International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 6 (Nov-Dec 2016), PP. 59-67

A SURVEY ON SECURITY PATTERNS AND ISSUES IN CLOUD COMPUTING ENVIRONMENT

[1] Arshad Hashmi, [2] Omar M. Barukab,
[1]Department of Information Systems , [2] Department of Information Technology,
[1,2] Faculty of Computing and Information Technology - Rabigh,
King Abdulaziz University P. O. Box 344, Rabigh, 21911, Saudi Arabia
[1] ahsyed@kau.edu.sa, [2] obarukab@kau.edu.sa

***Abstract*—Cloud Computing becomes an attractive proposition because of long-term potential advantage by reducing the cost of services and thereby gaining more business outcomes. It is capable of transferring facilities by using the internet in a secured manner economically. It has got interested from both industry and academia. The shared utilization characteristics enhance the proficiencies of the hardware resources of cloud computing. By virtue of this feature, a cloud is being used by commercial and specific users to make available their data in form of either application or service. Security concern originates because of the sharing environment in which external administration for the migration of user's assets takes place.**

A comprehensive review in order to find major gaps and issues related to security comes under cloud computing has been tried to present. The issues belong to security and its possible countermeasure has been found out and present. The increased number of cloud services becomes the root cause of infrastructural complexity behind the services. For operating and managing this complex infrastructure effective monitoring is essential. After conducting the study I found the survey lacks the comprehensive analysis for the monitoring of the cloud. So this paper also includes the detailed discussion of monitoring systems for the cloud. Current platforms and services related to Cloud monitoring have been discussed which is needed for making informed decisions. This survey also includes the discussions belong to research platform required for cloud infrastructure so that the researchers can identify the appropriate way for simulation or prototype implementation for further evaluation.

***Keywords*— Cloud computing, Multi-tenancy, Virtualization, Cloud resource monitoring, simulation.**

I. INTRODUCTION

It is a model which allows a user to share computing resources on demand. This resource may include networks, servers, storage, applications and services under some managing capabilities or service provider interaction. It focuses on sharing computing resources instead of maintaining local servers or particular devices to handle applications.

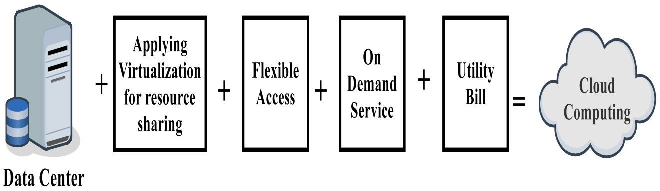

Fig 1: Pictorial definition of Cloud Computing.

Cloud computing comes under significant distributed computing pattern. It includes abstracted, virtualized, highly-scalable, being able to configure and reconfigure computing resources which can be permitted to use by the user and easily controlled with least management effort. Provided facilities can be categorized as "applications", "platforms", and "infrastructure".

Under the cloud environment users by registering themselves for any desired services can get rid of from the establishment of related hardware and software setup. In order to apply cloud computing infrastructure as a utility high-security concern has always been the major issues. Complex data and applications have been moved to cloud data centers to be implemented in a virtual computing environment using virtual machines. This poses multi-directional security challenges. Cloud server is responsible for this major threat which comes under the category of physical control of data. As a result unique identity and credential management, authentication, reliability, tempering, secrecy, theft and data loss has been posed. Xiao, Y. Xiao et al talk the security issues viewing integrity, confidentiality, availability, accountability with a slight argument which causes vulnerability. Some common security models related to a cloud environment, named as cube-model, risk assessment model, multitenancy model has been discussed by J. Che, Y. Duan and others. Tari also tried to explain the security concern to a cloud and related solutions. Six sub-categories has been introduced related to Security issues in cloud computing environments [1] [2] [3] [4] [5].

This includes (1) How to trace the cloud server to provide safety mechanisms, (2) how to keep the sensitive information confidential (3) how to protect illegal operation from malicious insiders (4) how to protect against fraud, phishing and exploitation (5) how to maintain multi-tenancy under virtual working environments (6) How to introduce and implement legal jurisdiction for the users against the providers.

To meet the expectations of customer's privacy issues appropriate use of the information is needed. Different cloud scenario has different privacy issues. It is divided into four sub-categories [1] [2] [6] and introduced as (a) how to prevent from unauthorized resale during storage and processing of data under the environment of cloud.(b) how to provide data replications by avoiding loss of data , unauthorized modification or fabrication and leakage (c) How to fix responsibility to ensure legal requirements for personal information.

Under the distributed computing environments, for maintaining security mechanism trust issue is an essential substitute because trust includes many easy-going security attributes, like dependability, reliability, trustfulness, security, competence etc.

Our survey is different from the aforementioned surveys on the ground of its comprehensiveness, vast discussion on security related problems existing with the cloud environment, and highlights most recent techniques to counter the effect. I have discussed the major security concern in existing cloud computing environments in order to identify tangible and intangible challenges related to a user. Our specific contributions are: (a) to include the most recent survey related to significant privacy and security concern that pose serious challenges in prevailing cloud environment; and (b) trust challenges, potential security threats and privacy issues have been tried to eliminate by analyzing them.

Section 2 has the details of the architecture of Cloud computing framework. Section 3 has detailed discussion on cloud monitoring issues in the environment of cloud computing. Section 4 has the prevailing solutions in the contemporary literature related to Simulation software. Section 5 elaborates the challenges belong to cloud computing security. Section 6 gives light on discussions while the segment 7 completes the desired survey.

II. ARCHITECTURE OF CLOUD COMPUTING FRAMEWORK

Various computing technologies have been integrated under cloud computing so that user can avail the service reliably. To get a better understanding of the security concern introductory perceptions related to the cloud computing has been briefed.

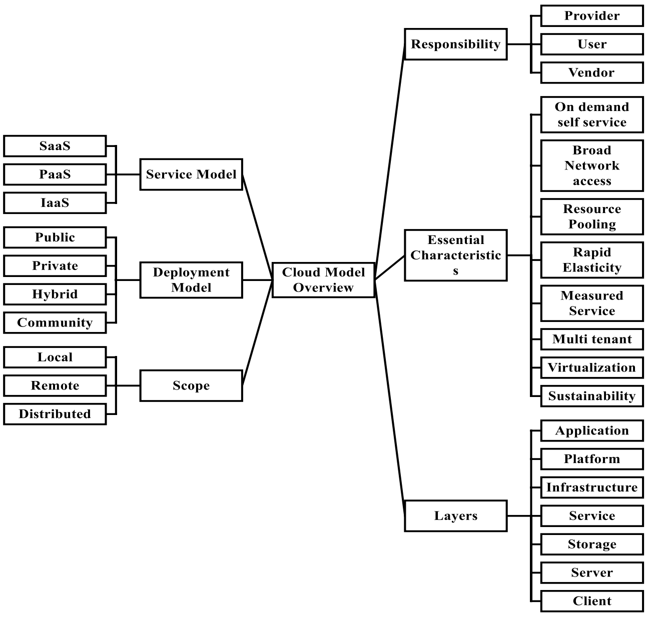

Fig. 2: Cloud Model Overview.

2.1 Cloud computing Layers

2.1.1 Service: A service is a mechanism that is capable of providing one or more functionalities, which is possible to use in compliance with provider-defined restrictions and rules and through an interface (Ellinger, 2013).

2.1.2 Platform: A platform is a fundamental computer system that includes hardware equipment, operating systems, and, in some cases, application development tools and user interfaces on which applications can be deployed and executed.

2.1.3 Infrastructure: It refers to essential physical components needed by a system for demonstrating its functionality. In information systems, these components can contain processors, storage, network equipment, and, in some cases, database management systems and operating systems.

2.2 Cloud computing service models

This model briefly discusses the SPI services commonly termed as SaaS, PaaS and IaaS.

Cloud Service Model		
Software as a Service (SaaS)	**Platform as a Service (PaaS)**	**Infrastructure as a Service (IaaS)**
It is also called SPI - Software, Platform and Infrastructure		

Fig. 3: Cloud Service Model

2.2.1 SaaS: A software or application that is executing on a vendor's infrastructure is recognized as a service provided that the consumer has limited permission to access; this provision is under thin client for sending data and receiving results and this hides the infrastructure of the application provider. Examples belong to this are Google Maps and Salesforce.com.

2.2.2 PaaS: This also known as cloud ware. This includes a platform for development having a set of services to support the design, to test the model, to deploy the application also to monitor and host on the cloud. This contains integrated development environments (IDE) to allow the consumer to develop acquired applications or software and manage their configuration settings.

2.2.3 IaaS: The consumer has developed the required applications and needs only a basic infrastructure. Under this CSP provides infrastructure related to hardware. Provisioned service has been offered to users by the virtualizing network, computing power, and storage. Amazon EC2, Microsoft Azure Platform are the examples of IAAS layer.

2.3 Basic deployment models

This model represents a particular kind of cloud environment, based on ownership, size, and access.

2.3.1 Public cloud: Public cloud allowing sharing of resources among all the customers on the basis of payment according to the resources used. Public cloud belongs to CSP. In this approach, the cloud owner provides public services in the vast majority of cases on the internet based on predefined rules, policies, and a pricing model.

2.3.2 Private cloud: "The cloud under the administration of a mono organization". The physical infrastructure might or might not be owned and administered by the organizational body

2.3.3 Community cloud: Share resources among several organizations by means of customer's community. For example used as the For the purpose of the mission, specific security requirements, specific policy, and considerations etc.

2.3.4 Hybrid cloud: Group of a pair or more different public, private, or community clouds led to the creation of a different cloud model called a hybrid cloud. The participating clouds maintain matchless entity position but share consistent or named technology.

2.4 Fundamental Characteristics

Cloud computing offers services to the end users by integrating different kinds of computing technologies .The fundamental characteristics has been briefly discussed as mentioned below

2.4.1 On-demand self-service- Users get required service by means of CSP management interfaces and Web services

2.4.2 Broad network access-This allows the services, application and data accessibility among the users.

2.4.3 Resource pooling-Allows sharing of resources among users under multi-tenant environment.

2.4.4 Rapid elasticity-According to customer demands scaling of resources are possible.

2.4.5 Measured service-On the basis of scaling of resources usage of service is measured.

2.4.6 Multi-tenancy- a Single resource can be used by multiple users belong to homo or heterogeneous organization.

III. Monitoring of Cloud

Monitoring of Cloud is a most important activity for both Providers and Consumers. This helps in preventing violations and also provides QoS offered through the Cloud.

3.1 The importance of Monitoring of Cloud: To resolve the issues of Cross-Layer Monitoring and network architectures proper monitoring systems are desired. So in this section, Cloud monitoring platforms have been discussed briefly. This can be classified into commercial and open source platform

Table-1: Cloud Monitoring Platform.

Platform used for Cloud Monitoring	
Commercial Platform	**Open Source Platform**
CoudWatch[7]	Nagios[16]
AzureWatch[8]	OpenNebula[17]
CloudCick[9]	CloudStackZenPack[18]
CloudStatus[10]	Nimbus[19]
Nimsoft[11]	PCMONS[20]
Monitis[12]	DARGOS[21]
LogicMonitor[13]	
Aneka[14]	
GroundWork[15]	

3.1.1 CloudWatch: It is a monitoring service which focuses on virtual platforms. Different kinds of monitoring information are gathered by CloudWatch and this information is stored for approximately two weeks.

3.1.2 Azure Watch: To monitor applications Windows Azure SDK proposed a specific software library and key performance metrics is being monitored with the help of Azure resources

3.1.3 Cloud Kick: It is a duplet-Cloud management platform having a moderate level of monitoring features and metrics. It has monitoring and configuring capability with alert systems to inform users in real.

3.1.4 Cloud Status: Cloud Status [10] is first independent monitoring service which supports AWS and Google App Engine. It monitors application performance of user providing the trends of monitored metrics.

3.1.5 Nimsoft: It has a capability of monitoring private and public Clouds including SLAs [12] belong to data centers. Its main feature is completeness and scalability.

3.1.6 Monitis: Resources monitoring [12] is accomplished using agents and informs consumers related to the performance by means of sending alerts. For customization of a platform, it deals with an API based on HTTP REST protocol.

3.1.7 Logic Monitor: Logic Monitor [13] is used for monitoring virtualized infrastructures with the help of an elastic multi-layer approach. It supports several environments under virtualization for example Citrix Xen-Server, VMware vSphere [22] and Cloud platform etc.

3.1.8 Aneka: Aneka [66, 23] is useful in developing, deploying and managing Cloud applications including monitoring by means of an extensible API. It has the basic services for system monitoring in addition to others. Aneka Clouds provide an assembly of services to interact with the Cloud having monitoring functionality implementing in this framework.

3.1.9 GroundWork: With the help of GroundWork [15] any devices or virtual object or even servers and security devices can be easily monitored. This monitoring is applicable for the infrastructure and applications available in the virtual or physical environment.

3.2 Platforms related to open source

The program which allows the user to use or modify the source code free of charge comes under the category of open source. In this programmers can modify the source code and share the changes with the community.

Following are the open source platforms related to cloud.

3.2.1 Nagios: Nagios [16] belongs to open source monitoring platform for Cloud infrastructures and capable to monitor virtual instances and repository services focusing on Extensibility.

3.2.2 OpenNebula: OpenNebula [17, 24] is toolkit which performs monitoring by means of a module called Information Manager to provide information to Cloud Providers.

3.2.3 CloudStack ZenPack: CloudStack by means of a Zenoss extension called ZenPack [25] monitors virtual and physical devices. XenServer, KVM, and Xen Cloud Platform have the compatibility with it. Timeliness is its main feature.

3.2.4 Nimbus: It is a tool for implementing infrastructure Clouds. Cloudinit.d and Context Broker related to this group.

3.2.5 PCMONS: The Private Cloud Monitoring System [20] is a tool to manage and monitor cloud. It consists of 7 modules as Node Information Gatherer, Cluster Data Integrator, Monitoring Data Integrator, VM Monitor, Configuration Generator, Monitoring Tool Server and User Interface.

3.2.6. DARGOS: DARGOS [21] is helpful to circulate resource monitoring information. It consists of Node Monitoring Agent (NMA) and Node Supervisor Agent (NSA).

IV. CLOUD SIMULATION SOFTWARE

Cloud testing as a Service "TaaS" is used for testing cloud-based web applications by simulated real-world web traffic. This includes for security, stress, load, performance, and interoperability. CloudSim, GreenCloud, NetworkCloudSim, CloudAnalyst, EMUSIM, SPECI, GROUDSIM, and DCSim etc. have been developed for performance analysis.

4.1 CloudSim: Extensible simulation framework used for simulation, modeling and experiment of infrastructures and application services belong to a cloud.

4.1.2 GreenCloud: The researchers can interact, observe and measure cloud performance using this.

4.1.2 NetworkCloudSim: It is an extended version of CloudSim, which is capable of implementing network layer in CloudSim, by reading BRITE file it can generate a topological network. It provides topology file which contains a number of nodes with different entities required in simulation [26]. In NetworkCloudSim [27], network CloudSim works properly as every entity is mapped to single BRITE node.

4.1.3 CloudAnalyst: This simulator is able to examine the behavior of large-scale Cloud applications having various deployment configurations and separating the simulation experimentation easily.

4.1.4 EMUSIM: It is a unified architecture to share service's behavior on cloud platforms.

4.1.5 SPECI: It is termed as Simulation Program for Elastic Cloud Infrastructure. Various aspects of scalability and performance of future data centers are analyzed by SPECI. It is assumed that when a size of data centers increases, then they do so in non-linear fashion, so it is required to analyze the behavior of such data centers.

4.1.6 GroudSim: It is event based simulator focusing IaaS but also able to support PaaS, or cloud storage [28].

4.1.7 DCSim: Its main aim is to simulate a data center hosting an Infrastructure as a Service cloud. DCSim is mainly focusing on virtualized data centers.

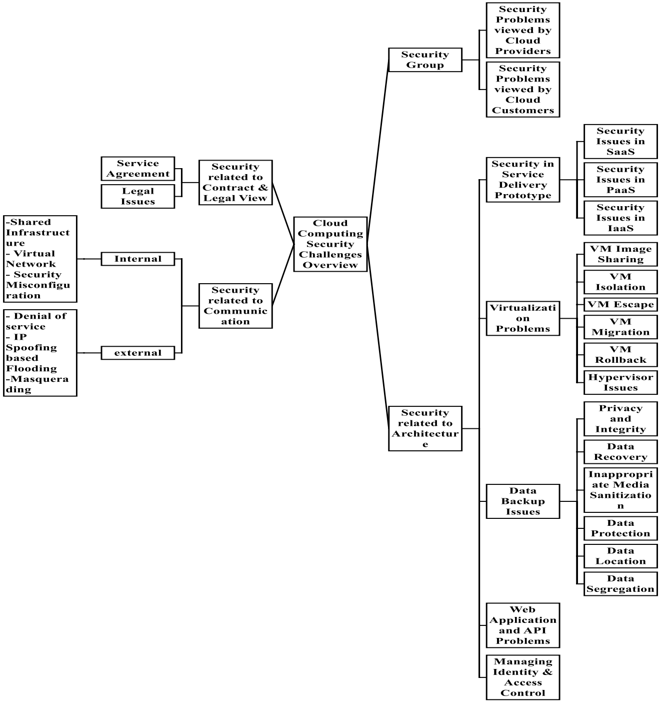
Security Problems viewed by Cloud Providers
Security Problems viewed by Cloud Customers
Security Group
Security Issues in SaaS
Security Issues in PaaS
Security Issues in IaaS
Service Agreement
Legal Issues
Security related to Contract & Legal View
Security in Service Delivery Prototype
Cloud Computing Security Challenges Overview
-Shared Infrastructure - Virtual Network - Security Misconfiguration
Internal
VM Image Sharing
VM Isolation
VM Escape
VM Migration
VM Rollback
Hypervisor Issues
Virtualization Problems
Security related to Communication
- Denial of service - IP Spoofing based Flooding -Masquerading
external
Security related to Architecture
Privacy and Integrity
Data Recovery
Inappropriate Media Sanitization
Data Protection
Data Location
Data Segregation
Data Backup Issues
Web Application and API Problems
Managing Identity & Access Control

Fig. 4: Cloud Security Challenges.

After reviewing the previous related works Jeffery et al. [5] and others a modified framework to visualize security detail of a cloud system has been shown in Fig-4. Main aspects are Security groups, Security related to architecture, Security related to communication, Security related to contract and Legal view.

V. THE CHALLENGES BELONG TO CLOUD SECURITY

With the help of multi-tenancy and virtualization techniques resource pooling permits various users to use the same pool but because of this some risk in the system also been introduced. The data might be visible to other users and also tracing of operation is possible. Management interface might be accessed without authorization as compared to the traditional system. Virtual machines (VM) and VM escape can generate malicious cooperation. Also, SaaS applications depend on PaaS and PaaS is depending on IaaS. The service model is operationally dependent which causes security challenges. Cloud specific susceptibilities and threats are more probable in the case of public, community and hybrid cloud because third party [29] has the administration of control for the different user's group. This needs more advanced security patterns.

5.1 Communication level challenges

With the help of internet cloud service are made accessible to the users. Data or application transmission take place between the customer and the cloud. The cloud has the internal communication between VMs.

Communication of cloud can be divided between customer and cloud (external communication) as well as within cloud (internal communication).

The challenges possessed due to external communication are the denial of service, IP Spoofing based flooding, and masquerading [30]. This can be resolved with the help of Internet Security Protocol (IPsec), algorithms of cryptography, Secure Socket Layer (SSL), detecting of Intrusion and preventive systems, cleaning of data movement, and by digital authentication mechanism using certificates [30].

5.2 Infrastructure level challenges

Allocation of network infrastructure components [31] and computational and storage resources respectively have been managed by resource pooling. Cross-tenant attack [32] is probably by dint of allocation of network infrastructure components. The IaaS service model can be affected by resource pooling characteristic of the cloud computing. There is no proper management of IP-based segregation of network and also it has not been associated with a specific group of users. Users have been allowed to manage their VMs [33] on the cloud by a role of super-user access. By dint of this permission, a user can get system IP or MAC address. IaaS network interfaces can be maliciously handled by the user and can introduce sniffing and spoofing attack over the network infrastructure.

5.2.1.1 Issues of Virtualization

Several customers can use the same physical resource under virtualization. Each user has a separate VM to provide an operating machine to the user. The same physical resources have been mapped to the several VMs to allow the resource pooling under the environment of multi-tenancy. Numerous operating systems can run concurrently on the same machine using VM monitor (VMM) or hypervisor. This leads security threats to the users under the cloud environment.

Under VM image sharing user can upload and download images from the repository.VM images sharing from the repositories can lead a serious risk if images having a malware can be uploaded by the user [34]. This can introduce malware in the cloud environment. Under VM isolation different VMS have the logical isolation, even though when user access the same physical resources there is a possibility of data breach and cross-VM attacks.

Under VM escape when a malicious user can be able to bypass hypervisor, called VM escape [35].Under this attacker can get access to other VMs and make this down [34] and also can be able to get access to hardware storage. This is a major threat. When transferring VM from one physical device to other under running state is termed as VM migration. This can cause the data privacy and integrity concerns.VM can be rollbacked to the previous state according to need under virtualization. But this rollback facility can give rise to vulnerability [36].

Hypervisor/VMM is responsible for generating, isolate and manage virtual resources. Attackers can bypass security restrictions because of the bugs in the VMM. When a host system has an increasing number of VMs and most of them are in an idle state after instantiation, this situation is termed as VM sprawl which causes the resource wastage of the host system.

5.2.1.2 Challenges for Virtual network

A physical network having a logical network fabricated on itself is termed as Virtual Network which allows communication between VMs. The current technique Intrusion detection and prevention mechanisms are not significantly efficient to monitor traffic over it causing serious threats for the VMs. DoS attack, spoofing and sniffing threats cannot be successfully checked by it. The risk to stop leak has not been effectively managed by cryptographic keys to prevent sniffing and spoofing occurring on a virtual network [37] as a result the data under transmission posed by serious threats.

5.2.1.3. Data/storage issues:

The management of servers and data are being taken care by the service providers under an environment of a cloud. VMs can be controlled by a user with certain levels only [38]. There can be a threat related to data security. The risk regarding the privacy and accessibility of data under the cloud environment as compared to a conventional model of computing is more [28].The data belong to a user can be accessed in an unauthorized way if one succeed to attack an individual entity. Because of this the data under process in addition to the data keep on hold come under the security threats [39].Further due to multitenancy malicious users might successfully attack the data belong to other users during the phase of processing [12]. Because of the lack of advance technique for managing the standard key to secure the cloud, standard mechanism of cryptography cannot be used for the model of cloud computing for better scaling [11].Therefore the cryptographic domain also enriches the major security concern belong to the data.

The users have been provided dynamic and on-demand provision of resources by the cloud by means of resource pooling. The resource sharing for a specific user can be allocated to a different user in the next span of time. By means of data recovery techniques, a malicious users can access the data belong to other users [33,41].So the sensitive data related to the user have major security threats under this prevailing condition which gives rise to data retrieval vulnerability. If the storage devices have not been properly destructed this comes under improper media sanitization. Because of improper sanitization by the CSP, the data can be visible to security risk [27].Multitenancy also causes device sanitization issues.

CSP must maintain the backup storage so that data can be retrieved easily under the adverse situation. In order to secure from accessing unauthorized way and tampering of data the backup storage must be protected nicely [42].Customer data separation is termed as Data segregation. Data leak prevention (DLP) mechanism has been used by cloud service provider to prevent unauthorized access in case data segregation fails.

5.2.1.3.1 Solutions to Data Security Challenges:

Information security optimum solution can be obtained using Encryption. In order to manage access related to cloud computing distributed access control architecture can be employed to get the best result. To protect data privacy of computational task to cloud server fine-grained access control mechanism can be used. For computing large files having different sizes addressing remote data security RSA security techniques can give the best result. To protect unauthorized data access use of appropriate key management techniques can resolve the issue.

5.2.1.4 The security concern belong to application programming interface (API) and Web application:

APIs are responsible for bridging among the users and the services in the environment of a cloud. The securing management and accessibility belong to the services of a cloud have been highly influenced by APIs security [36].The secured APIs is responsible for providing the access to cloud services protecting from a malicious user.

By means of APIs, the users can create or enhance the services [36]. APIs have been published by the CSP for marketing the features of their cloud. This ease the consumers to see the specific constituents and functioning belong to the cloud. But at the same time, cloud architecture might have been exposed to the attackers in some other way [36]. Therefore, insecurity of the APIs can be wearisome for both. The vulnerability of APIs causes pathetic security concerns in the applications [43].

5.2.1.5 Managing identity and access control:

The privacy and reliability of data, as well as services, is interrelated with the authentication management and accessing mechanism in the cloud scenario. The identity of a user and protecting the information from unauthorized access is remarkably significant [44].Weak identification management and access mechanism give rise to many security concern as denial of service , inadequate authorization verification, validation across a domain, and griddling attacks related to XML.

5.3 Contractual and legal levels challenges:

Putting the data as well as applications related to the organization under the control of CSP administrator causes many security issues like performance guarantee, Laws of regulation conformity, geographic rules, supervision of contractual induction etc. These are the challenging legitimacies.

5.3.1. Legal issues:

One of the main reason of jurisdiction conflict is an availability of CSP resources in various geographical location[45].When the data has been migrated between the locations having different laws, the configuration of security policy compliance is more difficult with new legitimate rules. Other user's confidentiality might be breached under this case [4, 46].

Table-2: Counter measure of Cloud security challenges.

Comparative study for the countermeasure of Cloud security challenges			
Work	**Counter Measure**	**Proposed Scheme**	**Features**
	Communication issues in cloud		
[47]		Architecture to monitor VM integrity and infrastructure constituents	Safeguards network and component of infrastructure, avoid cross VM attack
[48]		Virtual network security Application	Protects Virtual Networks, virtual VM as well as Network Isolation ,sniffing and spoofing safeguard
[49]		intrusion prevention application	Safeguards against intrusion
VM issues in cloud			
[50]		VM image management system	Protects from illegal accessing control, data removal and malware protection
[52]		Privacy and integrity of VM images	Protects from unauthorized accessing control
[53]		HyperCoffer	Protects against VM rollback
[54]		Scheme related to VM migration mechanism	Secures and trustful preserving maintaining privacy and integrity
[66]		Scheme for VM migration based on VMTP Protocol	Maintains privacy and integrity
[51]		Model for security context and migration of VM	Maintains privacy and integrity

[56]		HyperCheck, an Integrity monitor tool.	Provides security against rootkit DoS and evasion attacks maintaining low scalability.
[55]		SplitVisor	Protects VM and securing it from VM hoping and useless migrations maintaining medium scalability
Storage issues in cloud			
[67]		SecCloud	For storage security and privacy having medium scalability. It also supports computational audit.
[57]		FADE	Data privacy and integrity which has high scalability and provide assured deletion
[58]		TimePRE	Secures data sharing in cloud
[54]		Access management for cloud application	For Authentication, Authorization and Accounting
[59]		Cloud application integrity scheme	Provides application Integrity and platform integrity
[60]		API management platform	Secures cloud APIs for Access control
Managing Credential and administration of accessing strategies			
[61]		HASBE (Hierarchical Attribute-Set-Based Encryption)	Accessing control technique for cloud storage
[62]		Role based accessing scheme	Allows access of cloud resources on the basis of role
[66]		SPICE identity management framework	Maintains Group Signature
[63]		Identity management framework	Provides Authentication and Access administration
[64]		Framework related to reaction for change in security at runtime	Provides monitoring and enforcement
[65]		SPECS	SLA based approach for maintaining negotiation monitoring and enforcement

VI. Discussions

The above-mentioned issues discussed related to security elaborates conventional security concerns as well as the novel issues pertaining to the cloud by means of new technologies and practices. Data secrecy, application services as well as networking and communication belong to conventional issues. Virtualization, multi-tenancy, and shared resource pooling is the root cause of novel issues. For monitoring the traffic passing through a virtual network a strategy is needed to protect from malicious information flow. Still, there are certain open issues even after intensive research efforts that need proper attention to provide a secure cloud environment. The most important one is developing a compact security arrangement that meets all required security concern related to cloud. At the bottom level, for obtaining the required security solution it is mandatory to get a system for harmonizing different security solution. Using shared pool unauthorized access can be checked but due to dynamic nature of the resource and heterogeneous nature of services access control system becomes more complex. There is a procedure to map the identity of the organization to the cloud and it needs some time for translating this identity related to a cloud that affects the security and access control. In addition to this, we need an integrated tool for auditing and assurance to ensure better policy arrangement among various concerned entities.Multi-tenancy has been used for optimization of resource utilization but one of the major threat posed to the cloud is by the multi-tenancy itself which need to be fixed. The conflict related to SLA and their integration with legal concern is still not fully resolved. The issues related to audit still requires more work to confirm whether service level is encountered as it has been guaranteed in SLA or not. The customers want to switch their digital resource for many reasons over the cloud. However, this migration is not a simple task. It requires standard formats and protocols to assist customer during migration of data and application. In this perspective to avoid insider attacks identification of indicators becomes important to research area. The classification technique to find the standard and malicious user related to the cloud come under the new area of research. Although both the users and CSPs have the advantage of security solutions, but this lead to computation performance and pricing issue. The balance between the security needs, performance and cost must be maintained for finding security solutions. We have performed careful analysis related to cloud monitoring and their main activities concerning the security. The main platform including commercial and open source and its related service to indicate how they relate to such issues. The work in these areas will highly appreciable for helping them in order to accomplish quantifiable and practical analysis and provide the best option before migration of data on the cloud.

Conclusions

Though cloud computing has multiple advantages but the security concerns hamper the user to adopt it fastly.It is well-known facts for all users regarding the security threats prevailing in the cloud. Various users can be able to share same physical resources by means of multi-tenancy and virtualization. But this leads to cloud specific threats. Various legal issues arise related to users data and application because of the geographical extent of cloud computing. Owner organization has the limited administrative control because of this managing identity and accessing control belong to a digital resource of the organization have distinguishing forms in cloud computing.

The security threats which comes under sharing, virtualization, and public cloud have been elaborated and subsequent techniques have been presented as a counter measure. The security service scope has been specifically highlighted in the present analysis delivered by enriched techniques. The above-mentioned discussion makes light on related issues and further motivating the research community for future work.

REFERENCES

[1] Paquette S et al (2010), Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly; 27(3), pp. 245–253.

[2] Subashini S et al (2011), A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications; 34(1), pp. 1–11.

[3] Vaquero L M et al (2011), a survey on IaaS cloud security. Computing; 91(1), pp. 93–118.

[4] Takabi H et al (2010), Security and privacy challenges in cloud computing environments. IEEE Security & Privacy; 8(6), pp.24–31.

[5] Tchifilionova V (2011), Security and privacy implications of cloud computing - Lost in the cloud. Proceedings of the IFIP WG

[6] C.Vecchiola et al (2009) a software platform for NET based cloud computing, in: W. Gentzsch, L. Grandinetti, G. Joubert (Eds.), High Speed and Large Scale Scientific Computing, IOS, pp. 267–295.

[7] http://awsdocs.s3.amazonaws.com/AmazonCloudWatch/latest/acw-dg.pdf

[8] http://www.paraleap.com/azurewatch

[9] http://www.cloudkick.com/home

[10] S. Ruj et al (2014), Decentralized access control with anonymous authentication of data stored in clouds, IEEE Trans. Parallel Distrib. Syst. 25 (2), pp. 384–394

[11] http://www.nimsoft.com/solutions/nimsoft-monitor/cloud.

[12] http://portal.monitis.com/.

[13] http://www.logicmonitor.com/monitoring/storage/netapp-filers/.

[14] http://www.manjrasoft.com/

[15] http://www.gwos.com/features/.

[16] http://nagios.sourceforge.net/docs/nagioscore-3-en.pdf.

[17] http://opennebula.org/documentation:archives:rel2.0:img

[18] http://www.cloudstack.org/.

[19] http://www.nimbusproject.org/.

[20] S.A. Chaves et al (2011), toward an architecture for monitoring private clouds, IEEE Communications Magazine 49 (2011), pp. 130–137

[21] A. Corradi et al (2012) , DDS-enabled Cloud management support for fast task offloading, Computers and Communications (ISCC), 2012 IEEE Symposium on, 1–4 July 2012, pp. 67–74.

[22] http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html.

[23] http://www.manjrasoft.com/.

[24] http://en.wikipedia.org/wiki/OpenNebula

[25] https://github.com/zenoss/ZenPacks.zenoss.CloudStack.

[26] R. Calheiros et al (2013), CloudSim: a novel framework for modeling and simulation of cloud computing infrastructures and services. ArXiv: 0903 - 2525.

[27] A. Nunez et al (2012), iCanCloud: a flexible and scalable cloud infrastructure simulator, Journal of Grid Computing 10 (1), pp. 185–209

[28] S. Islam et al(2012), How a consumer can measure elasticity for cloud platforms, in: Proceedings of the 3rd Joint WOSP/SIPEW International Conference on Performance Engineering, ICPE ’12, Boston, Massachusetts, USA, 2012, pp. 85–96.

[29] B. Guan et al (2014), CIVSched: a communication-aware inter-VM scheduling technique for decreased network latency between collocated VMs, IEEE Trans. Cloud Comput. 2 (3), pp. 320–332.

[30] Sangroya A et al (2010), towards analyzing data security risks in cloud computing environments. Communications in Computer and Information Science; 54, pp. 255–265.

[31] R. Chandramouli et al (2014), Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, pp. 1–30. doi: 10.1007/978-1-4614-9278-8_1.

[32] K. Hashizume et al (2013), an analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) , pp. 1–13

[33] K. Bilal et al (2014), Trends and challenges in cloud data centers, IEEE Cloud Comput. Mag. 1 (1), pp. 10–20.

[34] D. AB. Fernandes et al (2014), Security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (2), pp. 113–170.

[35] M.H. Song (2014), Analysis of risks for virtualization technology, in: Applied Mechanics and Materials, vol. 539, pp. 374–377

[36] H. Wu et al (2010), Network security for virtual machine in cloud computing, in: 5th International Conference on Computer Sciences and Convergence Information Technology, pp. 18–21.

[37] H. Van et al (2010), Performance and power management for cloud infrastructures, in: Proceedings of the 3rd International Conference on Cloud Computing, IEEE, Miami, FL, USA, pp. 329–336

[38] L. Wei et al (2014), Security and privacy for storage and computation in cloud computing, Inform. Sci. 258, pp. 371–386.

[39] M. Sookhak et al (2014), a review on remote data auditing in single cloud server: taxonomy and open issues, J. Netw. Comput. Appl. 43, pp. 121–141.

[40] W. Liu et al (2014), Security-aware intermediate data placement strategy in scientific cloud workflows, Knowl. Inform. Syst. 41 (2), ,pp. 423–447

[41] W.A. Jansen et al (2011), Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), pp. 1–10.

[42] S. Subashini et al (2011), A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1), pp. 1–11.

[43] S. Carlin et al (2011), Cloud computing security, Int. J. Ambient Comput. Intell. 3 (1), pp. 14–19.

[44] B. Liu et al (2014), Information fusion in a cloud computing era: a systems-level perspective, IEEE Aerospace Electron. Syst. Mag. 29 (10), pp. 16–24.

[45] B. Hay et al (2011), Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, and pp. 1–7.

[46] N. Gonzalez et al (2012), A quantitative analysis of current security concerns and solutions for cloud computing, J. Cloud Comput. 1 (1), pp. 1–18.

[47] F. Lombardi et al (2011), secure virtualization for cloud computing, J. Netw. Comput. Appl. 34 (4), pp. 1113–1122.

[48] J. Li et al (2012), Cyber-guarder: a virtualization security assurance architecture for green cloud computing, Future Gener. Comput. Syst. 28 (2), 379–390.

[49] T. Xing et al (2013), an OpenFlow-based intrusion prevention system in cloud environment, in: IEEE Research and Educational Experiment Workshop, pp. 89–92.

[50] J. Wei et al (2009), Managing security of virtual machine images in a cloud environment, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 91–96

[51] Z. Tavakoli et al (2012), a framework for security context migration in a firewall secured virtual machine environment, in: Information and Communication Technologies, Springer, Berlin, Heidelberg, pp. 41–51

[52] M. Kazim et al (2013), securing the virtual machine images in cloud computing, in: Proceedings of the ACM 6th International Conference on Security of Info and Networks, pp. 425–428

[53] Y. Xia et al (2013), Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks, in: IEEE 19th International Symposium on High Performance Computer Architecture, pp. 246–257.

[54] M. Aslam et al (2012), Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 869–876.

[55] W. Pan et al (2012), Improving virtualization security by splitting hypervisor into smaller components, in: Data and Applications Security and Privacy XXVI, Springer, Berlin, Heidelberg, pp. 298–313

[56] F. Zhang et al (2015), HyperCheck: a hardware-assisted integrity monitor, IEEE Trans. Dependable Sec. Comput. (2013), M. Ali et al. / Information Sciences , pp. 305, 357–383 383

[57] Y. Tang et al (2012), secure overlay cloud storage with access control and assured deletion, IEEE Trans. Dependable Secure Comput. 9 (6), pp. 903–916.

[58] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Inform. Sci. 258 (2014), pp. 355–370.

[59] O.D. Alowolodu et al (2013), Elliptic curve cryptography for securing cloud computing applications, Int. J. Comput. Appl. 66

[60] M.Y. Wu et al (2013), Design and implementation of cloud API access control based on OAuth, in: IEEE TENCON Spring Conference, pp. 485–489.

[61] Z. Wan et al (2012), HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inform. Forensics Sec. 7 (2), pp. 743–754.

[62] S. Yang et al (2013), Design role-based multi-tenancy access control scheme for cloud services, in: IEEE International Symposium on Biometrics and Security Technologies (ISBAST), pp. 273–279.

[63] R.D. Dhungana et al (2013), Identity management framework for cloud networking infrastructure, in: IEEE International Conference on Innovations in Information Technology (IIT), pp. 13–17.

[64] M.L. Hale et al (2012), Risk propagation of security SLAs in the cloud, in: IEEE Globecom Workshops (GC Wkshps), pp. 730–735.

[65] M. Rak, N. Suri et al (2013), Security as a service using an SLA-based approach via SPECS, in: IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2,pp. 1–6.

[66] B. Danev et al (2011), Enabling secure VM-vTMP migration in private clouds, in: Proceedings of the ACM 27th Annual Computer Security Applications Conference, pp. 187–196.

[67] L. Wei et al (2014), Security and privacy for storage and computation in cloud computing, Inform. Sci. 258, pp. 371–386".