**CHAPTER 2**

**LITERATURE REVIEW**

**2.1 Survey on Cloud Computing**

Cloud computing, undoubtedly, has become the buzzword in the IT industry today. Looking at the potential impact, it has on numerous business applications as well as in everyday life, it can certainly be said that this disruptive technology and it is going to stay. Many of the features that make cloud computing attractive, have not just challenged the existing security system, but have also revealed new security issues. This author (Buyya et al. 2011) provides an insightful analysis of the existing status on cloud computing security issues based on a detailed survey carried by him and also makes an attempt to describe the security challenges in Software as a Service (SaaS) model of cloud computing and also endeavors to provide future security research directions. Cloud computing is becoming an increasingly popular enterprise model in which computing resources are made available on-demand to the user as needed. Fan et al. (2009) presents the unique value proposition of cloud computing creates new opportunities to align IT and business goals and it uses the internet technologies for delivery of IT enabled capabilities ‘as a service’ to any needed users, i.e. through cloud computing, end user can access anything that they want from anywhere to any computer without worrying about anything like about their storage, cost, management and so on. The author provides a comprehensive study on the motivation factors of adopting cloud computing and its several type of cloud deployment and

service models. Also, explores certain benefits of cloud computing over traditional IT service environment which includes scalability, flexibility,

reduced capital and higher resource utilization. These are considered as

adoption reasons for cloud computing environment and also cover security,

privacy, internet dependency and availability as avoidance issues. Later, the

author includes vertical scalability as a technical challenge in the cloud

environment.

Armbrust et al. (2004) presents a style of computing where scalable

and elastic IT related capabilities are provided as shared assorted services like

IaaS, PaaS, SaaS and DaaS which are metered by usage and the customer

builds on top of diverse technologies like virtualization, distributed

computing, utility computing and more recently networking, web

infrastructure and software services by using internet technologies. The

author represents a paradigm shift in how the enterprise think about their data,

the role of the computing devices and on managing the computing resources.

Being an emerging service technology with promising novel and valuable

capabilities, it attracts industrial research community with main focus onstandardization and customized implementation in every segment of society.

Cloud powered higher education institutions also gain significant flexibility

and agility. Also, the authors (Armbrust et al. 2010 and Zissis et al. 2012)

examine and discuss the concept of cloud computing from the perspectives of

diverse technologists, services and models available, cloud standards, cloud in

government, enterprises and higher education, along with opportunities,

challenges and future implications.

Cloud computing and how to bridge the gap between various

providers is getting increasing attention. In this context, Zhang et al. (2010)

gives an idea for efficient task scheduling on heterogeneous resources is of

extreme importance. The state-of-the-art for this field has been continuously

growing during the last years and has reached a point in which a comprehensive overview indicating current solutions and ongoing challenges

is of extreme importance for researchers. The author aims to offer this

analysis from a client-side scheduling perspective in which emphasis is not

put on physical resource selection, but on task to virtual machine mappings

and virtual machine allocation. Also, Ahmed et al. (2012) provides taxonomy

for the current state-of-the-art and a unified model concerning the various

metrics and goals used throughout literature and this model is designed to be

sufficiently generic, extensible and comprehensive to support most of the

future work in the field which provides promising research directions and

existing challenges.

In Buyya et al. (2008) and Doleys et al. (2011) research process in

the cloud computing field, they explain many computing models such as

parallel computing, distributed computing, and grid computing. Many normal

distributed computers collaborate of achieve a function like a super computer.

The computation will be assigned to this super computer rather than local

computer or remote server and it is the basic concept of cloud computing.

However, there is a new implementation of cloud computing which introduces the concept of super cloud (Casalicchio et al. 2011), based on the

millions of computers connected by using internet. Cloud computing has

several advantages such as the user does not need to worry about how the

cloud runs, viruses, maintenance and also expects that it is going to reshape

the IT industry. Also, discusses cloud computing from different angles such

as concept, characteristics and classifications of cloud computing.

The system model is in a multi-cloud environment which is defined

as the network of clouds that may interoperate to serve their individual user

bases in each local intra cloud (Celesti et al. 2012) and the inter (Local) cloud

may share services among other clouds in order to load balance or meet peak

demands. Using this model, the author proposes an effective proportional andintegral feedback control scheme based on control theory to share limited

resources to satisfy the requirements of multiple users wanting fast response

and/or high utilization of cloud resources. The control scheme is based on a

self-tuning feedback theory which considers not only the actual versus target

value of resource utilization, also the history of application computing rates.

After that, it shows about the theoretical analysis of the system stability and

its guideline for selection of feedback control parameters to stabilize the

resource utilization at a desirable target level. The author performs a

simulation that has been conducted to demonstrate the proposed scheme and it

can be an effective multi-cloud computing controller for ensuring fast

response and high resource utilization.

As per Marshall et al. (2010) research study, the infrastructure as a

service (IaaS) cloud offers capabilities for the high availability of a wide

range of systems, from individual virtual machines to large-scale high

performance computing (HPC) systems. But it is argued that the widespread

uptake for such systems will only happen if cloud providers or brokers areable to offer bilateral service level agreements. Fito et al. (2010) and Dillon

et al. (2010) show that how to measure and use quality of service (QoS)

information to be able to predict availability, quantify risk, and consider

liability in case of failure and they demonstrate through the research work that

there is a pressing need for such an understanding and explore a set of

benchmarks that offers an interesting characterization of resource

performance variability which can be quite significant. They also

subsequently identify that how such information might be used both directly

by a user and indirectly via a cloud broker in the automatic construction and

management of SLAs which reference certain kinds of financial portfolios.

With inter-cloud, the distributed cloud and open cloud exchange

(OCX) are emerging. A comprehensive resource allocation (Lloyd et al. 2013) approach is fundamental to highly competitive cloud market and an intelligent

economic approach for dynamic resource allocation is proposed with the

improved combination of double auction protocol devised to enable various

kinds of resources traded among multiple consumers and multiple providers at

the same time enable task partitioning among multiple providers. A price

formation mechanism is proposed to make the bidding and asking reasonable

auction and determine eligible transaction relationship among providers and

consumers which consists the back propagation neural network (BPNN)

based price prediction algorithm and a price matching algorithm. Also, a

reputation system is proposed and integrated to exclude dishonest participants

from the cloud market. The winner determination problem (WDP) is solved

by the improved paddy field algorithm (PFA) and the simulation results have

shown. It is not only to help to maximize market surplus strength but also to

encourage participants to be honest.

**2.2 Survey on Server Hardening**

Cloud computing is current buzzword in the market and it is

paradigm in which the resources can be leveraged on per usage basis thus

reducing the cost and complexity of service providers. Cloud computing

promises to cut down the operational and capital cost which is more

importantly, let the IT departments focus on strategic projects instead of

keeping data centers running. Tirthani et al. (2014) and Tripathi et al. (2011)

explain that it is much more than simple internet. They give the idea of

security architecture construct that allows user to access applications that

actually reside at location other than user’s own computer or other Internetconnected

devices. For instance, other company host user application. This

implies that they handle the cost of servers, they manage software updates and

depending on the contract user pays less i.e. for the service only.

Confidentiality, integrity, availability, authenticity, and privacy are the essential concerns for both cloud providers and consumers as well.

Infrastructure as a Service (IaaS) serves as the foundation layer for the other

delivery models, and a lack of security in this layer will certainly affect the

other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. It

also elaborates study of IaaS components’ security and determines

vulnerabilities (Chen et al. 2012), counter measures and service level

agreement (SLA).

The major focus is on practical securing Linux production systems

and Rewagad et al. (2013) discusses basic Linux security requirements for

systems that need to pass various audits in an enterprise environment. It also

presents the direction to detect the vulnerabilities in the system by scanning

configuration files and server files. Also, to determine the computer activities

by scanning the log files thereby securing the system by replacing the

vulnerable attributes with secured attributes. Application security is ensured

by scrutinizing the signatures of various applications and displaying all the

functionalities in GUI format that makes more user friendly. A very important step in securing a Linux system is to determine the primary

function or role of the Linux server. In general, end user has difficult time to

understand what needs to be secured and hence securing the Linux system

proactively won’t be that effective. Therefore it is very critical to look at the

default list of software packages that don’t comply with the security policy.

Information is in and around the globe and has so much to be

linked up with the cyber infrastructure. This sophisticated infrastructure is

said to be secure to some extent, perhaps the vulnerabilities always exists and

paves a way for catastrophes. The security concern for the same has grown in

recent times of internet age which led to a concept known as “Cyber

Security”. The cyber security is one of the major aspects of research in the

information security domain (Sulochana et al. 2013 and Sultan et al. 2013). The author provides all the required security policies with ample algorithms

in order to with stand attacks on the cyber infrastructure in various

enterprises. As most of the enterprises depend on the information analytical

processing for decision making, the storage areas viz., servers became the

central entities of protection. This concept of server security emerged in

order to safe guard the security assets in the storage environments with

respect to the security fundamentals the information integrity, confidentiality

and availability; is called “Server Hardening”.

The vulnerability of Cloud Computing Systems (CCSs) to

Advanced Persistent Threats (APTs) is a significant concern to government

and industry. Subashini et al. (2011) presents a cloud architecture (Cloud

Enterprise Architecture, 2012) reference model that incorporates a wide range

of security controls and best practices, and a cloud security assessment model

– Cloud Trust - that estimates high level security metrics to quantify the

degree of confidentiality and integrity offered by a CCS or cloud service

provider (CSP). The Cloud-Trust is used to assess the security level of four multi-tenant IaaS cloud architectures equipped with alternative cloud security

controls and to show the probability of CCS penetration (high value data

compromise) is high if a minimal set of security controls are implemented.

The CCS penetration probability drops substantially if a cloud defense in

depth security architecture is adopted that protects virtual machine (VM)

images at rest, strengthens CSP and cloud tenant system administrator access

controls and which employs other network security controls to minimize

cloud network surveillance and discovery of live VMs.

Security concern (Chen et al. 2010) has given a rise to emerge an

active area of research due to the many security threats that many enterprises

have faced at present. The author is addressing these issues that require

getting the confidence from user for cloud applications and services. It has cast light over the major security threats of cloud computing systems while

introducing the most suitable countermeasures for them. The author is also

cited the aspect to be focused on when talking about cloud security and

categorized these threats according to different viewpoints, providing a useful

and little-known list of threats and also some effective countermeasures are

listed.

**2.3 Survey on Private Cloud Computing**

Cloud computing is a major change, caused by the underlying

commoditization of IT. It is expected to see a future dominance of the open

source model in cloud computing which will solve the major adoption

concerns for users. Even a small private cloud built as intranet that gives an

idea of the dominance of cloud computing in near future. The scope of the

cloud built in is scalable; allocate more capacity only when it needed as

dynamic instance creation and termination (Koh et al. 2007) upon receiving a

request. Cloud computing services-A comparison has recognized as one of

the top 10 technologies of 2010 by Gartner and Yim et al. (2009) provides a

report that the cloud computing has generated a lot of interest and competition

in the industry. With the emergence of new cloud providers, identifying one

that best suits the business needs of an enterprise is a challenging and difficult

task. Adopting a cloud provider requires a detailed study of parameters like

data security, SLA's and options that address the reduction of capital

expenditure. The author published an article that carries out a high level

comparison of the significant features delivered by key public cloud providers

of the industry and key considerations that enterprises need to take into

account while they embark on cloud computing like setting up of private

cloud to provide IaaS (Providing an Operating System to the user) And SaaS

services (Michael Kuperberg et al. 2011).

Cloud Computing allows the user to access the cloud services

dynamically over the internet wherever and whenever needed. Cloud is

majorly divided into two types; private cloud and public cloud. Ken et al.

(2011) publishes an article to discuss about implementing a private cloud

using open source software and operating system. The private cloud is

capable of providing the infrastructure and platform as a service.

Infrastructure includes the storage, servers, virtualization, compute and

network services and platform as a service includes the operating system,

middleware and runtime environment (Geelan et al. 2009). The author

experiments the research to implement the private cloud using OpenStack and

Ubuntu.

Cloud computing security (sometimes referred to simply as "cloud

security") is an evolving sub-domain of computer security, network security,

and more broadly information security (Rong et al. 2013). It refers to a broad

set of policies, technologies and controls deployed to protect data,

applications and the associated infrastructure of cloud computing. Private

Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing

processing power to match elastic demand and supply (Gong et al. 2010),

whilst reducing capital expenditure.

However, the successful implementation of cloud computing is to

effectively manage the security in the cloud applications which gives benefit

in term of cost. Security consciousness and concerns arise as soon as one

begins to run applications beyond the designated firewall and move closer

towards the public domain. The purpose of the research is to provide an

overall security perspective (Kalpana et al. 2012) of cloud computing with the

aim to highlight the security concerns that should be properly addressed and

managed to realize the full potential of cloud computing. Also, Gartner list on cloud security issues, as well the findings from the International Data

Corporation enterprise panel survey based on cloud threats.

Cloud computing is an increasingly popular paradigm for accessing

computing resources. In practice, cloud service providers tend to offer

services that can be grouped into three categories: software as a service

(Salesforce, 2010), platform as a service, and infrastructure as a service. York

et al. (2008) discuss the characteristics and benefits of private cloud

computing as well as implementation. It also outlines the responsibilities of

private cloud provider and the facilities to consumer.

In traditional computing, end user install software programs on

system update the hardware as per the requirements and documents are

created or stored in the computer which can be accessible on their own

network, but they cannot be able to access outside of their network. Using of

cloud computing, the software programs aren’t running from one’s personal

computer, but are rather stored on servers accessed via the Internet. Cloud computing provides resources and capabilities of Information Technology

(e.g., applications, storages, communication, collaboration, infrastructure) via

services offered by cloud service provider. Cloud computing has various

characteristics (Jadeja Yashpal et al. 2012) as shared infrastructure, selfservice,

pay-per use model, dynamic and virtualized, elastic and scalable.