Security Issues for Cloud Computing

Sedieg A.Elatab[1] , Rabeah H.Ghareb [2]
[1] *Scientific Affairs Department , College Of Technical Engineering* **,** *Libya*
[2]*Sabratha University , Economy College , Libya*
[1]It2017Cisco@gmail.com
[2]Rabee7878@gmail.com

Abstract— **Cloud computing is becoming an adoptable technology for many of the organizations with its dynamic scalability and usage of virtualized resources an a services as a service through the Internet. It represents a shift a way from computing as a product that is purchased , to computing as a service that is delivered to consumers over the internet from large –scale data centers or "clouds" . Whilst cloud computing is gaining growing popularity in the academia appeared to be lagging behind the rapid developments in this field [1] .**

The main features of cloud computing is that the user does not have any setup of expensive computing infrastructure and the cost of its services is less. The cloud provider provides its services through the Internet and uses many web technologies that arise new security issues. In the recent years, cloud computing integrates with the industry and many other areas, which has been encouraging the researcher to research on new related technologies.

The biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications .

This paper discussed about the basic features of the cloud computing. Moreover, the paper describes several key topics related to the cloud, namely cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, security issues, threats and attacks and their solutions.

Keywords— **Cloud computing ;security issues; cloud technology** .

I. INTRODUCTION

Nowadays , the term "cloud computing" has been an important term in the world of Information Technology(IT).Cloud computing is a kind of computing which is highly scalable and use virtualized resources that can be shared by the users. Users do not need any background knowledge of the services. A user on the internet can communicate with many servers at the same time and these servers exchange information among themselves (Hayes , 2008)[2]. Cloud computing is currently one of the new technology trends(virtualization, fast connection and broadband internet).Cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing , one must also utilize the resource allocation and scheduling provided by clouds. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, resource scheduling, virtualization, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure[3]. This paper is designed as following, Section I illustrates the cloud computing architectural framework. Section II essential characteristics of cloud computing . Cloud services models are presented in Section III . Finally conclusion is given in

II.CLOUD COMPUTING ARCHITECTURAL FRAMEWORK[4]

The National Institute of Standard and Technology(NIST) defines cloud computing by describing five essential characteristics , three cloud service models, and four cloud deployment models. They are summarized in visual form in figure1 and explained in detail below .

ISSN 1737-930X

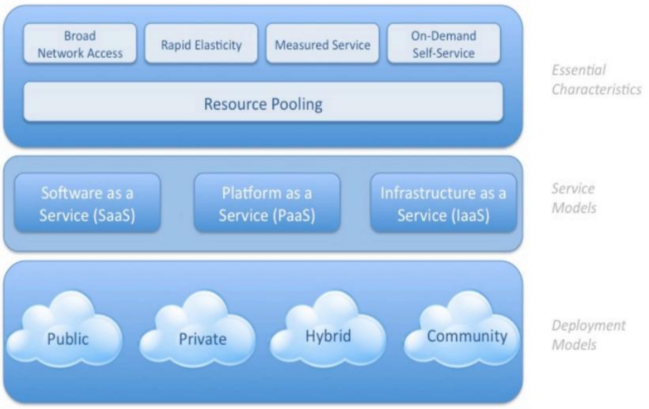

Fig. 1. NIST Visual Model of Cloud Computing Definition

In the researcher point of view the cloud computing is a model for enabling ubiquitous, 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 .

III.ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

There are five essential characteristics associated to the cloud services which demonstrate their relation to , and their differences from , traditional computing approaches:

A. On-Demand Self-Service

A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically , without requiring human interaction with a service provider.

B. Broad Network Access

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) as well as other traditional or cloud based software services.

C. Resource Pooling

The provider 's computing resources are pooled to serve multiple consumers using a multi-tenant model , with different physical and virtual resources dynamically assigned and reassigned according to consumer demand . Examples of resources include storage , processing , memory , network bandwidth , and virtual machine .

D. Measured Service

Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage , processing , bandwidth , or active user accounts). Resource usage can be monitored , controlled , and reported-providing transparency for both the provider and consumer of the service.

E. Rapid Elasticity

Capabilities can be rapidly and elastically provisioned-in some cases automatically – to quickly scale out ; and rapidly released to quickly scale in . To the consumer , the Capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

IV.CLOUD SERVICES MODELS

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the "SPI Model" where "SPI" refers to Software ,Platform or Infrastructure (as a Service), respectively – defined thus

D. Cloud Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

The applications running are accessible from various client devices through a thin client interface such as a web browser (e.g. , web-based email). The consumer does not manage or control the underlying cloud infrastructure including network , servers , operating systems , storage , or even individual application capabilities , with the possible exception of limited user-specific application configuration setting.

E. Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network , servers , operating systems , or storage , but has control over the deployed applications and possibly application hosting environment configurations.

F. Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing , storage , network , and other fundamental computing resources where the consumer is able to deploy and run arbitrary software , which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems , storage , deployed applications , and possibly limited control of select networking components (e.g., host firewall).

V.CLOUD DEPLOYMENT MODELS

Regardless of the service model utilized (SaaS,PaaS , or IaaS) there are four deployment models for cloud services , with derivative variations that address specific requirements.

G. Public cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services .

H. Private cloud

The cloud infrastructure is operated solely for a single organization . It may be managed by the organization or a third party , and may exist on –premises or off-premises.

I. Community cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission , security requirements , policy , or compliance considerations) . It may be managed by the organizations or a third party and may exist on-premises or off-premises.

J. Hybrid cloud

The cloud infrastructure is a composition of two or more clouds (private , community , or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load – balancing between clouds) .

VI. Cloud security concepts

The cloud security covers various security issues and threats. The paper identifies the source of the vulnerability and threats to understand the concept of cloud security. This section discusses some cloud specific concepts like virtualization, multi-tenancy, cloud platforms, data outsourcing, data storage standardization and trust management, to understand the security issues present in the cloud.

K. Virtualization aspect

Virtualization is a conceptual process of extracting the services, applications, computing resources and operating system from the hardware on which they run. The Virtual Machine (VMs) and Virtual Machine Manager (VMMs) are referred as a component of the virtualization. A VM is an image of large size contents per-image of the operating system (OS) called guest OS content memory and storage. The guest OS is responsible for running multiple programs on it.

The main feature of VM image is, it can easily move to another place, easily copied and make clones. Cloud delivers high available and scalable services to their customer. In case of machinery cloud which have a lack of resources, but due to the VM it can not be realized that the resources are limited.

L. Multi-tenancy

Multi-tenancy is a feature of cloud computing environment, that introduce the sharing concept, in which each running instances can be shared by one or more users called tenants. It provides capability to share single cloud platform among multiple users. Consider an IaaS provider, VMMs is referred to a multi-tenancy sharing platform while VMs refers to the instances. In a PaaS provider, Virtual Platform (VP) enables user to run multiple applications such as Java Virtual Machine (JVM) and .NET in multi-tenancy environment. Resulting from them, attacker can access neighbour VMs or running applications. Denial of Service (DoS) attack is another issue that can happen by consuming much resources.

M. Security controls

Security controls are countermeasure used to reduce or avoid risk. The countermeasures also prevent or respond to security threats. A list of security countermeasures, how to use them and all related information about countermeasures is given in the security policy. It contains a set of rules and practices used for implementation of security controls in a system, service or security plans. The security controls help us to achieve maximum security of sensitive data and critical resources.

N. Security policies

Security policy is a mechanism to establish set of security rules and regulations. This security policy further defines how these rules and regulations are implemented in a security system. For example, security policies can be helpful to know positioning and usage of security controls and mechanisms.

O. Cloud security services

The cloud security service is a complex service, technique, regulation and behaviour that is composed to protect IT assets. IT security measures aim to define security services for the cloud. This security service helps us to understand the need for security. The four fundamental cloud security services are defined as follow:

- **First main security service is confidentiality**, that refers to only authorized parties or system having permission to access the IT resources.
- **A key term of integrity** in the information security refers the characteristic in which data have not been modified by an unauthorized party. This security service is achieved by protecting assets from unauthorized deletion, modification or fabrication.
- **The authentication** is a process of verifying of an entity that a subject made to act on behalf of a given principal. The authentication attack aim is to verify own identity as a legitimate user. For restriction of unauthorized access and maintain the privacy of user accounts on a cloud required a strong authentication. The weak password, easy recovery method, and insecure registration process can break the authentication.
- **The high availability feature** of cloud computing aim is to minimizing application downtime and preventing business disruption. It refers the characteristic that having ability to every IT resource is accessible and usable during a specified period of time. In the cloud computing environment, the cloud provider and the cloud carrier are responsible for the availability of cloud IT resources.

P. Security identification of the threats

The most challenging issues at the time of implementation of suitable countermeasure in an IS, is identifying the unique security threats. In the standard security system designing process, first aim is to identify security threats associated with them, then find the security requirements then apply selected security controls to achieve the high reliability, maintainability and supportability. The confidentiality, integrity, availability is the building block of designing any security system. These important security aspects necessary applied to be made a secure cloud. The cloud architectural design provides a number of security advantages, which included the high availability, centralization of security, redundancy, and data process segmentation.

Q. Cloud platforms

Cloud users want to deploy their application and services to the cloud, it required some workable frames those are helpful to deploy their application. For example, VMM (a virtualized layer) is used as a cloud platform for IaaS services. In case of PaaS, .NET, and JVM platform is used as a development platform. These platform provides the tools that are required to build SaaS applications. The platform provides APIs, and IDE for development of the cloud applications. All the tools depend upon the underlying infrastructure of the platform and the programming language.

VII.CLOUD COMPUTING SECURITY CHALLENGES

Cloud security is a part of computer security. It describes set of policies, technology, and control that is helpful to protect the data and services. The threats and attacks directly or indirectly affect the cloud system. Integrity, availability and confidentiality of the cloud resources as well as service of different layers are breach, that may be raised new security concern[5].

The benefits introduced by cloud computing are legion. The most beneficial aspects of using cloud include fast and easy deployment, the pay-per-use model, and reduction of in-house IT costs. However, they also point out that security is the most important issue to be addressed in order to promote the widespread use of cloud computing.

Cloud computing providers need to solve the common security challenges of traditional communication systems. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself. In this section, we have categorized the main cloud security issues as traditional and new cloud security challenges.

R. Traditional security challenges

Although the security concerns in traditional communication systems also apply to the cloud, the use of cloud computing introduces new attack vectors that will make attacks either possible or simply easier to carry out.

The authentication and authorization applications for enterprise environments may need to be changed to work with a cloud environment. Such vulnerabilities represent an even more serious problem in multi-tenant environments, where the compromise of a virtual machine can affect all users on the same physical server. Cloud providers, therefore, might need to reconsider traditional security concerns from different angles.

S. Cloud security challenges

As end-users utilize the cloud services and store their data in the provider's infrastructure, the most critical security concern is about privacy and user data confidentiality. End-users want to know where their information is stored, and who is in control of that information in addition to the owners. They also want to be guaranteed that the critical information is not accessed and used illegally, even by the cloud providers.

VIII.THREATS TO CLOUD COMPUTING

In computer security, threat is defined as anything which is capable of causing serious harm to a computer system. Threats can lead to potential attacks on the computer system or network infrastructure. The paper (Hubbard and Sutton, 2010)[6] presented the top threats that are related to the security architecture of the cloud services. This paper exhibits several potential threats that are harmful to the cloud is shown in Table 1.

Table 1. Exhibits several potential threats

A comprehensive study on cloud threats described by the CSA in 2013 and its solutions			
Threats	Effects	Affected Cloud Services	Solutions
Malicious insiders	Penetrate organization recourses, damage assets, affect an operation	PaaS,SaaS,and IaaS	Use agreement reporting and breach notifications.
Shared technology issues	Interfere one user services to other user services by compromising hypervisor	IaaS	Audit configuration and vulnerability, for administration task use strong authentication and access control
Data loss and leakage	Personal sensitive data can be deleted , destructed, corrupted or modified	PaaS,SaaS,and IaaS	Provide data storage and backup mechanisms
Service/Account hijacking	Stolen user account credentials, access the critical area of the cloud.	PaaS,SaaS,and IaaS	Adoption of strong authentication mechanisms,security polices , and secure communication channel
Risk profiling	Internal security operations, security policies , auditing and	PaaS,SaaS,and	Acknowledge partial logs,data and infrastructure aspect, to secure data use monitoring and altering

When cloud adopted new technology in cloud infrastructure, definitely new attacks have come.

There are some attacks those are launch when cloud adopt new cloud technology.

The survey is summarized in Fig. 2. The Fig. 2 creates a building block in the reader's mind that is helping to understand the current security issues. The presented data storage and computing issues, virtualization and platform related issues are coming under the cloud delivery models. Additionally, the survey going on Internet related issues. Finally, the survey cover security issues related to trust and legal issues.

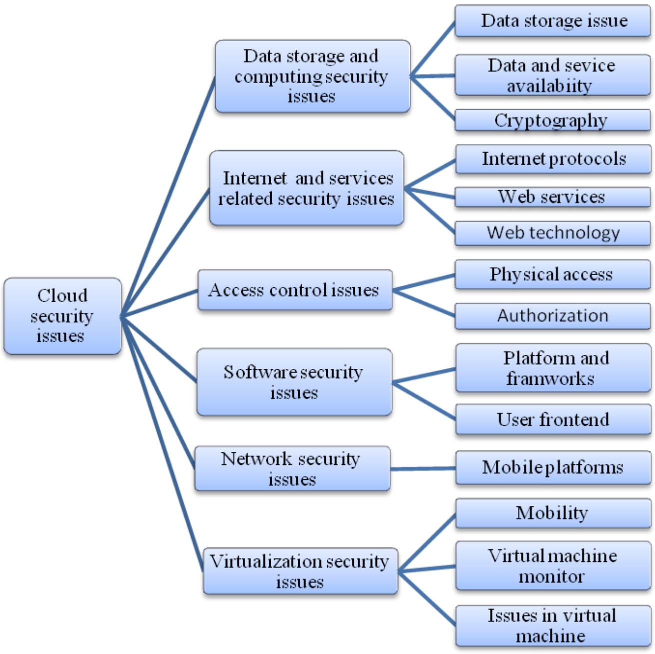

Fig. 2.A summary of the computing security issues

IX.Issues Of Security To Clarify Before Adopting Cloud Computing

The world's important information technology, advisory company, research and has identified seven security apprehensions that an enterprise cloud computing user should discourse with cloud computing providers (Edwards, 2009)[7] before approving.

- **User Access.** Ask providers for unambiguous information on the hiring and oversight of privileged administrators and the controls concluded their access to information. Major Companies should demand and enforce their own hiring principles for personnel that will operate their cloud computing environments.
- **Data location**: Enterprises should necessitate that the cloud computing provider store and process data in specific jurisdictions and should follow the privacy rules of those Jurisdictions.
- **Data Segregation:** Realize what is done to segregate your data, and probe for proof that encryption schemes are deployed and are effective.
- **Disaster Recovery.** Ask the provider for a contractual commitment to sustenance specific types of investigations, such as the research involved in the discovery phase of litigation, and verify that the provider has successfully supported such activities in the past. Deprived of evidence, don't assume that it can do so.
- **Regulatory Compliance**. Create sure your provider is willing to submit to external Audits and security certifications.
- **Disaster Recovery Verification**. Know what will happen if adversity strikes by asking whether your provider will be capable of utterly restore your data and service, and find out how long it will take.
- **Long-term Viability**. Ask forthcoming providers how you would get your data back if they were to fail or be assimilated, and find out if the data would be in a arrangement that you could easily import into a replacement application.

X.COUNTERMEASURES AND CONTROLS

The vulnerabilities and threats in the cloud are well documented. Each cloud service provider and cloud consumer have to devise countermeasures and controls to mitigate the risks based on their assessment. However, the following are some of the best practices in countermeasures and controls that can be considered[8] .

- **End-to-end encryption.** the data in a cloud delivery model might traverse through many geographical locations; it is imperative to encrypt the data end-to-end.
- **Scanning for malicious activities.** end-to-end encryption while highly recommended, induces new risks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to have appropriate controls and countermeasures to mitigate risks from malicious software passing through encryption.
- **Validation of cloud consumer**. the cloud provider has to take adequate precautions to screen the cloud consumer to prevent important features of cloud being used for malicious attack purposes.
- **Insider attacks.** cloud providers should take precaution to screening employee and contractors, along with strengthening internal security systems to prevent any insider attacks.
- **Secure leveraged resources.** in a shared/multi-tenancy model, the cloud provider has secure shared resources such as hypervisor, orchestration, and monitoring tools.

XI.CONCLUSION

Cloud computing provides the benefit of quick deployment, cost efficiency, large storage space and easy access to the system anytime and anywhere. So, the cloud computing is very much evident rapidly emerged technology and widely accepted computing environment around the world. However, there are many security and privacy concerns that obstacle to adoption of the cloud computing. All the cloud users should be well aware of the vulnerabilities, threats and attacks existing in the cloud. The awareness of security threats and attacks will help the organizations to carry out fast rate adoption of the cloud.

Cloud computing is a model to provide convenient, on-demand access to a shared pool configurable computing resources. In cloud computing, IT-related capabilities are provided as services, accessible without requiring detailed knowledge of the underlying technologies, and with minimal management effort. The great savings promised by the cloud are however offset by the perceived security threats feared by users. Cloud Computing is a rapidly revolution with IT and will become the default method of IT delivery moving into the future-organizations would be advised to consider their approach towards beginning a move to the Clouds sooner, rather than later [9] .

The researcher summaries the three operational domains of concern for cloud computing which can be applied to any combination of cloud service and deployment model as explained in the following points

- ***Application Security***. Securing application software that is running on or being developed in the cloud . This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).
- ***Encryption and Key Management***. Identifying proper encryption usage and scalable key management This section is not prescriptive, but is more informational is discussing *why* they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.
- ***Identity and Access Management***. Managing identities and leveraging directory services to provide access control . The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity and Access Management(IAM).

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physician machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

References

[1] Ahmed E.Youssef and Manal Alageel , A Framework for Secure Cloud Computing , Dept.of Information System , King Saud University Riyadh, 1154,KSA , IJCSI International Journal of Computing Science Issues, Vol.9, Issue4, No3, July 2012 , ISSN(Online): 1694-0814, www.IJSI.org.

[2] Peter Mell,Timothy Grance , The NIST Definition of Cloud Computing ,The National Institute of Standard and Technology, U.S.Department of Commerce ,Special Publication 800-145

[3] Security Issues for Cloud Computing , Technical Report UTDCS-02-10, Department of Computer Science, The University of Texas at Dallas, February 2010, (*Kevin Hamlen, Murat Kantarcioglu, Latifur and Bhavani Thuraisingham*).

[4] Security Guidance for Critical Area of Focus in Cloud Computing V2.1, Prepared by the Cloud Security Alliance December 2009.

[5] Ashish Singh, Kakali Chatterjee ,Cloud security issues and challenges: A survey - Department of Computer Science & Engineering, National Institute of Technology Patna 800005, Bihar, India.

[6] Hubbard and Sutton, 2010: Hubbard, D., Sutton, M., 2010. Top threats to cloud computing v1.0 Cloud Security Agency.

[7] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing , The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017).

[8] Edwards, 2009- Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.

[9] Understanding the Cloud Computing Stack SaaS , PaaS , IaaS , At site : www.rackspaceclouduniversity.com.