Smart Computing Review

Cloud Computing Security Models, Architectures, Issues and Challenges: A Survey

Muhammad Alyas Shahid* **and Muhammad Sharif**

COMSATS Institute of Information Technology, Wah Cantt. Pakistan / mashahid79@gmail.com, muhammadsharifmalik@yahoo.com

*Corresponding Author: Muhammad *Alyas Shahid*

Received October 23, 2015; Revised November 29, 2015; Accepted December 25, 2015; Published December 31, 2015

Abstract: Cloud computing a new recently emerged environment for the hosting and delivery of IT services over a network typically includes on-demand, reliable, customized, self service computing environment guarantees dynamic access and quality of service for end users. This computing paradigm introduces many changes with flexible and dynamically scalable pools of often virtualized resources. With these multitudinous benefits and characteristics, a cloud system can prospectively perk up information technology and encourage business to work on, and invest in new alternate computing system. It offers a quick start, flexibility, scalability and cost-effectiveness for hosting and expanding resources but new threats and opportunities for exploitation are introduced requiring essential values and control policies to guide the protection and safety of systems and data. The cloud computing environment also provides opportunities to share resources, information and services among the peoples of the world. With all the advantages of cloud computing, there are a few limitations with respect to data security and quality of service, because this environment brings new security issues, challenges and threats. Management must understand and analyze the risks of this new and emerging paradigm of cloud in order to protect and secure the system, resources and data from exploitation. This paper focuses on cloud computing Security Models, Security Architecture, risks, issues, threats and challenges of security to any cloud computing environment.

Keywords: Cloud Computing Environment, WSDL, Virtualization, Hypervisor, Virtual Machines

DOI: 10.6029/smartcr.2015.06.010

Introduction

In the 1990s, the renting of memory, power and cooling and the increasing expenses of operating operations led to the espousal of cloud computing through virtualization. Though grid and cloud computing, users can connect and utilize measured utilities. Enabling infrastructure for the virtualized and mutual use by all consumers or clients, service providers and users must change the business model to provide tenuously arranged services with cost reductions. As services become more and more dispersed, the need for assimilation and administration of these services has become essential. This has led to the service oriented architecture (SOA) which has evolved to provide information technology resources "as a service".

Like any other technology many issues raised in cloud computing, such as security, control and management, disaster recovery and business stability, supply management, policies and legislation, as well as a lack of standards and strategy. To reduce the impact of these threats and problems, risk reduction is essential if organizations are interested in accessing many of the clouds services, and in protecting memory, systems and data.

Section I of this article focuses on an introduction to the cloud computing environment. Section II provides the general idea of cloud computing and in Section III security models of the cloud environment are determined. The security architectures of a cloud computing is discussed in Section IV, with the issues, threats, challenges and risks of cloud computing security described in Section V. The conclusion and future studies follow in Section VI.

100-Mile Overview

There are many definitions of cloud computing such as: "large-scale distributed computing paradigm, that includes in economies of scale, in which a pool of abstract virtual, dynamically scalable, manageable computing power, storage, platforms and services provided at the request of external clients via the Internet." [1]

Another definition provided by the National Institute of Standards and Technology (NIST) [2] for the cloud computing environment in which all major aspects of cloud computing environment are covered. So cloud computing is a model for enabling, convenient, ubiquitous access to the network card to a shared pool of configurable computing resources (eg, networks, servers, storage, applications and services)that can be rapidly provisioned and released with minimal management effort or service provider interaction[100].

The cloud computing environment may be defined as, a paradigm of services with support to provide scalable and quality of service QoS[3] and guaranteed, as a rule, personalized and affordable computing infrastructure on demand in a simple and common way [4-5].

Another definition of cloud computing is the management and provision of resources, software, applications and information services via the cloud (the internet) on demand. The cloud computing environment model is used to access computing resources as a shared pool, which can be quickly managed and released with negligible effort by management or interaction with a service provider. On the Internet to avoid a large, direct and fixed cost, there is an ability to provide dynamically scalable [6] and shared resources. Cloud computing has appeared as a recent and new and encouraging hosting environment, in which the collected services (information, applications, and infrastructure comprising computers, information, networking, and memory storage resources) are intelligently used.

As a special example of distributed computing, cloud computing is scalable resources (eg, servers, networks, applications, storage, and services), and is a cost-effective, flexible and dynamically adjusted environment. Moreover it can work simultaneously on request [7], with an elastic, shared pool of resources, and dynamic resource planning for general purpose [8]. These are encapsulated as an intangible entity that provides different services levels to clients through the cloud. These services can be delivered on demand and services can be dynamically allocated and configured by using virtualization or many other approaches) [9].Infrastructure providers manage cloud platforms and resources, rent those services and rent other resources from one or more other service providers of infrastructure services for end-users. They solve resources, storage and computing problems associated with four main factors 1) the needs for computing power and storage capacity increases and hardware cost reduction; 2) the advent of hundreds or thousands of multi-core architectures and of modern supercomputers; 3) the exponential growth of scientific data; and 4) the acceptance of extensive computing services, resources and applications for Web 2.0.

This new method of delivering computing services, resources, applications and new technology, is based on the model for providing Internet services, which provides computing, storage and Internet-conferences, for all users in all markets, including the financial users, health care and government[10].This new cost-effective environment has found lush ground and attracts significant international investment. Cloud computing is a new field of high availability is most economical, offers good performance, and many others features. In addition, almost all companies find it mandatory to start their

businesses with cloud computing providers, because of the fear of data loss. Due to the minimal availability of suitable management policies and security guarantees weaknesses, however, this leads to great vulnerability in that environment [11].

Vulnerability is a major factor and one of the buzz words in the world of computers these days. This includes sharing resources, which includes software, applications and infrastructure platforms. This environment aims to be a self-motivated, consistent and customizable with guaranteed quality of service. Cloud computing seems to be everywhere, eminently scalable and on-demand, which can be purchased on a "pay-as-you-go" basis, without making reservations or needing a pre-subscription [2]. This often takes the form of online and web-based applications and tools. It means users can access these tools by using any web browser, which is installed locally on their own computers. In a cloud computing the included software, applications and tools are (software-as-a-service, SaaS), hardware or infrastructure as a service (IaaS), and technology tools (platform-as-a-service or PaaS) [12]. All are available on demand; as licensed software and tools from any hardware provider. In most cases for the tip term of service and requirements for quality of service with cloud computing, there is a service level agreement (SLA) between the consumer and the service provider [13].It is based on pay-per-use model as convenient on-demand and as required access control to the common resources. They are easily configurable and can be easily released and produced with minimal effort or interaction and by service providers. Under these conditions, a number of factors can affect the companies that become suppliers of cloud computing. These factors may help to make a lot of money, use your existing investments, protect the franchise, attacking moves, to develop a relationship on the shoulder of buyers and use the platform as shown in Figure 1

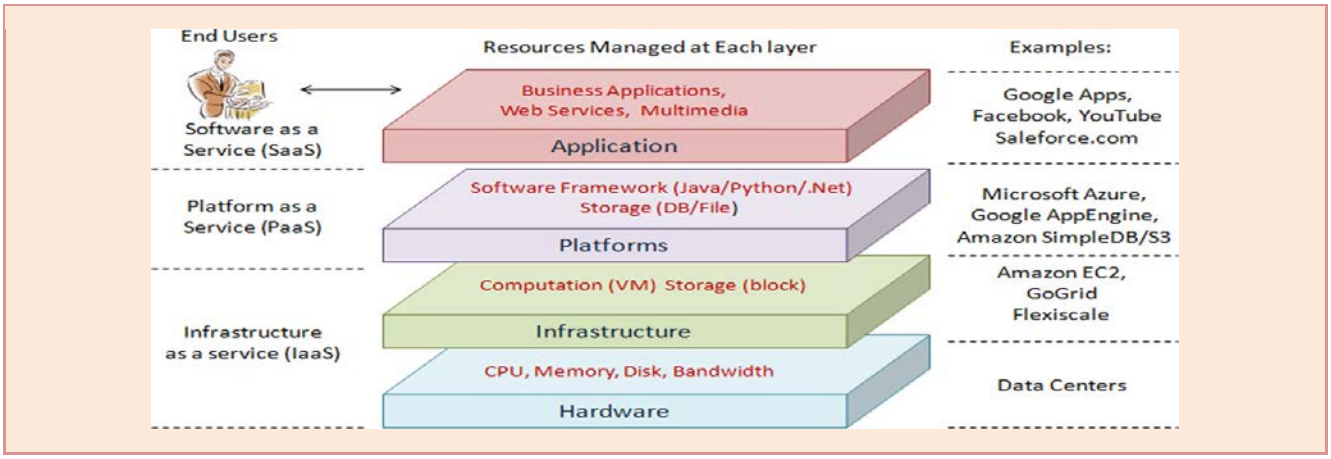


Figure 1. Cloud Computing Architecture [10]

In addition, a cloud computing environment also offers dynamically scalable resources which are already provided as a service such as shared hardware to multiple online users or on the web [14]. This promises huge cost-effective benefits among the distributed adopters. Instant messaging, e-mail, business software and web content management are of the many applications that can be provided via the cloud [15].Cloud computing is a revolution for the companies that implement it in their information systems. Cloud computing has raised new limits, offering resources, memory storage and data transfer performance in a market environment with scalable and flexible computing power to supply the demand with elasticity, great reducing capital costs. As a result, acceptance of a cloud computing is spreading rapidly which provides a new paradigm and opportunity that all companies should not ignore because of its huge impact on computing environment utilization [16].

The five basic elements of a cloud computing environment are broad network access, measured services, on-demand self-service, rapid elasticity, and resource pooling" [17].

In deployment model implementation inside or outside, there are four cloud computing modalities identified by NIST which are as follows?

- Private Cloud

Enterprise-owned or leased and maintained by a private network company with the greatest specific security level [18].

- Community General Cloud

An infrastructure runs by different organizations for specific community sharing, or a cooperative for common interests [19].

- Public Cloud

Sold to the public, providing off-site internet services, having a mega-scale infrastructure and shared resources [20]

- Hybrid Cloud

A combination and composition of more than two clouds to form a unique entity combined to form a single cloud [21-22].The hierarchy of deployment models of cloud computing are shown in Figure 2.

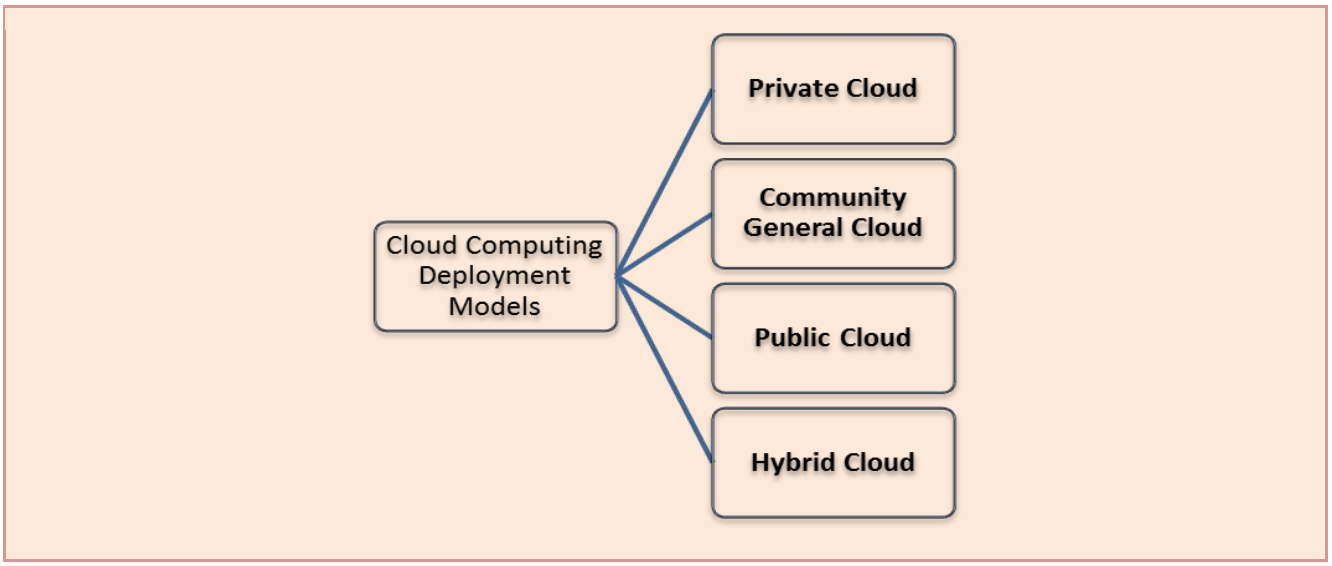


Figure 2. Hierarchy of Deployment Models of Cloud Computing

Cloud Computing Security Models

Four clouds computing security models are described here in Figure 3.

■ The Model of Multiple Tenancies

In multi tendency environment multiple applications are run by service providers to offer services to clients on demands with the provision to isolate faults and viruses, and prevent invasion by the other virtual machines [24-26].

■ The Cloud Risk Accumulation Model of CSA

This consists of three components, Platform as a Service provides the ability to support tools created using programming languages and provide a consumer-created cloud infrastructure or acquired applications to deploy to users [27]; Software as a Service use software applications, provided by the cloud infrastructure provider i.e. via web browser [28]; and Infrastructure as a Service provides the ability to use operating systems and applications software arbitrarily with management or control by cloud users but without control over operating systems, memory storage, deployed software applications, and selected networking devices and components (e.g. host firewalls) but possibly with other limited control[29-30].

■ JericoFormu's Cloud Cube Model

This describes information about properties and attributes of security, entailed in the cloud service and cloud-deployment models of cloud computing without any restrictions and limitations [31].

■ The Mapping Model of Cloud, Security and Compliance

This shows security control, a cloud model ontology and compliance in a good manner for the study and analysis of interruptions and gaps between the cloud computing architectures and frameworks for confirmation and compliance.

Relevant policies and security controls must be available and provided by cloud services providers to clients, customers or third parties [32-33].

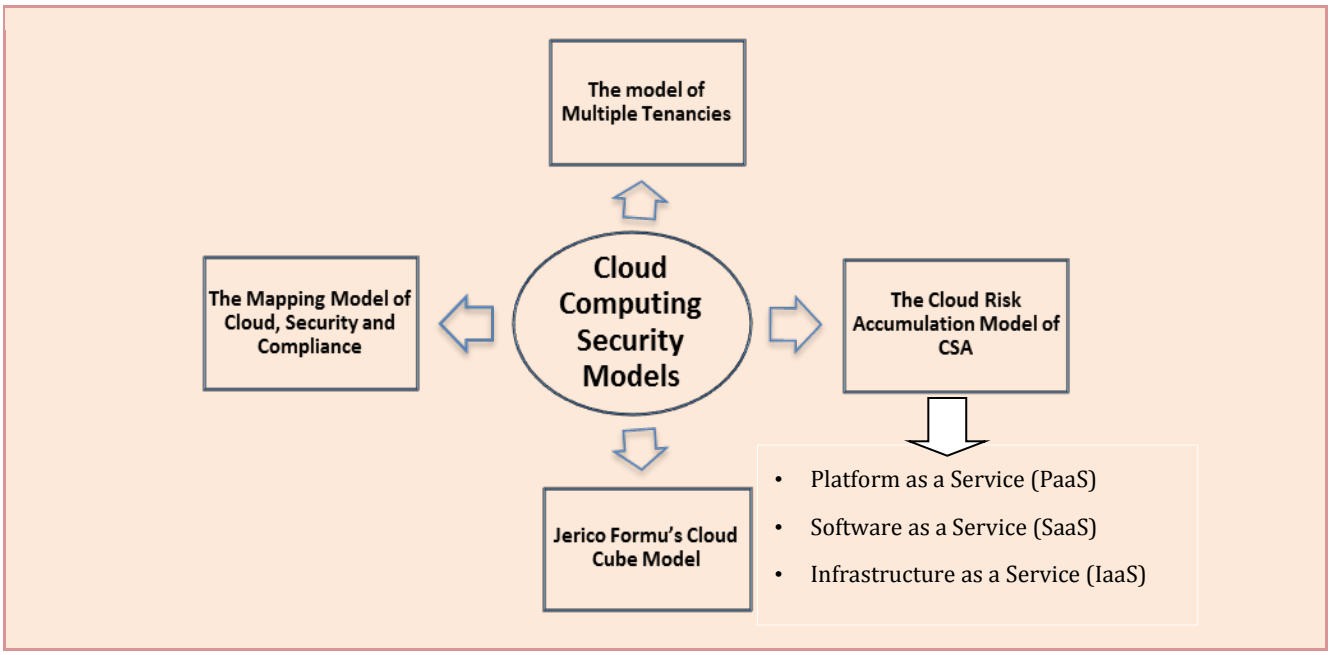


Figure 3. Cloud Computing Security Models

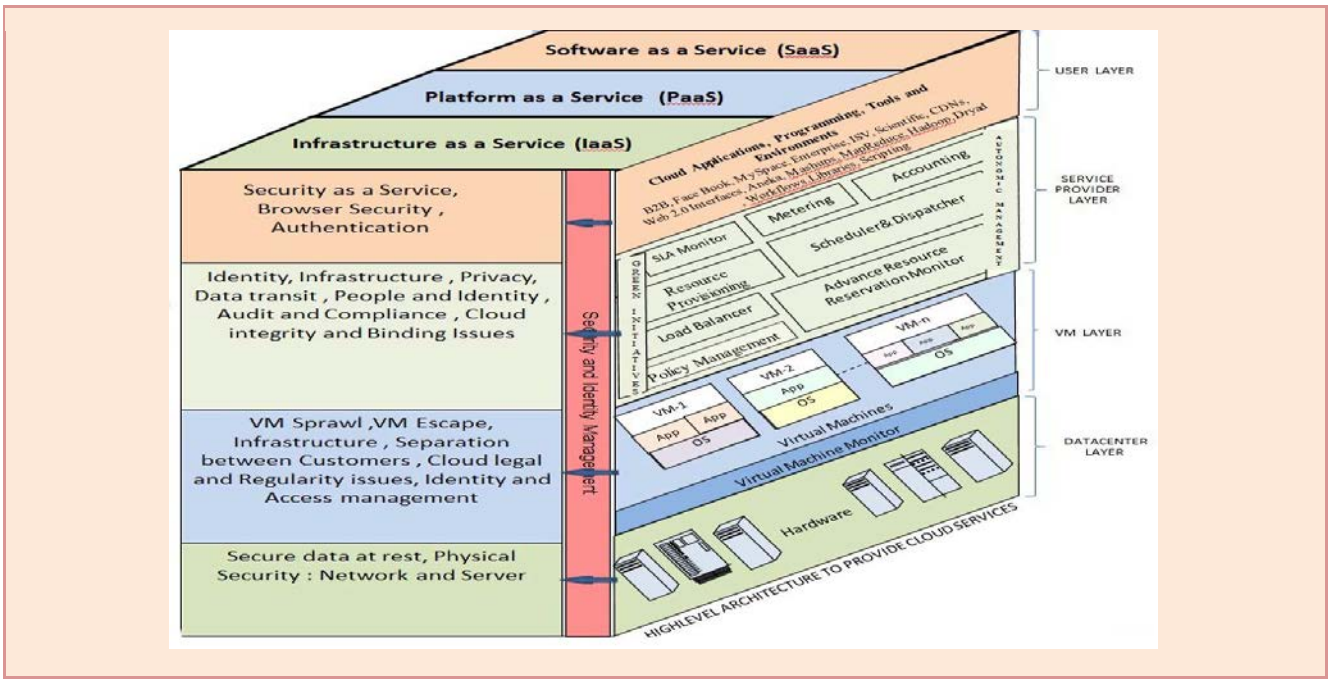


Figure 4. Security Architecture of Cloud Computing [39]

Cloud Computing Security Architectures

A Signal Processing in the Encrypted Domain (SPED) architecture in computing clouds which is based on a cryptography technique that is based on multiparty computation or homomorphic encryption. SPED enables secure and verifiable outsourcing of signal processing. The users communicate by using an application programming interface (API)[34]as a plugin with the middleware to arrange new inputs and retrieve outputs. This plugin is parallelized within the Trusted Cloud to provide a clear API from cryptographic information and complete protocols are introduced. Another architecture

for cloud computing security was introduced which use a tamper-proof hardware token to generate Garbled Circuits (GCs)that are afterwards commutated in parallel by the cloud. The token gets the description of a value based on Boolean circuit and produces the corresponding GC using a constant memory size [35].

Open Security Architecture (OSA) is a security architecture that provides easily integrated and free frameworks in applications; for security. Some patterns are used that are based on schematics or format to show a stream of information traffic flow for a specific and particular implementation with a line of action and policies implemented at each and every step for cloud security? [36].

The security architecture for security issues, threats, risks and challenges in a cloud computing environment to implement security for clients is based on four layers of services. The categorizations based on services are IaaS, PaaS, and SaaS [37-38].The four layers are elaborated on, with mapping of different security threats and issues for each layer in Figure4.

Security Issues & Challenges in the Cloud Computing Environment

Privacy and security are the two main issues and concerns of a cloud computing environment. In this environment virtualization is used which allows cloud users to approach and access a computing environment. That environment is actually larger than its physical world. To access this virtual environment, the user is obligated to go through and transmit data to the cloud. Therefore several security issues and problems arise. These security issues and threats [40]for cloud computing, involves a lot of technologies, including databases, virtualization, networks, resource planning, operating systems, load balancing, transaction management, memory management and concurrency control. Thus, safety concerns for these systems and technologies are applicable to cloud computing. For example, a network that is connected to cloud systems must be safe. The paradigm of virtualization present in a cloud computing environment, results in many security concerns. For example, the mapping of any virtual machine to a physical machine should be accomplished with reliability. Data privacy and security includes data encryption ensuring that appropriate policies are provided and applied to data communication and sharing. Therefore some memory management and resource allocation algorithms must be fortified and protected. Finally, methods of data analysis may also be applied to the discovery and detection of malware in the clouds [41].The hierarchy of security issues and challenges in cloud computing is given in Figure 5.

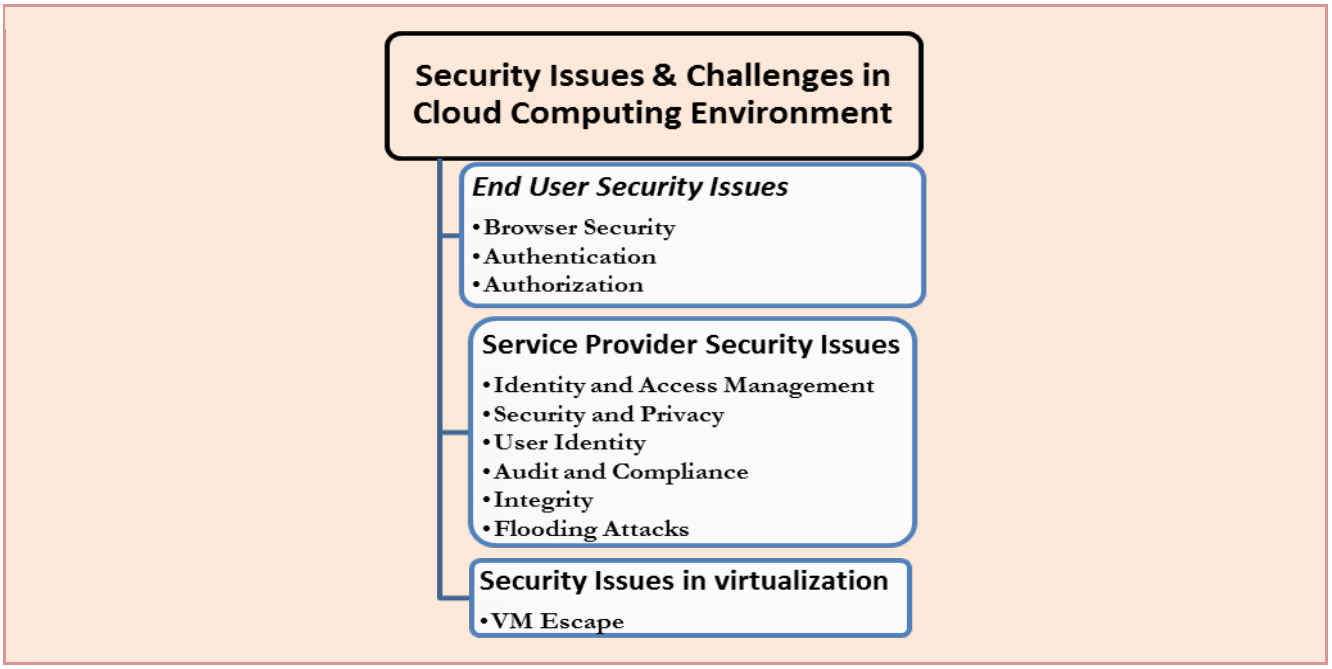


Figure 5. Hierarchy of Security Issues and Challenges in Cloud Computing

■ End User Security Issues

Access to shared resources by end users over any cloud computing environment must be kept in mind; access control agreements must be kept in mind for acceptable use based on interests or conflicts. The customer and user organizations

have mechanisms and processes to find vulnerable programs or protocols or code at checkpoints, such as; firewalls, mobile devices, or servers as well as distributed patches or signals on intrinsic and native systems, if they can be found. The cloud computing environment should block any user who has malicious or malevolent intent; to gain control of and access to the data/information [42].

- **Browser Security**

Cloud computing's distant servers are used for calculations whereas client or user nodes are used for input / output(I/O)processes [43].For authentication and authorization of information in a web browser environment that is not based on client applications, it is convenient for all users who use the cloud worldwide. This environment can be categorized into the following types: web applications, Web 2.0 and software as a service. Transport layer security is used for encryption of data and for the authentication of any host. Any cloud operating system (e.g. Google Chrome) provides the main foundation for I/O for the client and user. The challenges, threats and issues facing security for browsers in any cloud computing environment are many. The line of cloud defence for any web browser is the Same Origin Policy (SOP) used by server, which can be considered to observe the original destinations and sites of the web server browser whenever the request is sent, and only accepts requests that arrives from the same place that has already been verified as a structure with enough security. The main problem is that a web browser cannot use XML signature /encryption but this feature might be included in future web browsers. They can then use transport layer security (TLS) or Secure Socket Layer [44], which is explains it into two stages: the recording stage and handshake TLS. It provides the main system of security for any web browsers but the digital certificate of the server and all its pages are not included in this security. The main weakness in TLS is phishing, in which users deceptively aim to gain another person's login details by using a malicious web site. If any attacker succeeds in accessing this data, TLS is useless for the protection of the data [45].

- **Authentication**

In any cloud computing paradigm, the chief foundation for the user is authentication and access control [46], but access control is more important. All the data are available to all users on the Internet. A Trusted Platform Module (TPM) is strongly and widely used for authentication via user name and password. Trusted Computing Group (TCG) is an Interface for Metadata Access Points (IF-MAP)for authoritative users and other security threat standard in a real-time communication between any customer and cloud services provider. Based on the storing of user's identifications, a user is allocated or discharged [48]. The individuality of a control system can be determined by the cloud user in real time, so within a few seconds, access to the cloud for any user can be annulled or altered. Trusted computing always provides authentication [49]to improve security in any cloud computing environment to client nodes and other attached devices. For any frequently targeted attack, authentication and virtual hosting services are required. Some protective procedures are used for process authentication to prevent recurrent attacks by various means in order to authenticate client information provided by the user [50]. The Stages which provide authentication must, observe the sensitivity of requests and materials available for risks. With the increase in cloud computing, providers support security assertion markup language (SAML) which is used to manage users and their identities when granting access. SAML also provides a way to exchange information between cooperating domains. For example, any transaction may permit SAML [51- 52] declarations such that a user is authenticated by providing privileged information. After reception of the information, the service provider uses the given information to grant access to the appropriate user based on identity and authorizations. SAML demands and retort posts are usually presented on simple object access protocol (SOAP), which is based on extensible markup language (XML) for the given format [53].

- **Authorization**

Another important requirement is authorization which is used to maintain the security of a cloud computing environment to confirm and maintain referential integrity. For this purpose the user's information or authorizations are saved for future determinations. [54] Authorization is tracked by managing and providing the benefits of processing streams in any cloud. Authorization is preserved by any system administrator in a private cloud environment [55].

■ Service Provider Security Issues

In a public cloud computing environment that offers services, the provider must authenticate the strength of any cloud computing environment and validate any organizational security needs and supplier administration for software security requirements. The cloud services supplier provide essential security to protect records and applications in any organization, and furthermore offers proof as to the efficiency of these controls, migratory administrative evidence and roles in the cloud [56].

- **Identity and Access Management**

In any cloud computing environment and its architecture, identity and access management (IAM) is conducted whenever any data are provided to transitional party or any third party, especially for administration or storage inside a extensive users atmosphere. Appropriate safety steps and security rules with policies must be provided to ensure full control over uninterrupted data. IAM[57]is based on authorization, authentication and accounting (AAA) of clients or users and for any users that are using cloud computing facilities. There are few "trust boundaries" in any association that are frequently inert and that accomplish software requests that are organized to enable any association. In any categorized data centre, any one must be able to depend on the fringes of the systems, network and applications that are delivered over network security controls, within virtual private networks (VPN), an intrusion detection system (IDS), multi-factor authentication and intrusion prevention system (IPSS) that is using the cloud computing environment. Safety control claims and customer access will recompense the loss of network control and assurance of confidence. Strong authentication may be based on authentication of roles or claims, identity federation, trustworthy sources for user activity, single sign-on (SSO), auditing and the exact attributes[58].In a distributed computing system a protocol is required to face new problems i.e. data communication lines, intrusion detection, continuous monitoring control and public communication in a system. This server model needs a cloud services provider's guarantee on the records of all clients using a virtual server. IAM directs the security information center to recognize entities based on information that is given, to control the resources that should be allowed (or not) on the Internet [59].

- **Security and Privacy**

Privacy and security in a cloud computing environment is a most important issue which is a basic feature in the success of a new technology. Instructions for personal information change in any region of the world bring a number of imposed restrictions, whether they are stored outside or inside of any country [60],for any cloud computing services providers, in every acceptable area of the same service. The foundation of these obligations over the data which can be stored in any country as to privacy requirements [61], is very difficult to confirm. Personal and private data is increasing quickly,as is the danger of threats and the possible costs to company that process them. But the development of privacy and security services by experts in cloud services is mandatory. An efficient assessment approach should contain data security observance, identity management, privacy, safe process and other security-related lawful issues [62]. Cloud computing environment includes both the server side and client side with the importance typically located on the server, so the client can simply be overlooked. Many cloud providers and applications organized by the services, may have applications for privacy and security which allocates to only an authorized user to right to use the protected data [63-64].

Customers may also need a small, trivial application operation for mobile access as well as desktop. Many extension and plug-ins for browsers are disreputable when it comes to safety [65].Maintenance of logical and physical security for customers can be upsetting particularly with smart phones [66] and to a certain extent in a web browser. The growing accessibility and utilization of public media, private webs and other community sites is a real problem, because they are extra procedures that serve common engineering, which may unfavorably influence the privacy and safety of the any customer in its essential stage and in the access of cloud services. A key logger, backdoor Trojan, or other malware on any client device undermine the confidentiality, privacy and security of community cloud services [67].

- **User Identity**

Only authenticated users in any enterprise environment should access data and applications are and all unauthenticated clients access must be blocked. In a cloud computing environment to enlarge enterprise and many user communities, these controls are of more importance. Cloud computing environment provides a new and privileged working environment for users of the cloud services provider. An important need is privileged monitoring of users with loging that includes physical and background monitoring. The authorization and authentication in the background allowing clients to access easily and quickly the services of the cloud computing environment is managed [68].

- **Audit and Compliance**

In a cloud computing environment, during management of audit and compliance an interior policy can be compromised [36]. While undergoing audit security administration different operations, practices, policies, and other technical fundamentals are intended to review for managing the organization in turn assessing, detection, compliance, protection, and forensics security. Mandatory and regular checks for security are very important, and must not focus only on responsive checks that are done due to any incident that took place. There may also be active security checks arranged in order to control and assess of adequate and practical security processes, procedures, security control, and operations to save any critical possession of any organization. An approach to monitoring, auditing and compliance that helps to arrange service provider and their clients brings an increasing need to the development of cloud-based models. Auditing,

effectiveness, risk management and compliance need strong inner control supervision in conjunction with a vigorous outer audit [69].

- **Integrity**

A key feature to information security of any system is integrity. This indicates how to use secrete data [70]. Integrity also specifies how certified resources (hardware, data and software) can be altered by certified parties? Mostly atomicity, consistency, isolation and durability properties ought to be imposed over all cloud computing environments and all models [71-72].Integrity of data refers to the security of data against unauthorized modification, workmanship or deletion with acceptance to manage and protect company possessions to ensure valuable services and data are not stolen, misused or misappropriated [73]. These processes offer great access in influence who or what can the information system or data, affecting integrity. Authorization is a way by which any system indicates the levels of access for any particular authorization of a user who has to use the possessions prescribed by any system [74].With the increase of users in a cloud computing environment, it is essential to ensure only authorized access points and individuals may use the data [75].A cloud services provider make sure that all safety measures guarantee the data in any cloud memory storage against becoming altered or damaged; A safe supposition, without a specific service level agreement (SLA)to be managed [76], is that cell phone services providers can store customers data (i.e. contact list, a personal text messages, etc. But the level of data integrity, revival, and time to recover remains to be checked [77].

- **Flooding Attacks**

Another important feature of a cloud computing environment is the core of operational problems from outsourcing by the services providers of the cloud. The main task is to preserve the server and its related hardware; in its place of having to run its own interior data core model of a cloud computing environment which allows users to rent a server and its related hardware on requirement (IaaS).The approach that provides the main economic benefits is the dynamics to load data onto any server. Instead of purchasing a server and its related hardware for times of, a cloud computing environment allow active addition of the hardware needed for the definite consignment to occur. In principle, the attainment may be realized with deployment of virtual machines on servers of any data center in the cloud. If any company demands more power, it simply may be supplied with virtual equipment for the services. For security reasons, the provided architecture faces serious disadvantages [78].The immediate and consequential risk is flooding attacks. Flooding attacks are mainly sent by the attacker in a large quantity of useless requests for any service or application. Because these requests must be processed and implemented for any service to decide their invalidity, in cases of a flooding requests will typically result in a denial of service. One kind of threat is the denial of service (DoS) attack [79],in which hackers use all infected hardware to connect to any website, sending overloaded queries to a server which causes that server to be blocked and to stop working efficiently. DoS attacks are sent to a server of a cloud computing owner of a website which then may be charged a large amount of money by the cloud services provider for the use of more resources to meet the requirement of the server [80].

■ Security Issues in Virtualization

A virtual machine (VM) is a software implementation that executes different programs on the same machine [81]. Virtual machines in a private cloud are extensions of a corporate network environment that affects the privacy and security of all. The central technology is virtualization that makes the cloud computing environment possible [82].Thus we may say that virtualization is a backbone support for any cloud computing environment. This virtualization allows a server or PC to simultaneously run more than one session of the operating system (OS), which allows clients to run the softwares designed on one computer for a different OS [71].

Many virtualization environments have the capability to build switches that are software-based and to configure a network in virtualization of virtual machines for one host to access more effectively [83].For example, for any virtualization environment that does not need exterior control for any networking environment, most virtualized software may support the host network in a public subnet of internal host computers. In some hypervisors that can allow any network to monitor their utilities which are mainly not in equipments used to monitor the networks[84],an effect of virtualization is a possible loss of the partition of everyday jobs in the existing management for any organization. In conventional computing, a computer administrator may not arrange the machinery of any network privacy and security, such as firewalls, intrusion detection and prevention systems [85-86].

- **VM Escape**

Virtual machines have impressive handling of the host machines, and if any VM is configured incorrectly, it can enable functions to avoid virtualization. The VM escape is a complete root access or center to the joint users which results in a consistent system breakdown for privacy, safety or insulating layers. Some more threats for the virtualization hypervisor [87] are parts of any virtual machine that allows a VM host/ insulation and source division. It gives the essential partition

in any considered attack to establish how a virtual machine can persist to be any threats, issue or risk. A guest operating system (i.e. rogue hypervisors) can be loaded in a virtual machine operation under conventional operating system control for input / output devices and traffic on a network. But if it is proscribed by any hypervisors, the given hypervisors control the system fully, including the host computer and not just the virtual machine. As the threats of denial of service [88] increase, any widespread attack on virtualization compromises not only virtualized systems, but the virtual machines that distribute the possessions of any host, such as input / output devices, CPU, memory storage, disks and so on. In this case Denial of service attack [89] against the different hosts and virtual machines, or on an exterior check is considerably augmented [90].

Conclusions and Discussion

Cloud computing projections and forecasts show considerable growth in the execution and implementation of services in an emerging cloud computing paradigm. To make cloud computing environments more reliable, adequate control, safety and minimized security risks should be accomplished and carried out. This survey, presents a layout and overview of the cloud computing environment, its benefits, its security models, its security architectures, and security issues and risks to assisting and supporting management in implementing cloud computing processes, controls and procedures. Consideration must be given to the risks, issues and threats in order to provide a guarantee of availability, completeness and data integrity of the resources, software applications and hardware in the cloud. These issues include end user security issues (browser security, security-as-a-service, authentication, and authorization etc), service provider security issues (security and privacy, user identity, audit and compliance, integrity, flooding attacks, accounting and accountability, identity and access management etc) and security issues in virtualization (VM escape etc).

■ Future Directions

Further research and study will be focused on the growth of such a full, risk free and controlled framework or environment for cloud computing based on virtualization. This will guide management to assist with guidelines, standards and policies, so management can decide to be consistent with the cloud environment and will concentrate on virtualization issues and risks. Privacy and security of each and every component of the cloud will continue to be a serious issue, untill all users must are fully aware of the architecture and "depth" of the cloud. That includes who facilities and controls all the users, as long as the company can expand and afford to "give" and provide all the information about the cloud environment. A decision taken only after careful study and analysis of threats, challenges, issues, risks and political considerations of cloud computing on the other hand, can get lost in the cloud.

Assurance of organizational competitiveness and flexibility is crucial, in place of effective confrontation management for an organizational setup to determine a model that prevents cyber threats and malicious cyber activities when such threats arise. Incident handling processes are complicated by the distributed nature of the cloud[91].Planning research tasks and steps of the framework in depth, especially highlight the need of the organization to review existing tools that may be used to sustain a process with the framework guidelines [92].Due to the serious concern over security and privacy, the institutions that have cloud computing environment are currently thin and dysfunctional, so future work might be helpful to examine how ethical, political, cultural and social factors are allied with security issues in cloud computing [93].To formalize the security models in a cloud computing, some comprehensive computation (linear program computation, data mining, layered compression [94],virtual disk storage[95], etc.) can be considered to spot light the preserve of privacy issues in all the above mentioned computations [96].The security of cloud computing, which to be addressed needs can be considered a significant research problem. In the future anything-as-a-service (XaaS) will be the service model that will be used which will provide everything as a service [97].

In the near future a new era of cloud computing will be seen, in which the Internet of Things can be considered a new technological innovation [98].In the near future re-encryption techniques also need to be discussed in the cloud computing environment[99].

References

[1] Foster, Ian, Yong Zhao, Ioan Raicu, Shiyong Lu., "Cloud computing and grid computing 360-degree compared," *In Grid Computing Environments Workshop*, 2008. GCE'08, pp. 1-10. IEEE, 2008.

[2] Zhang, Qi, Lu Cheng, Raouf Boutaba., "Cloud computing: state-of-the-art and research challenges," *Journal of internet services and applications*, vol. 1, no. 1, pp. 7-18, 2010. Article (CrossRef Link)

[3] George Pallis, "Cloud Computing," *IEEE*, pp.70-73, 2010.

[4] Wang, Lizhe, Gregor Von Laszewski, Andrew Younge, Xi He, Marcel Kunze, JieTao, Cheng Fu., "Cloud computing: a perspective study," *New Generation Computing 28*, no. 2, pp. 137-146, 2010. Article (CrossRef Link)

[5] Buyya, Rajkumar, RodrigoN. Calheiros, XiaorongLi., "Autonomic cloud computing: Open challenges and architectural elements," *In Emerging Applications of Information Technology (EAIT), 2012 Third International Conference on*, *IEEE*, pp. 3-10, 2012.

[6] Chang, Hyokyung, Euiin Choi., "Challenges and security in cloud computing," In *Communication and Networking*, *Springer Berlin Heidelberg*, pp. 214-217, 2010.

[7] Hashizume, Keiko, David Rosado, Eduardo Fernández-Medina, Eduardo B. Fernandez., "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, 4, no. 1, pp. 1-13, 2013.

[8] Qian, Ling, ZhiguoLuo, Yujian Du, LeitaoGuo., "Cloud computing: An overview," In *Cloud computing*, *Springer Berlin Heidelberg*, pp. 626-631, 2009. Article (CrossRef Link)

[9] Kumar, Ashish., "World of Cloud Computing & Security," *International Journal of Cloud Computing and Services Science (IJ-CLOSER) 1*, no. 2, pp. 53-58, 2012.

[10] Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee et al., "A view of cloud computing," *Communications of the ACM 53*, no. 4 pp. 50-58, 2010.

[11] Ertaul, Levent, Sarika Singhal, Gökay Saldamli, "Security Challenges in Cloud Computing," In *Security and Management*, pp. 36-42, 2010.

[12] Rimal, Bhaskar Prasad, Eunmi Choi, Ian Lumb., "A taxonomy and survey of cloud computing systems," In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*, *IEEE*, pp. 44-51, 2009.

[13] Almond, Carl., "A practical guide to cloud computing security," *A white paper from Accenture and Microsoft*, pp. 3-9, 2009.

[14] Basson, Benhardus., "The right to privacy: how the proposed POPI Bill will impact data security in a Cloud Computing environment," *PhD theisis., Stellenbosch:Stellenbosch University*, pp. 1-67, 2014.

[15] Modi, Chirag, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan., "A survey on security issues and solutions at different layers of Cloud computing," *The Journal of Supercomputing 63*, no. 2, pp. 561-592, 2013. Article (CrossRef Link)

[16] Srinivasamurthy, Shilpashree, D. Liu., "Survey on Cloud Computing Security," In *Proc. Conf. on Cloud Computing, Cloud Com*, vol. 10. Pp. 412-421, 2010.

[17] Dillon, Tharam, C. Wu, E. Chang," Cloud computing: issues and challenges," In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pp. 27-33. IEEE, 2010.

[18] Singhal, Paridhi., "Data Security Models in Cloud Computing," *International Journal of Scientific & Engineering Research*, Vol. 4, No. 6, pp. 789-793, Jun. 2013.

[19] Carlin, Sean, K. Curran., "Cloud computing security," *International Journal of Ambient Computing and Intelligence (IJACI) 3*, no. 1, pp. 14-19, 2011. Article (CrossRef Link)

[20] Srivastava, Prashant, S. Singh, A. Alfred Pinto, S. Verma, Vijay K. Chaurasiya, Rahul Gupta., "An architecture based on proactive model for security in cloud computing," In *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, pp. 661-666. IEEE, 2011.

[21] Curran, Kevin, Sean Carlin, Mervyn Adams., "Security issues in cloud computing," *Elixir 38* : 4069-72, pp 200-208, 2011.

[22] Al-Anzi, Fawaz S., Sumit Kr Yadav, J. Soni, "Cloud computing: Security model comprising governance, risk management and compliance," In *Data Mining and Intelligent Computing (ICDMIC), 2014International Conference on*, pp. 1-6. IEEE, 2014.

[23] Blakstad, Kåre Marius, M. Andreassen., "Security in Cloud Computing: A Security Assessment of Cloud Computing Providers for an Online Receipt Storage," pp. 1- 103, 2010.

[24] Nguyen, Thuy D., Mark A. Gondree, David J. Shifflett, J. Khosalim, Timothy E. Levin, and Cynthia E. Irvine," A cloud-oriented cross-domain security architecture," In *Military CommunicationsConference,2010-Milcom 2010*, pp. 441-447. IEEE, 2010. Article (CrossRef Link)

[25] Padhy, Rabi Prasad, M. R. Patra, S. Chandra Satapathy., "Cloud Computing: Security Issues and Research Challenges," *International Journal of Computer Science and Information Technology &Security (IJCSITS) 1*, no. 2, pp. 136-146, 2011.

[26] Khalil, Issa M., A. Khreishah, S. Bouktif, A. Ahmad., "Security concerns in cloud computing," In *Information Technology: New Generations (ITNG), 2013 Tenth International Conference on*, *IEEE*, pp. 411-416, 2013. Article (CrossRef Link)

[27] Goyal, Vikas, C. Kant., "Security issues for Cloud Computing," *Journal AnuBooks* : pp. 274-282, 2011.

[28] Mewada, Shivlal, U. Kumar Singh, P. Sharma., "Security Based Model for Cloud Computing," *Int. Journal of Computer Networks and Wireless Communications (IJCNWC) 1*, no. 1, pp. 13-19, 2011.

[29] Zhang, Rui, Ling Liu., "Security models and requirements for healthcare application clouds," In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 268-275. IEEE, 2010.

[30] Vaquero, LuisM., L. R. –M, Daniel Morán., "Locking the sky: a survey on IaaS cloud security," *Computing 91*, no. 1, pp. 93-118, 2011. Article (CrossRef Link)

[31] Kaur, Barinder, S. Sharma., "Parametric Analysis of Various Cloud Computing Security Models," *International Journal of Information&Computation Technology*, Vol. 4, No. 15, pp.397-402, 2014.

[32] Alabbadi, Mohssen M., "Cloud computing for education and learning: Education and learning as a service(ELaaS)," In *Interactive Collaborative Learning (ICL), 2011 14th International Conference on*, pp. 589-594. IEEE, 2011.

[33] Vijay.G.R, Dr.A.Rama Mohan Reddy., "Investigational Analysis of Security Measures Effectiveness in Cloud Computing: A Study," *Computer Engineering and Intelligent Systems*, Vol.5, No.7, pp 23-30, 2014.

[34] Bhadauria, Rohit, Rituparna Chaki, N. Chaki, Sugata Sanyal., "A survey on security issues in cloud computing," *arXiv preprint arXiv*:1109.5388, pp.1-15, 2011.

[35] Bugiel, Sven, S. Nürnberger, A. -Reza Sadeghi, T. Schneider., "Twin clouds: Secure cloud computing with low latency," In *Communications and Multimedia Security*, Springer Berlin Heidelberg, pp. 32-44, 2011. Article (CrossRef Link)

[36] Andrei, Traian, Raj Jain., "Cloud computing challenges and related security issues," *A Survey Paper*. http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud.Pdf, pp. 1-10, 2009.

[37] SO, Kuyoro., "Cloud computing security issues and challenges," *International Journal of Computer Networks*, pp. 247-255, 2011.

[38] Jansen, Wayne, T. Grance., "Guidelines on security and privacy in public cloud computing," *NIST special publication 800*, 144, 2011.

[39] Reddy, V. Krishna, Dr. LSS Reddy., "Security architecture of cloud computing," *International Journal of Engineering Science and Technology (IJEST) 3*, no. 9, pp. 7149-7155, 2011.

[40] Zhao, Gansen, C. Rong, M. Gilje Jaatun, F. Eika Sandnes," Reference deployment models for eliminating user concerns on cloud security," *The Journal of Supercomputing 61*, no. 2 : 337-352, 2012. Article (CrossRef Link)

[41] Roberts II, John C., Wasim Al-Hamdani., "Who can you trust in the cloud?: A review of security issues within cloud computing," In *Proceedings of the2011 Information Security Curriculum Development Conference on*, pp. 15-19. ACM, 2011.

[42] Fernandes, D. AB, L. FB Soares, João V. Gomes, Mário M. Freire, Pedro RM Inácio., "Security issues in cloud environments: a survey," *International Journal of Information Security 13*, no. 2 pp. 113-170, 2014.

[43] SO, Kuyoro., "Cloud computing security issues and challenges," *International Journal of Computer Network*, pp. 247-255, 2011.

[44] Fauzi, A. Azila Che, A. Noraziah, T. Herawan, Noriyani Mohd Zin, "On cloud computing security issues," In *Intelligent Information and Database Systems*, Springer Berlin Heidelberg, pp. 560-569, 2012.

[45] Onwubiko, Cyril, "Security issues to cloud computing," In *Cloud Computing*, Springer London, pp. 271-288, 2010. Article (CrossRef Link)

[46] Nafi, K. Wazed, T. Shekha Kar, S. Anisul Hoque, M. M. A. Hashem., "A newer user authentication, file encryption and distributed server based cloud computing security architecture," *arXivpreprint arXiv:1303.0598*, 2013.

[47] Kulkarni, Gurudatt, J. Gambhir, T. Patil, A. Dongare., "A security aspects in cloud computing," In *Software Engineering and Service Science (ICSESS), 2012IEEE 3rd International Conference on*, pp. 547-550. IEEE, 2012.

[48] Subashini, Subashini, V. Kavitha., "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications34*, no. 1 pp. 1-11, 2011. Article (CrossRef Link)

[49] Reddy, A. Rama Mohan., "Data Security in Cloud based on Trusted Computing Environment," *International Journal of Soft Computing and Engineering (IJSCE)*, Vol. 3, No. 1, pp. 187-191, Mar. 2013.

[50] Shen, Zhidong, Qiang Tong., "The security of cloud computing system enabled by trusted computing technology," In *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, vol. 2, pp. V2-11. IEEE, 2010. Article (CrossRef Link)

[51] Celesti, Antonio, F. Tusa, M. Villari, A. Puliafito., "How to enhance cloud architectures to enable cross-federation," In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 337-345. IEEE, 2010. Article (CrossRef Link)

[52] Gharehchopogh, F. Soleimanian, S. Hashemi, "Security Challenges in Cloud Computing with More Emphasis on Trust and Privacy," *International Journal of Scientific & Technology Research 1*, no. 6 pp. 49-54, 2012.

[53] Almorsy, Mohamed, J. Grundy, I. Müller., "An analysis of the cloud computing security problem," In *Proceedings of APSEC 2010 Cloud Workshop*, Sydney, Australia pp. 2-7, 30th Nov. 2010.

[54] Nurmi, Daniel, Richard Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, D. Zagorodnov., "The eucalyptus open-source cloud-computing system," In *Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on*, pp. 124-131. IEEE, 2009.

[55] Ramgovind, S., Mariki M. Eloff, E. Smith., "The management of security in cloud computing," In *Information Security for South Africa (ISSA)*, 2010, pp. 1-7. IEEE, 2010. Article (CrossRef Link)

[56] Subashini, Subashini, V. Kavitha., "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications 34*, no. 1, pp 1-11, 2011.

[57] Dorey, P. G., A. Leite, "Commentary: Cloud computing–A security problem or solution?," *Information security technical report 16*, no. 3 pp. 89-96, 2011.

[58] Gonzalez, Nelson, C. Miers, F. Redígolo, Marcos Simplício, Tereza Carvalho, Mats Näslund, Makan Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing." *Journal of Cloud Computing1*, no. 1 pp. 1-18, 2012.

[59] Sajay K R, Dr. S. Sasidhar Babu, Y. Vijayalakshmi, "Investigative Analysis of Security Issues and Challenges In Cloud Computing And Their Counter Measures", *Journal Impact Factor*, Vol. 5, No. 12, pp. 57-63, Dec. 2014.

[60] Jansen, Wayne, T. Grance, "Guidelines on security and privacy in public cloud computing." *NIST special publication 800 144*, pp. 1-70, 2011.

[61] Zissis, Dimitrios, D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems 28*, no. 3 pp. 583-592, 2012.

[62] Mohamed, EmanM., Hatem S. Abdelkader, S. El-Etriby."Enhanced data set curity model for cloud computing," In *Informatics and Systems (INFOS), 2012 8th International Conference on*, pp. CC-12. IEEE, 2012.

[63] Wang, Qian, Cong Wang, Jin Li, KuiRen, Wenjing Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," In *Computer Security–ESORICS 2009*, Springer Berlin Heidelberg, pp. 355-370, 2009.

[64] Xin, Zhang, L.S.-Q., L.N.-wen., "Research on cloud computing data security model based on multi-dimension." In *Information Technology in Medicine and Education (ITME)*, 2012 International Symposium on, vol. 2, pp. 897-900. IEEE, 2012.

[65] Wang, Cong, Sherman SM Chow, QianWang, KuiRen, Wenjing Lou., "Privacy-preserving public auditing for secure cloud storage." *Computers, IEEE Transactions on 62*, no. 2, pp 362-375, 2013.

[66] Tchifilionova, Vassilka., "Security and privacy implications of cloud computing–Lost in the cloud," In *Open Research Problems in Network Security*, Springer Berlin Heidelberg, pp. 149-158, 2011.

[67] Ko, Ryan KL, P. J. pramana, Miranda Mowbray, Siani Pearson, MarkusKirchberg, Qianhui Liang, Bu Sung Lee., "Trust Cloud: A framework for accountability and trust in cloud computing," In *Services(SERVICES), 2011 IEEE World Congress on*, pp. 584-588. IEEE, 2011.

[68] Okuhara, Masayuki, T. Shiozaki, T. Suzuki., "Security architecture for cloud computing," *Fujitsu Sci. Tech. J 46*, no. 4 pp. 397-402, 2010.

[69] Chen, Zhixiong, John Yoon., "IT auditing to assure a secure cloud computing." In *Services (SERVICES-1), 2010 6th World Congress on*, pp. 253-259. IEEE, 2010. Article (CrossRef Link)

[70] M Mohamed, Eman, H. S Abdelkader, S. El-Etriby., "Data Security Model for Cloud Computing." In *ICN 2013, The Twelfth International Conference on Networks*, pp. 66-74, 2013.

[71] Ramgovind, S., Mariki M. Eloff, E. Smith., "The management of security in cloud computing." In *Information Security for South Africa (ISSA)*, 2010, pp. 1-7. IEEE, 2010. Article (CrossRef Link)

[72] Tianfield, Huaglory., "Security issues in cloud computing," In *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*, pp. 1082-1089. IEEE, 2012. Article (CrossRef Link)

[73] Paquette, Scott, PaulT. Jaeger, Susan C. Wilson., "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly 27*, no. 3 pp.245-253, 2010. Article (CrossRef Link)

[74] Zhao, Gansen, C. Rong, M. G. Jaatun, F. Eika Sandnes., "Deployment models: Towards eliminating security concerns from cloud computing." In *High Performance Computing and Simulation (HPCS), 2010 International Conference on*, pp. 189-195. IEEE, 2010.

[75] Brodkin, Jon., "Gartner: Seven cloud-computing security risks," *Network World*, pp. 1-2, July 2008.

[76] Lar, S-U., Xiaofeng Liao, Syed Ali Abbas., "Cloud computing privacy& security global issues, challenges,&mechanisms," In *Communications and Networking in China (CHINACOM), 20116th International ICST Conference on*, pp. 1240-1245. IEEE, 2011.

[77] Sotto, Lisa J., Bridget C. Treacy, Melinda L. McLellan., "Privacy and Data Security Risks in Cloud Computing," *World Communications Regulation Report 5*, no. 2, pp. 1-6, 38, 2010.

[78] Jensen, Meiko, J., N. Gruschka, Luigi Lo Iacono., "On technical security issues in cloud computing, " In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, pp. 109-116. IEEE, 2009. Article (CrossRef Link)

[79] Ertaul, Levent, S. Singhal, Gökay Saldamli., "Security Challenges in Cloud Computing," In *Security and Management*, pp. 36-42, 2010.

[80] Lonea, A. Madalina, D. Elena Popescu, H. Tianfield., "Detecting DDoS Attacks in Cloud Computing Environment." *International Journal of Computers Communications &Control 8*, no. 1, pp70-78, 2012.:

[81] Ritesh G. Anantwar, Dr. P.N. Chatur, Swati G. Anantwar, "Cloud Computing and Security Models: A Survey", *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol. 1, No. 2, pp. 39-44, Nov. 2012.

[82] Rimal, Bhaskar Prasad, E. Choi, Ian Lumb., "A taxonomy and survey of cloud computing systems," In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*, pp. 44-51. IEEE, 2009.

[83] Yang, Yun, Lie Wu, WenpingHu., "Security architecture and key technologies for power cloud computing," In *Transportation, Mechanical, and Electrical Engineering (TMEE), 2011 International Conference on*, pp. 1717-1720. IEEE, 2011.

[84] Kazim, Muhammad, R. Masood, M. A. Shibli, Abdul Ghafoor Abbasi, "Security Aspects of Virtualization in Cloud Computing," In *Computer Information Systems and Industrial Management, Springer Berlin Heidelberg*, pp. 229-240, 2013. Article (CrossRef Link)

[85] Chen, Yanpei, V. Paxson, Randy H. Katz., "What's new about cloud computing security," *University of California, Berkeley Report No. UCB/EECS-2010-5 January20*, no. pp.1-8, 2010.

[86] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, Eduardo B. Fernandez., "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications 4*, no. 1, pp. 1-13, 2013. Article (CrossRef Link)

[87] Rocha, Francisco, M. Correia., "Lucy in the sky without diamonds: Stealing confidential data in the cloud," In *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP41st International Conference on*, pp. 129-134, IEEE, 2011.

[88] Dawoud, Wesam, I. Takouna, C. Meinel, "Infrastructure as a service security: Challenges and solutions," In *Informatics and Systems (INFOS), 2010 The 7th International Conference on*, pp. 1-8. IEEE, 2010.

[89] Choubey, Rajnish, R. Dubey, J. Bhattacharjee., "A survey on cloud computing security, challenges and threats." *International Journal on Computer Science and Engineering (IJCSE) 3*, no. 3, pp. 1227-1231, 2011.

[90] Meetei, M. Zico, A. Goel., "Security issues in cloud computing." In *Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on IEEE*, pp. 1321-1325, 2012.

[91] AbRahman, N. Hidayah, K. –K. Raymond Choo., "A survey of information security incident handling in the cloud," *Computers& Security 49*, pp. 45-69, 2015.

[92] Rebollo, Oscar, Daniel Mellado, E. Fernández-Medina, Haralambos Mouratidis., "Empirical evaluation of a cloud computing information security governance framework," *Information and Software Technology*, pp.44-57 58 ,2015.

[93] Kshetri, Nir., "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," *Telecommunications Policy 37*, no. 4: 372-386, 2013. Article (CrossRef Link)

[94] N., Rana Muhammad, M. Sharif, Mudassar Raza, Aman Ullah Khan., "Layered Compression Technique (LCT) Based on Entropy or Dictionary Methods," 2007.

[95] S. Muhammad, N. M. Butt, M. Raza, M. Arshad., "Distributed Virtual Disk Storage System." *Control Theory and Informatics 2*, no. 1, pp. 17-23, 2012.

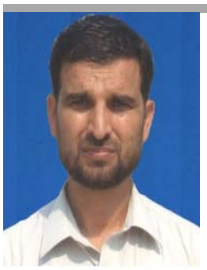
[96] Wei, Lifei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, Athanasios V. Vasilakos., "Security and privacy for storage and computation in cloud computing." *Information Sciences 258*, pp. 371-386, 2014.

[97] A., Mansaf, K. A. Shakil., "Recent Developments in Cloud Based Systems: State of Art.," *arXiv preprint arXiv*:1501.01323, 2015.

[98] S., Omprakash, P. Das, R. K. Chawda., "Hybrid Cloud Computing with Security Aspect," *International Journal of Innovations&Advancement in Computer Science, IJIACS*, Vol. 4, No. 1, pp. 76-80, 2015.

[99] Das, Sangita, A. Chandrakar, R. Pradhan., "A Review On Issues And Challenges Of Cloud Computing," *International Journal of Innovations & Advancement in Computer Science IJIAC*, Vol. 4, No. 1, pp. 81-88, 2015.

[100] Mell, Peter, Tim Grance., "The NIST definition of cloud computing," 2011.



Muhammad Alyas Shahid received his Master in Computer Science from Alkahir University, Islamabad. He is studying his MS (CS) from COMSATS, Wah Cantt with specialization in Image Processing. He is into teaching field from 1998 till date. Currently he is working as Head of Department Computer Section in POF Institute of Technology, Wah Cantt. His research interests are Image Processing, Computer Networks & Security, Multimedia Processing, Database and Computer Languages.

Muhammad Sharif, PhD, Associate Professor COMSATS, Wah Cantt received his MSc in Computer Science from Quaid-e-Azam University, Islamabad. He received his MS(CS) and PhD(CS) from COMSATS Islamabad with specialization in Image Processing. He is into teaching field from 1995 till date. His research interests are Image Processing, Computer Networks & Security, Parallel and Distributed Computing (Cluster Computing) and Algorithms Design and Analysis.