] Jyotiprakash Sahoo, Subasish Mohapatra, and Radha Lath. Virtualization: A survey on concepts, taxonomy and associated security issues. In *Computer and Network Technology (ICCNT), 2010 Second International Conference on*, pages 222–226. IEEE, 2010.

[12] Peter Mell and Tim Grance. The nist definition of cloud computing, special publication 800-145. 2011.

[13] Hae-Gill Choi and Sung-Ho Sim. Advanced security framework model for cloud computing environment. *Life Science Journal*, 11(7s), 2014.

[14] Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan, and Andrew Bernoth. A layered security approach for cloud computing infrastructure. In *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, pages 763–767. IEEE, 2009.

[15] Kandukuri Balachandra Reddy, Paturi V Ramakrishna, and Dr Rakshit Atanu. Cloud security issues. In *IEEE International Conference on Services Computing*, 2009.

[16] Mohamed Almorsy, John Grundy, and Ingo Müller. An analysis of the cloud computing security problem. In *Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov*, 2010.

[17] Hassan Takabi, James BD Joshi, and Gail-Joon Ahn. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6):24–31, 2010.

[18] Klaus Julisch and Michael Hall. Security and control in the cloud. *Information Security Journal: A Global Perspective*, 19(6):299–309, 2010.

[19] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, and Sugata Sanyal. A survey on security issues in cloud computing. *arXiv preprint arXiv:1109.5388*, 2011.

[20] Akhil Behl. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In *Information and Communication Technologies (WICT), 2011 World Congress on*, pages 217–222. IEEE, 2011.

[21] Shirlei Chaves, Carlos Westphall, Carla Westphall, and Guilherme Geronimo. Customer security concerns in cloud computing. In *ICN 2011, The Tenth International Conference on Networks*, pages 7–11, 2011.

[22] Danish Jamil and Hassan Zaki. Security issues in cloud computing and countermeasures. *International Journal of Engineering Science and Technology (IJEST)*, 3(4):2672–2676, 2011.

[23] David Teneyuca. Internet cloud security: The illusion of inclusion. *Information Security Technical Report*, 16(3):102–107, 2011.

[24] Dr Giles Hogben Dr Marnix Dekker. Survey and analysis of security parameters in cloud slas across the european public sector. Technical report, ENISA, 2011.

[25] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, and Dawn Leaf. Nist cloud computing reference architecture , special publication 500-292. *NIST special publication*, 500:292, 2011.

[26] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. A survey on security issues and solutions at different layers of cloud computing. *The Journal of Supercomputing [Springer]*, 63(2):561–592, 2012.

[27] Ms Disha H Parekh and R Sridaran. An analysis of security challenges in cloud computing. *IJACSA) International Journal of Advanced Computer Science and Applications*, 4(1), 2013.

[28] Top Threats Working Group et al. The notorious nine: cloud computing top threats in 2013. *Cloud Security Alliance*, 2013.

[29] SSGL Ryan Ko and S Lee. Cloud computing vulnerability incidents: A statistical overview. *CSA (Cloud Security Alliance)*, 2013.

[30] Louis Marinos. Enisa threat landscape 2013 overview of current and emerging cyber-threats 11 december 2013. Technical report, ENISA, 2013.

[31] Dave Wichers. Owasp top-10 2013. 2014.

[32] Richard Kissel. *Glossary of Key Information Security Terms*. NIST, rivision2 edition, May 2013.

[33] R. Shirey. Internet security glossary, version 2, 2007. URL https://tools.ietf.org/html/rfc4949.

[34] Ciske van Oosten. Verizon 2014 pci compliance report. Technical report, 201.

[35] Online Trust Alliance. 2014 data protection & breach readiness guide. Technical report, Online Trust Alliance, 2014.

[36] Ponemon. 2013 cost of data breach study: Global analysis. Technical report, Ponemon, 2013.

[37] Cnn report of date breach. URL http://money.cnn.com/2014/09/18/technology/security/home-depot-hack/.

[38] anthom data breach report. URL http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/.

[39] KPMG. Data loss barometer a global insight into lost and stolen information. Technical report, KPMG, 2014.

[40] Huawei. 2013 botnets and ddos attacks report. Technical report, HUAWEI, 2013.

[41] Ponemon. Second annual cost of cyber crime study benchmark study of u.s. companies. Technical report, Ponemon, 2011.

[42] Neustar. When businesses go dark. Technical report, Neustar, 2012.

[43] Felix Leder Daniel Plohmann, Elmar Gerhards-Padilla. Botnets: Detecdete, measureme, discuss. Technical report, ENISA, 2011.

[44] David McIntire Andrew P. Moore Randall Trzeciak Adam Cummings, Todd Lewellen. Insider threat study: Illicit cyber activity involving fraud in the u.s. financial services sector. Technical report, Carnegie Mellon University., 2012.

[45] URL http://www.suretyit.com.au.

[46] CSCC. Security for cloud computing. Technical report, Cloud standdards Customer council, 2012.

[47] URL http://social.technet.microsoft.com/wiki/contents/articles/3800.compliance-issues-in-the-cloud.aspx.

[48] SANS. Cloud security and compliance. Technical report, SANS, 2010.

[49] URL http://www.technologydecisions.com.au/content/cloud-and-virtualisation/article/compliance-issues-lead-cloud-security-concerns-10167711

[50] Kashi Venkatesh Vishwanath and Nachiappan Nagappan. Characterizing cloud computing hardware reliability. *ACM*, 2010.

[51] URL http://www.govplace.com/2013/07/government-cloud-and-natural-disasters/.

[52]

[53] URL http://www.thewhir.com/web-hosting-news/malware-distributors-using-major-us-cloud-co

[54] CISCO. Cisco 2014 annual security report. Technical report, CISCO cloud, 2014.

[55] URL http://www.theregister.co.uk/2014/01/16/amazon_cloud_security_nightmare/.

[56] URL http://www.forbes.com/sites/joemckendrick/2011/11/20/cloud-computings-vendor-lock-in-problem-why-the-industry-is-taking-a-step-backwards/.

[57] URL http://www.linuxinsider.com/story/79417.html.

[58] URL http://www.itsmportal.com/columns/vendor-lock-and-cloud-computing#.VVi9HZMlkr4.

[59] Daniele Catteddu. Cloud computing: benefits, risks and recommendations for information security. In *Web Application Security*, pages 17–17. Springer, 2010.

[60] Harshal Mahajan and Nupur Giri. Threats to cloud computing security. In *VESIT, International Technological Conference-2014 (I-TechCON)*, 2014.

[61] Cloud Vulnerabilities Working Group CSA. Cloud computing vulnerability incidents: A statistical overview. 2013.

[62] Farzad Sabahi. Virtualization-level security in cloud computing. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pages 250–254. IEEE, 2011.

[63] Chunming Rong, Son T Nguyen, and Martin Gilje Jaatun. Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, 39(1):47–54, 2012.