Journal of Network and Computer Applications 79 (2017) 88–115

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Cloud security issues and challenges: A survey

Ashish Singh*, Kakali Chatterjee

Department of Computer Science & Engineering, National Institute of Technology Patna 800005, Bihar, India

ARTICLE INFO

Keywords:
Cloud computing
Cloud framework
Cloud security
Cloud security challenges
Cloud security issues

ABSTRACT

The cloud computing provides on demand services over the Internet with the help of a large amount of virtual storage. 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. 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. Due to the availability of its services & scalability for computing processes individual users and organizations transfer their application, data and services to the cloud storage server. Regardless of its advantages, the transformation of local computing to remote computing has brought many security issues and challenges for both consumer and provider. Many cloud services are provided by the trusted third party which arises new security threats. The cloud provider provides its services through the Internet and uses many web technologies that arise new security issues. This paper discussed about the basic features of the cloud computing, security issues, threats and their solutions. Additionally, the paper describes several key topics related to the cloud, namely cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, threats, and attacks. The paper also discusses a lot of open research issues related to the cloud security.

1. Introduction

In the history, computer would take enough space like a room with extravagant electronics parts as network devices, processor to generate less processing output, consuming as much power as compared to the modern computer. Nowadays, those enough spaces are replaced by small hard drives and expensive electronics parts replaces by economical network devices. This enhancement of processing power and infrastructure nodes can be originate a large distributed system that merges a large number of resources in a unit, that support highly exhausting computation like scientific simulations.

The two well known components for a distributed system are clusters and grids (Stanoevska-Slabeva et al., 2009). Clusters and grids both are different approaches. The cluster model supports coupling of homogeneous networks, whereas grids is the design for large distributed and heterogeneous networks. The cluster model is more expensive due to costly central processing unit such as parallel supercomputers. Standalone resources such as desktop computers is connected by the middle-ware like MPICH and it is a cheaper approach. The grid is most commonly architecture used by the desktop and home users for making servant computational nodes and it is created over the Internet. The Large Hadron Collider (LHC) computing grid of the CERN is a good example of such grid. The main disadvantage of grid computing is to it increased management and task assignment complexity and create the interference at result gathering time.

When any electric appliance is plugged into a channel, we think neither how electric power is generated nor how it passes into the channel. This phenomena is possible because the electricity is virtualized. This power is available from a wall socket, but it hides power generation station and large distributed grid. When researcher extends information technology, this concept is the base for their research means delivering useful data and services in which user does not know their internals works. The computational environment is considered as completely virtualized.

Based on the above phenomena first introduce cluster, then the grid and now cloud computing has developed in the year 2008 as a new distributed computing model with the aimed of attaining the computing as a utility. The computing as a utility term first introduces by Corbato and Vyssotsky in 1965, provide a business model for on demand transmission of computing resources, that is based on pay-as-you-go manner means customers get to choose whatever resources (platforms, security policies, CPUs, memory, bandwidth, and hardware load) they require, as like public user obtain services from traditional public utility services such as water, electricity, gas, and telephone. The new paradigms aimed is providing a huge amount of computing power in a completely virtualized manner, by combining all computing

* Corresponding author.
E-mail addresses: ashish.cse15@nitp.ac.in (A. Singh), kakali@nitp.ac.in (K. Chatterjee).

http://dx.doi.org/10.1016/j.jnca.2016.11.027
Received 15 August 2016; Received in revised form 3 November 2016; Accepted 27 November 2016
Available online 30 November 2016
1084-8045/

Table 1
Comparison of the related work with the survey based on the cloud overview, cloud automation, security requirements, cloud trust, Cloud security (abstraction, threats & attacks), Cloud security issues, Security solutions, and Open issues.

Survey paper	Year	Topic discussed	Cloud overview	Cloud automation	Security requirements	Cloud trust	Cloud security (abstraction, threats & attacks)	Cloud security issues	Security solutions	Open issues
Takabi et al. (2010)	2010	Virtualization, trust management, secure service management, security & privacy	–	X	X	✓	–	–	X	X
Zhou et al. (2010)	2010	Security requirements (availability, confidentiality, integrity, control, and audit), privacy	–	X	✓	X	X	X	X	X
Grobauer et al. (2011)	2011	Cloud specific vulnerability, cloud risk, authentication, authorization, and access control	–	–	–	X	X	–	X	X
Vaquero et al. (2011)	2011	IaaS cloud security, cloud threats and attacks, VMM security	X	X	X	–	✓	–	–	X
Behl (2011)	2011	Cloud security issues, cloud security challenges	–	X	X	X	X	–	X	✓
Zissis and Lekkas (2012)	2012	Cloud trust, cryptographic method for security, security requirements, trusted third party authentication, certification based authorization	–	X	✓	✓	–	X	X	X
Modi et al. (2013a)	2013	Cloud threats and attacks, security issues at different layer, authentication and virtualization security issues	X	X	✓	✓	✓	–	–	✓
Oktay and Sahingoz (2013)	2013	Cloud security attacks, Intrusion detection system, intrusion prevention system	✓	X	X	X	✓	X	X	X
Fernandes et al. (2014)	2014	Cloud concept and technologies, cloud security issues	✓	✓	✓	✓	X	✓	X	✓
Abbas and Khan (2014)	2014	Cloud security requirements, privacy persevering approaches, open research issues in E–health cloud	X	X	✓	X	X	X	X	✓
Ali et al. (2015)	2015	Cloud computing overview, cloud security issues, cloud security solutions, security issues in mobile cloud computing	✓	X	X	–	–	–	–	✓
Tari et al. (2015)	2015	Security issues present in public and private clouds, service availability, access control, multi–tenant services, identity and data protection	X	X	X	X	–	–	–	X
This survey		**Cloud overview, cloud technologies, cloud security requirements, cloud trust, Cloud security (abstraction, threats & attacks), cloud security issues and their solutions, future research directions**	✓	✓	✓	✓	✓	✓	✓	✓

The "–" symbol denote the less discussion on respective aspect. The "✓" and "X" symbol denote the specific domain is covered and domain is not covered with respect to given aspect respectively.

resources and services in a single system. The cloud computing environment with the virtualization concept fulfills these requirements. So, it is accepted by the National Institute of Standards and Technology (NIST). This NIST community defines a cloud deployment models include public, private, hybrid, and community cloud (NIST, 2015). It also discuss essential characteristic such as broad network access, rapid elasticity, measured services, on demand self service and resource pooling. Finally, talks about service delivery models consist of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

The cloud computing is addressing many solutions in a protected view. Although this point of time cloud features is understood very well, especially from a business point of view. But, this feature includes some security faults that are yet a challenging issue in cloud environment. Day by day cloud computing is in growth as many organizations adopted the cloud technology, but parallel several security issues are raised. Each organization chooses a secure infrastructures when they move its data to remote locations. According to the NIST security, portability and interoperability are the major obstacle to adoption of cloud computing. In 2009, many firms give their opinions and concern more about the cloud security issues. The International Data Corporation (IDC) is a market research and analysis firm gives their suggestions to company Chief Information Officers (CIOs) on the most vulnerable security issues. The survey results clearly say that 87.5% of the survey notice that the security field as a top priority. In the cloud environment, many risks are involved for storage of the sensitive data, hence many organizations hesitate to transfer their sensitive data to remote storage clouds (Armbrust et al., 2009).

The cloud used virtual environment to attain multi-tenancy. Virtual machine contains vulnerabilities that introduce explicit threat to the security and privacy of the cloud services. The other factor of cloud services are online and data migration over the Internet. Many security vulnerabilities are present at the browser Application Program Interface (API) and in the network channel. The cloud resources are distributed and shared among multiple users by the use of multi-tenancy concept. This concept is a barrier to establish a security architecture that completely protect the data and services. Due to transparency issues, the cloud service provider resists its users to implement security monitor or intrusion detection systems into the management service layer at the rear of virtualized cloud environment. When data is stored in the remote storage, cloud user looses the control over the data, at this time consumers may not be conscious the details security policies, vulnerability and malware information. For example, an attacker may achieve the cloud data by applying back channel attack and fix a kernel level rootkit. The community also knows about the physical level attacks such as reading the cloud stored data.

For achieving the high level security and privacy of related data and services, cloud service provider settles a Service Level Agreement (SLA) to the cloud consumers. But, unfortunately there is no standard procedure to design an SLA. The paper (Kandukuri et al., 2009) describe an SLA report related to the provided services, which is helpful for consumers and provider both. But, these SLA reports do not completely fulfill the consumer losses. Many cloud providers like Google, Amazon (2015), and SalesForce does not give full SLA to guarantee that its user data is fully secure and it hides many other parameters related to the service. The best example is- Amazon Elastic Cloud Computing (EC2) (Amazon, 2015) implements the abstraction of virtual hardware to its consumers, included all types of related failures like a hardware node failure, software node failure and operator node failure. In forthcoming, the researcher made an SLA based Google App Engine (Google, 2015) that handles all cases of failure.

From the existing literature survey (discussed in Section 2.), we have found the detail discussion on different security issues and challenges of cloud computing in Ali et al. (2015), Fernandes et al. (2014), Hashizume et al. (2013), Modi et al. (2013a), Rong et al. (2013), Xiao and Xiao (2013), security and privacy of the cloud service provider in Abbas and Khan (2014), Ahuja and Komathukattil (2012), Subashini and Kavitha (2011), Zhou et al. (2010), virtualization security problems of the cloud computing in Pearce et al. (2013), Perez-Botero et al. (2013), Vaquero et al. (2011), and cloud data storage security issues in Aguiar et al. (2014), Kulkarni et al. (2012). But, there is a lack of discussion between the security issues and their solutions in the above mentioned papers. Also, some of the papers (Oktay and Sahingoz, 2013; Takabi et al., 2010; Zhou et al., 2010; Zissis and Lekkas, 2012) does not focus on open issues present in the cloud and some papers (Ali et al., 2015; Oktay and Sahingoz, 2013; Tari et al., 2015; Zhou et al., 2010; Zissis and Lekkas, 2012) does not focus on cloud security threats and attacks.

Thus, the contribution of this survey paper with respect to other studies are presented in Table 1 using different symbols with different meaning. The survey paper provides a comprehensive study of different security issues and its solutions, which we have mentioned in the subsequent summary table in each subsection. Also, the paper provides extensive discussion of cloud security threats, the attack and its solutions. From the analysis of several security issues discussed in the survey, some open issues are coming out for further research.

The rest of the paper is categorized as follows. Section 2 are concerned about the related work and elaborates the contribution of many other papers. The discussion topic in Section 3 is a general view of cloud computing and some general models related to cloud. The next Section, 4 presents detail study of cloud technologies. The next Section 5 discussed about cloud security concepts. Section 6 elaborate cloud security issues and their solutions. In Section 7 of this survey discussed some open issues present in the cloud. Finally, this survey is closed with the conclusion in Section 8.

2. Related work

The security paradigm is most widely discussed area in both industry person and researcher. The European Conference, ACM Workshop on Cloud Computing Security, the International Conference on Cloud Security Management are some international conferences that only focus on cloud security. Also, there are several international journals for cloud security. In this section, several survey papers are included which is the best of our knowledge.

The paper (Ali et al., 2015) elaborate a compressive survey on cloud architecture, current security challenges. The author mainly focuses on the current cloud security issues. The study overview various security issues, including communication security issue, architectural security issue, and Compliance and legal security issue. But, in this paper we found only three types of cloud security issues. This paper also mentioned how authentication, authorization, integrity can be provide in the web services in a secure manner. Additionally, the work discusses security issue in mobile cloud computing. Lastly, the work discusses several open issues that are not solved till date.

The studies of the paper (Modi et al., 2013a) over viewed different types of cloud security issues in a new way. The author divides each security issue according to the cloud computing layers and studies each layer issue. In this paper, very short discussion is found about the data storage security issues and virtualization security issues and their solutions.

The paper (Fernandes et al., 2014) has provides a categorization of security issues on the basis of several security topics. The work provides an overview of previous research work. The author present several topics related to cloud security and provide security issues related to each topic. The security landscape in this paper is very wide as compare to other papers. At the end, this paper gives some recommendations of various open challenges that to be solved in the future. The recommendations is very fruitful for future research work in this area.

The paper (Kulkarni et al., 2012) describe the service model and deployment model of the cloud computing. In this paper, the author

directly focus on the service model and deployments of the clouds, which included cloud storage architecture, storage as a service and its security requirement. They also describe security issue related to cloud storage.

The paper (Zhou et al., 2010) presents a detailed study about the cloud security and privacy for cloud service providers. The author describes the security and privacy both term separately. First, focus on security terminologies such as confidentiality, integrity, access control, availability, and auditing characteristic, after that focus on widely used privacy methodology. In addition, the paper contributes some solution on multi-location storage server.

The paper (Oktay and Sahingoz, 2013) provides an overview of cloud computing architectural framework. After that, it discusses various types of attack in the cloud computing. After analyzing the attacks, they pointed out intrusion detection system and its prevention in the cloud scenario. In this paper, the authors only covers cloud overview, security attacks, intrusion detection system and its prevention.

The IaaS cloud security (Vaquero et al., 2011) includes security on virtualization, storage, networking, and physical sides of cloud infrastructure networks. Multi-tenancy is a property of the cloud, which allows the users to access the resources in a shared manner. Multi-tenancy is the major property of the cloud that lead many security threats and issues. Authors analyzes the security issues and threats from Cloud Security Alliance (CSA) orientation report that is publish in 2010.

The paper (Subashini and Kavitha, 2011) focuses on a framework that describes security issues related to the service delivery models. The authors first consider the security scope of each delivery model. After analyzing the model authors finds a number of issues in the SaaS service model.

The paper (Ahuja and Komathukattil, 2012) gives a security framework to cloud providers after finding the many threats and associated risks in the cloud. They also discussed data management and security model of some cloud service providers.

The paper (Pearce et al., 2013) presents a comprehensive survey based on virtualization security problems, in a platform independent manner. Authors first explain basic of cloud virtualization, after that they illustrate a generous framework for cloud system virtualization. The study discussed secure system isolation and presented issues that arises from strong virtualization properties and from weak implementation of core virtualization.

The paper (Aguiar et al., 2014) focuses on the topic related to the cloud data computing and storage security. The authors presented several issues, current topics and recent developments regarding cloud data computing and storage security. They analyzed some problems related to web services, authentication and authorization, availability, and accountability. For each attribute, they derives some technique and mechanisms to gain secure storage and privacy on remote storage data and computation.

The paper (Xiao and Xiao, 2013) presents a systematic overview of security issues arises due to attribute-driven paradigm used in the cloud based system. First, they specify a relationship among the security and privacy attributes (confidentiality, integrity, privacy, and availability), then they have discussed the vulnerabilities, threats and their defense strategies in cloud computing.

The paper (Rodero-Merino et al., 2012) gives detail survey about security threats in PaaS cloud architecture. The survey is based on the concept of multi-tenancy, which gives sharing based platform, concentrate on Java and .NET based platform for isolation.

The paper (Takabi et al., 2010) discusses the various cloud security issues like outsourcing data and application, resource sharing, virtualization and hypervisors, heterogeneity, authentication and authorization, access control and identity management, trust and secure service management, data storage security and privacy. But, the authors doesn't provides any solution. Also, the open issues are missing in this paper.

The paper (Abbas and Khan, 2014) does not provide any information about cloud computing technologies and its services. The paper talks about only privacy issues in e-health cloud. They also talks counter measures and open issues. But, the discussion is limited, discuss only privacy term in the cloud. So, privacy solution does not remove all the security issues.

The authors (Hashizume et al., 2013) presented a survey on some cloud security issues and after that they describe associated security solutions. The cloud computing technology, framework, service model, and open challenges are not present in this paper.

The authors (Pearson, 2013) contribute a chapter in the book that provides security, privacy, authentication and trust management in a cloud environment. The chapter suggests the basic concept of cloud computing, but every time its main focus on security, trust and privacy issues in the cloud.

The paper (Tari et al., 2015) discusses the security issues and challenges present in the public and private clouds. After the discussion, they discussed some more security issues like service availability, multi-tenant service issues, data storage issues, identity and access control issues. They mainly focus on data utilization management aspects.

The paper (Perez-Botero et al., 2013) proposes a Xen and Kernel-based virtualization machine (KVM) hypervisors for categorized vulnerabilities. The base of the categorization is open source intelligence, available in various vulnerability databases. National Vulnerability Database (NVD) and SecurityFocus are such example of vulnerability database. Authors focused on three features of proposed model: the hypervisor functionality, the trigger source, and the attack target.

The authors in Rong et al. (2013) describes all security issues related to the cloud computing. The primary aim of the authors is to describe the cloud computing concept and associated cloud security issues. But, the main drawback of the paper is, it does not describe the solution of cloud security issues. Also, the authors are not focused on open issues present in the cloud environment.

In this survey paper, we have elaborated many security issues and their solutions to cover the gap found from the above discussed papers. The survey not paying attention to a particular area rather than it cover all security aspects. This work provides a broader perspective high level description of each security issue with their solutions. Furthermore, at the end of each issue the work is summarized with solutions, which provides some guidelines and recommendations, that is useful to understand a secure cloud environment. This comprehensive survey enables the reader to quickly catch up the basic concepts, under the security parameters and analyze the security issues of the current cloud environment.

3. Cloud computing architectural framework

In this section, the basic cloud computing architectural framework is presented, shown in Fig. 1. To understand the security issues, first it is important to understand the basic concept and framework of cloud computing. The NIST defines three service delivery models, five essential characteristics, and four deployment models, that is widely accepted (NIST, 2015).

3.1. Essential characteristics

There are many characteristics of cloud computing, but here we focus on five main characteristics, provided by the NIST (2015):

3.1.1. On-demand self service

It enables consumers to directly request, manage and access the services through the web services and management interfaces without any human interaction.

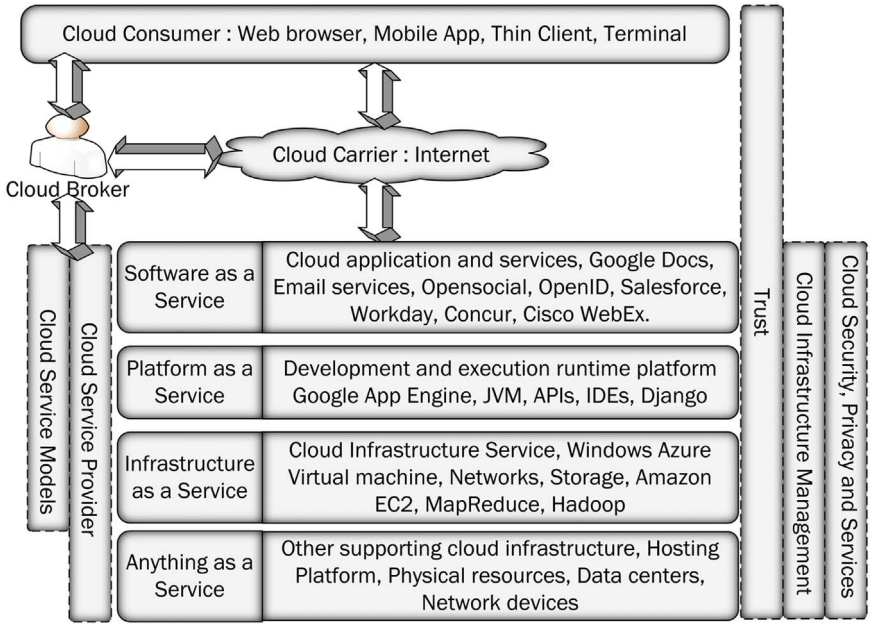

Fig. 1. A complete cloud computing architectural framework.

3.1.2. Broad network access

The data and services are presented in the cloud must be accessible through using any standard device like mobile phones, PC, desktop, laptop. These devices work over some standard protocols and technology. The nature of the cloud computing should support all the standard protocols.

3.1.3. Resource pooling

The cloud provider provides a large physical or virtual computing resources that are shared among multiple users. These resources are allocated dynamically in a multi-tenant environment.

3.1.4. Rapid elasticity

Elasticity is a major property of the cloud. Using this property resources is scaled according to the consumer requirements. Customers have unlimited resources that can be purchased as needed in pay-*per*-use manner.

3.1.5. Measured service

According to the user demand and paying service the meter capability of the cloud system automatically control and scaled the resources.

3.2. Service models

Service model provides a list of services; those are provided by the service provider and consumed by the consumer.

3.2.1. Software as a Service

The SaaS provides a standard Integrated Development Environment (IDE) to its client to access the applications and transfer the data and applications to remote storage server through on-line software services. Salesforce.com and Customer Relationship Management (CRM) are such example, which fulfill the SaaS model.

3.2.2. Infrastructure as a Service

The IaaS refers to the virtualized resources offered by the cloud service provider in the form of on-demand, including the computation, storage, network, memory, processor, and communication. Amazon Web Service (Amazon, 2015) (AWS) is the best example of IaaS, which gives EC2 services like virtual machine with a software stack.

3.2.3. Platform as a Service

The platform-oriented cloud provides a higher level of programmable platform, known as Platform as a Service. A easily programmable cloud platform provides multiple programming models, IDE, specialized services, operating systems, and platform level resources which is used by the cloud consumers to create, execute, deploy and manage their applications. Google App Engine is the best example of a Platform as a Service, which provide an extensible environment, in which developer develop and host web applications.

3.3. Deployment models

Deployment model of cloud computing says about the types of cloud.

3.3.1. Private cloud

A private cloud is operated and maintained internally by a single organization or through a Third Party Auditing (TPA).

3.3.2. Public cloud

A public cloud is run and managed by the CSP and the physical infrastructure may presented at off-site location of the user. The cloud resources are shared among the multiple people and people pay to the cloud provider according to the services they use.

3.3.3. Community cloud

A cloud that is deployed and shared among a group of people for share common interest, such as mission, security policy, application and services is known as community cloud.

3.3.4. Hybrid cloud

A hybrid cloud is mixing of two or more clouds with same infrastructure and capabilities.

3.4. Storage models

The storage model tells about how to store data in the cloud and availability of storage space. Cloud environment provides many types of storage solution. Each solution has its own benefits and limitations, based on requirement and available data consumer choose an appropriate storage system (Kulkarni et al., 2012).

3.4.1. Shared file/block storage system

A file consists of number of data that are located in folders, which are shared among multiple users/hosts using the Internet. Multiple user's access the files through standard protocols or capabilities. They can use any one of the protocols like Network File System (NFS), Server Message Block (SMB), and Common Internet File System (CIFS) for storage and access data.

3.4.2. Object storage system

In the object storage system, data are stored/accessed in the form of objects. Every object is accessed by a Global key, Hash, or Uniform Resource Locater (URL) using Representational State Transfer (REST) or web service based cloud services using Hypertext Transfer Protocol (HTTP) as prime protocols. Cloud Data Management Interface (CDMI) provides an object storage interface for accessing objects.

3.4.3. Database or table storage system

Many industries stored their data in form of Relational Database or Relational Database Management System (RDBMs), so they stored in the form of row and column. In the relational database, we maintained data integrity and avoid data redundancy. Scaling and performance are major issues in the cloud based relational database.

3.5. Cloud role and boundaries

The cloud provides different types of predefine role to the organization and human. The following subsection describes each participant role and responsibilities and how they interact with the cloud.

3.5.1. Cloud provider

A cloud provider refers as an individual or organization that implements/provides cloud resources. The main responsibilities of the cloud provider are to make and provide cloud services to the cloud users, according to SLA guarantees.

3.5.2. Cloud consumer

A cloud consumer is a human or an organization that consume the cloud IT resources provided by the cloud provider.

3.5.3. Cloud service owner

A cloud consumer or a cloud provider both are identified as a cloud service owner. The cloud service owner referred to person or organization that legally owns a cloud service.

3.5.4. Cloud resource administrator

The person or organization that performs administration task for a cloud based services, including cloud resources known as the cloud resource administrator.

3.5.5. Organizational boundary

An organizational boundary defines the physical boundary that encircles a set of cloud based IT resources that is really owned by an organization. The organizational boundary does not mean the boundary of an actual organization, encircle only an organized set of IT resources.

3.5.6. Trust boundary

When a cloud consumer access the cloud based IT resources, it must be need a trust that crosses the physical boundary of the organization to combine element of the cloud environment. A trust boundary is a logical encircles that typically cover whole cloud architecture (Begum and Khan, 2011) to represent the trusted IT resources.

3.5.7. Additional roles

A **cloud auditor** main role is to examine all computing process, storage space, performance, and security threats in the cloud space. Generally, auditor is a third party authenticator entity who provides a secure access environment for all entities.

3.5.8. Cloud broker

Cloud broker is generally an application program or individual, which provides an interface between client and provider.

3.5.9. Cloud carrier

Cloud carrier is a connection, communication link, or medium among all entities, Which enables consumer to access different services. Generally in cloud, Internet is a carrier, uses HTTP protocols to transfer information to all entities.

4. Cloud technology

In modern days, cloud use set of technology component that enables key features and characteristics of cloud computing. In this section, we define such technologies that help us to understand how these technologies are deployed over cloud infrastructure.

4.1. Broadband network and Internet technology

The Internet is allowing users to access remote cloud IT resources in order to support ubiquitous network access. This unavoidable requirement creates a built-in dependency on the Internet. The Internet facility is established and deployed by the Internet Service Provider (ISP). Each ISP can freely choose, manage, deploy and add another ISP in their networks. There are two types of connection available in networking technology, one is connectionless packet switching (datagram) and another one is router based interconnection.

In connectionless packet switching, the sender data are divided into multiple packets (datagram) and each packet follow different routes to reach the destination address. In router based interconnectivity, the sender data are divided into multiple fixed size packets, follow the same route to reach the destination address with the help of the router.

4.2. Data center technology

Data center technology contains multiple technologies and components that are typically composed with one another. The data center has both physical and virtualized IT resources. The physical IT resources including networking systems, houses computing, servers and equipment, composed with hardware systems. The virtualized IT resource is residing over the virtualization layer that are operated and managed by virtualization platform. Modularity and standardization are the basic requirements for reducing the limitation, operation and investment cost of the cloud. The data center is built with the help of standardized commodity hardware and modular architecture, multiple aggregation, unique building blocks to provide scalable, incremental growth of the services.

4.3. Virtualization technology

The virtualization is a conversion process that translates physical IT resources into a virtual IT resources. The IT resources include servers, storage, network and power. The virtualization software provides a coordination capacity of the host that permit multiple virtual server which is connected and communicate with each other in the same host. The virtualization allows to virtual servers to create a virtual disk image that contains a backup file of the virtual server. The virtualization is created by two types: operating system based virtualization and hardware based virtualization. In operating system based virtualization, the virtualization software is installed on a pre-existing operating system (host operating system). The second hardware based virtualization refers the installation of virtualization software directly on the

physical host hardware. After installation it is passed to the host operating system.

4.4. Web technology

The web technology is an emerging trend for development of cloud computing. The fundamental concept of cloud computing is based on Internet. The web browser, web based application and services are implemented and managed by specialized web technology. The World Wide Web (WWW) is a Internet based technology, that is used for connection of several IT resources. The two fundamental constituent of the web technology is web client and web server. Proxies, routers, cache server, and gateways are known as the secondary components of the web technology. The URL, Markup Languages (Hyper Text Markup Language (HTML), eXtensible Markup Language (XML)), HTTP Protocol is additional components that improve the scalability, security and performance of the system.

4.5. Multi-tenant technology

The same application logic is simultaneously accessed by multiple users using multi-tenant technology. Multi-tenant applications ensure that each tenant has a separate own view of the application and tenant have not allowed to access data and application to other tenants. Each tenant can individually manage their features of the application, such features is the user interface, business process, data model, and access control. The most common features of multi-tenants application is usage isolation, data recovery, data tier isolation, data security, application upgrades, system scalability, and metered usage.

4.6. Service technology

The service technology is the basic foundation of the cloud computing, used for creating “as-a-service” cloud delivery models. The web service, REST service, service agents, and service middleware are the basic technologies for building the cloud based environment. Web Service Description Language (WSDL), XML schema definition language, Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI) is the standards coming from the first generation of the web services. Like web services, REST service does not have a separate standard interface. The REST service share a common interface, that is typically built by the use of HTTP protocol. The common interface known as the uniform contract/ interface, Client-server, stateless, cache, layered system and on demand code is the six constraints reside in the REST services.

5. Cloud security

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. In this section, our aim is to explore several security concepts, which will help to better understand the cloud security issues.

5.1. 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.

5.1.1. 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. It's like a host OS, but it does not provide direct access to the hardware. This resource is accessible by VMMs, responsible for allocating the virtual hardware resources include CPUs, memory, network, and hard disk to each VM. If new VM sends hardware resource request to VMMs, a new image of that resource is quickly created and assign that resource to the requested VM. VMMs is also responsible for connecting multiple VMs. At the last, VMs are connected to virtual switches and it composed with external and internal networks.

Some specific VMs or virtual Network Interface Card (NICs) can be used as a hardware connection device. VMware and vSphere are some platform support virtual features. VMMs are responsible for creation, deletion and allocation of the virtual resources to the VMs, supporting on-demand and elastic features of cloud computing. There are several free VMM solutions include RedHat-maintained KVM, VMware Player, Oracle VirtualBox, Microsoft Hyper-V, Xen and so on. Other commercial paid VMMs include Oracle VM Server, VMware Workstation and vSphere, Citrix XenServer, and Parallels Desktop and Virtuozzo.

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.

5.1.2. 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. The multi-tenancy can be exploited in the form of co-tenancy, co-location, and co-residence attacks because of customer valuable data may be located at the same physical location. Resulting from them, attacker can access neighbor VMs or running applications. Denial of Service (DoS) attack is another issue that can happen by consuming much resources.

5.1.3. Threat agents

An entity that creates a threat called the threat agents, capable of tackle an attack. This threat is originated by human or any software program, happening internally or externally.

An external software program or external human called anonymous attacker sends off network level attack by using the public network. This is a non-trusted cloud service consumer, those living in the cloud environment without permission of the cloud administrator.

A program that holds compromised or malicious logic, exists externally, intercept and potentially corrupt messages called as a malicious service agent. This can be able to move or transfer network traffic flow within a cloud.

A trusted attacker is a trusted cloud consumer that may share IT resources in the same cloud infrastructure. The trusted attacker launches their attack within the cloud trust boundary by break-in valid credentials of a user.

Malicious insider is human threats acting on behalf of cloud providers. They are typically employees or a third party agents, working in the cloud provider organization. This type of attack is very dangerous

because they can get administrative privileges for accessing cloud consumer IT resources.

5.1.4. 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.

5.1.5. Security mechanisms

Security mechanisms are some defensive framework for protecting IT resources, sensitive data, services and information. Security mechanisms are described in term of countermeasures and safeguards to enhance the security of the system.

5.1.6. 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.

5.1.7. Cloud security services

The cloud security service is a complex service, technique, regulation and behavior 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 five 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. The threats and number of access points will increase due to increase number of tenants, device, and application. Sometimes data confidentiality in the cloud is correlated with the user authentication, in which user resources are protected from unauthorized access. There is a complex problem to secure user account from theft in order to control the access of the objects, including device, software, and memory etc.

A key term of integrity in the information security refers the characteristic in which data have not been modified by an unauthorized party. The alteration of data, software or hardware only possible by an authorized person in an authorize way. 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 authorization provides some permission to a subject can perform a certain operation, if the subject is authenticated. In order to complete the authentication and authorization, first authentication done then provide authorization. The insufficient authorization, session/credential prediction, session expiration, and session fixation can lead to access a protected areas beyond their privileges.

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 is responsible for the availability of cloud IT resources.

5.1.8. 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.

5.1.9. Data outsourcing

Nowadays, the organizations used outsource data model for their business purpose. It refers to a mechanism in which people give data extraction and collection responsibility over certain subject to a third party provider. This third party usually other company work on a contract basis. This feature provides both capital investment and operational investment. This data outsourcing concept are adopted by many IT industries. Data outsourcing concept provides data storage, data management, computing and security services to the IT industry. There are some drawbacks of this data outsourcing is, it create a physical separation between data owner and their data. The customer losses control over the data so, when a customer gives her data to the third party first he insures that the data computing and storage are happening in a secure manner.

5.1.10. Data storage standardization and security

In the Open System Interconnection (OSI) model several security mechanisms are implemented, including digital signature are used for checking integrity, authentication mechanisms is used for control data access and various security protocols. The organization gives a high level certification to their customers, for this company adopt certificate authority like the International Organization for Standardization (ISO). In the cloud, data processing is a heavy task because of cloud hold massive amounts of data. Additionally, reliable data storage is another aspect. Backing policy is also required. Clouds spread the data into multiple data center even cloud provider are same. This mechanism provides geographical redundancy to data, meaning that a copy of this data can be located in multiple data centers to avoid single point of failure. The paper (Leopando, 2013) defines an accepted data backup guideline known as 3-2-1 rule. The guideline says that owner contains at least three replica in two different formats with one replica in local hard disk. In the cloud context, this scenario could be applied by having three copies, cloud provider contain two copy and one copy is in the local enterprise hard disk.

5.1.11. Trust management

Trust is a non-measurable parameter in the cloud security. It assign to the self infrastructure, the data center, the hardware, and the network configuration is based on the faith of the decisions. The trust evaluation process is based on several factors, including multi-faced and multi-phased phenomena. Therefore, trust is a highly volatile and strongly rely upon the underlying aspect. The trust issue arises in the cloud computing due to customer data and services are located at remotely and it is managed by second or third party.

5.1.12. 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 and process segmentation.

5.2. Requirements of cloud security

This subsection describes the requirements of the cloud security. Each business organization chooses some security strategy before using any of the services. There are six security requirements: authentication or identification, authorization, confidentiality, integrity, non-repudiation and availability. Each service model (IaaS, PaaS, and SaaS) requires authorization for public cloud to prohibit unauthorized access. The hybrid cloud is more secure as compared to public and private cloud because the hybrid cloud model requires high security parameters as compared to public and private cloud. Also, the integration options, add an additional layer of security in the hybrid cloud. All the cloud security models, integrity are essential requirement, for checking the data correctness. The security model in SaaS provides security for the web and service based access applications. The high availability and integrity of the services required strong security mechanisms in the underlying network.

5.3. 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) presented the top threats that are related to the security architecture of the cloud services. This paper discusses several potential threats that are harmful to the cloud is shown in Table 2.

5.3.1. Different service delivery/receiving model

Cloud computing model and business model both use different way of delivery/receiving services. So, cloud computing is capable to change own way for delivering the services. All services and application are allocated to remote site provided by the cloud service provider, company need to examine all the risk associated with the loss of control over the cloud. Cloud data are traversing from one location to another location, both locations use different security laws. This is the major threats which are generated at the time of usage. For removal of such threats require a strong end-to-end encryption, a common standard security laws and trust management scheme.

5.3.2. Abuse and nefarious use of cloud computing

Unlimited bandwidth, network and storage capacity are such utilities provided by IaaS providers. Some providers provide their services to use for a predefine trial period. Which is often coupled with a frictionless registration process where anyone can register without any secure process and access the cloud services. At this trial period they do not have sufficient control over the user. As the result, spammers, malicious code authors and other criminals are able to execute their attack, other possible threats include Distributed Denial of Service (DDoS), password and key cracking, captcha solving farms, and hosting malicious data. This type of threats affect the IaaS and PaaS service infrastructure. To protect the cloud from this type of threats, the initial registration process should be follow strong authentication process, do proper validation, and verification.

5.3.3. Insecure interface and API

The cloud provider provides set of software interfaces and API's to their users for communicating with the cloud services. These interfaces are located on the top of the cloud framework in the form of a layer, which increases the complexity of the cloud. Such interfaces provides all provisioning, management and monitoring services to their customer. So, the security and availability of the cloud is very much relied on the security of these API's. But, sometimes, both accidental and malicious attempts can hamper the security of these API's. This type of API threats may affect the PaaS, IaaS, and SaaS service models. Another type of risk can also be there as third parties often build upon these interfaces to offer services to the customers. This can prevent by adoption of proper authentication and access control mechanism and a secure interface model.

5.3.4. Malicious insiders

One of the most major threats in the cloud computing is malicious insider threats, because of many organizations does not provides information about her hiring procedure for employees and access level of internal resources for their employees. This threat is mainly executed due to the lack of transparency and the IT services and customers working under single management domain. Somehow, an employee gets a higher level of access resulting from this, the confidentiality of data and services are penetrated. This also results in a situation, where an insider attacker can access the confidential data and affect the cloud services. This can happen by an insider attacker who can easily entered into the system via firewall or intrusion detection system when the

Table 2
A comprehensive study on cloud threats described by the CSA in 2013 and its solutions.

Threats	Effects	Affected cloud services	Solutions
Different service delivery/ receiving model	Loss of control over the infrastructure of the cloud	PaaS, SaaS, and IaaS	Offered services under the control and monitored
Abusive use of cloud computing	Loss of validation, service fraud, stronger attack due to unidentified sign-up	PaaS and IaaS	Observe the network status, provide robust registration and authentication technique
Insecure interface and API	Improper authentication and authorization, wrong transmission of the content	PaaS, SaaS, and IaaS	Data transmission is in encrypted form, strong access control and authentication mechanism,
Malicious insiders	Penetrate organizations resources, damage assets, loss of productivity, affect an operation	PaaS, SaaS, and IaaS	Use agreement reporting and breach notifications, security and management process is transparent
Shared technology issues	Interfere one user services to other user services by compromising hypervisor	IaaS	Audit configuration and vulnerability, for administrative task use strong authentication and access control mechanisms
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, allowing the attacker to compromise the security of the services	PaaS, SaaS, and IaaS	Adoption of strong authentication mechanisms, security policies, and secure communication channel
Risk profiling	Internal security operations, security policies, configuration breach, patching, auditing and logging	PaaS, SaaS, and IaaS	Acknowledge partial logs, data and infrastructure aspect, to secure data use monitoring and altering system
Identity theft	An aggressor can get identity of a valid user to access that user resources and take credits or other benefits in that user name	PaaS, SaaS, and IaaS	Use strong multi-tier passwords and authentication mechanisms

security system assume it as a legal activity.

5.3.5. Shared technology issues in multi-tenancy environment

The services are delivered by IaaS vendors in multi-tenant environment, use virtualization concept. Virtualization provides the facility to share the same resource among multiple users. The hypervisor in a multi-tenant environment may allow a malicious user to gain the information about the user. This leads to a major threat as the infrastructure are not designed to offer strong isolation in a multi-tenant environment. The concept of sharing may affect the overall cloud infrastructure by allowing one user access information about another user. Strong authentication and access control are some mechanisms to prevent this issue.

5.3.6. Data loss and leakage

The example of data loss is the deletion, alteration and theft of data without a backup of the original content, loss of an encoding key may also produce data loss, due to the productive and sharing nature of cloud computing. The main reason of data loss and leakage is lack of authentication, authorization, and access control, weak encryption algorithms, weak keys, risk of association, unreliable data center, and lack of disaster recovery. This Threats can affect the IaaS, PaaS, and SaaS service models. Secure API, data integrity, secure storage, strong encryption key and algorithms, and data backup are some prevention methods.

5.3.7. Service/account hijacking

The service hijacking is a process, in which the client may redirect to a harmful website. This can be executed through fraud, phishing and exploitation of software vulnerabilities. The reuse of credentials and password are often leads to such attacks. In cloud computing, if an attacker can access someone's credentials, they can capture the activities, transaction data, manipulate data, return falsified information or redirect the client to illegitimate sites and the hacked account.

5.3.8. Risk profiling

Due to the heavy workload cloud are less involved with ownership and maintenance of hardware and software. The cloud gives contract to organization to maintenance of software and hardware. This concept is good, but cloud does not know the organization internal security procedure, patching (Fan et al., 2013), auditing, security policies, hardening, and logging process. This unawareness comes greater risk and threats. For removal of threats cloud have an awareness of partial infrastructure details, logs and data, and cloud should have a monitoring and altering system.

5.3.9. Identity theft

Identity theft is a type of trickery in which someone impersonate the identity, credits, associated resources and other service benefits of a legitimate user. Resulting from these threats, the victim suffers many unwanted results and looses. This threat can happen due to the weak password recovery method, phishing attacks and key loggers, etc. The security model includes strong multi-tier authentication mechanisms, strong password recovery method.

5.4. Attacks on cloud security

Companies know the value of cloud computing in a business environment. Day by day new technologies have emerged, which formulate new attacks for cloud computing. 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 Table 3 describes several security attacks, effects on cloud with some solutions.

Table 3
A comprehensive study on cloud attacks and solutions.

Attacks	Attack surface/procedure	Affected cloud services	Effects	Solutions
Zombie attack (DoS/DDoS attack)	Direct/indirect SYN packet flooding to host, attack on VM, attack on hypervisor, network based attack	SaaS, PaaS, and IaaS	Service availability affected, may be create a fake service	Strong authentication and authorization
Service injection attack	Distractive service entering through accessing service identification files, application and VM level attack	PaaS	Service integrity distressed, Malicious service provided to users instead of valid service	Strong isolation mechanisms between VMs, use hash function to check service integrity, Web service security, adopt secure web browsers and API
Attack on virtualization/ hypervisor	Settlement with the hypervisor, breakout virtual layer. VM and hypervisor level attack	IaaS	Access the credentials and control to another user	Need a hypervisor security solutions, monitor hypervisor activities, VM isolation required
User to root attacks	Accessing the whole resources of a valid user. user level attack	SaaS	Affect the privacy of user's sensitive information and services	Use strong password, better authentication mechanism
Port scanning	Scan the open port and gain information about open port	IaaS, SaaS, and PaaS	Abnormal behavior of the service, affect service availability	Required strong port security
Man-in-middle attack	By accessing data transmission between two individual	SaaS, PaaS, and IaaS	Penetrate the data privacy and security	Required a proper secure Secure Socket Layer (SSL) architecture
Metadata spoofing attack	Modify service information file such as WSDL. service level attack	SaaS and PaaS	Abnormal behavior of the service, affect privacy of the service	Service functionality and other details should be kept in encrypted form, to access the file required a strong authentication mechanism
Phishing attack	By accessing a fake web link	SaaS, PaaS, and IaaS	Affect the privacy of the user credentials that should not be revealed	Use secure web link (HTTPS)
Backdoor channel attack	Settlement with the valid user VMs, VM and hypervisor level attack	IaaS	Affect the service availability and data privacy, provides rights for gaining valid user's resources	Required strong authentication, authentication and isolation mechanisms

5.4.1. Denial of service attack

Denial of service attack is a type of attack in which an attacker sends thousand of request packet to the victim, through the Internet. The main aim of the attacker is to exhaust all the resources of the victim. An attacker may flood a large number of requests to waste the computational power, performance time and cryptographic operations. This type of attack may affect the cloud actual behavior and availability of cloud services.

The attacker sends different type of packets including Transmission Control Protocol (TCP) packet, User Datagram Protocol (UDP) packet, and Internet Control Message Protocol (ICMP) echo request packet. An attacker flooded numbers of TCP packet with the SYN flag set to its victim. The victim thinks that this request are coming from a reliable user and victim make a TCP connection with the help of three way handshake protocol with the attacker. Victim many times are consuming to make connections and for each connection he reserved some spaces in the buffer. This is the most happening attack known the SYN flood attack. In the second type of packet, attacker send a large number of UDP packets to a non listening port on the victim. After receiving the packet victim send ICMP respond message "Host unreachable". This cause victim many time consume to send response packet. In the third type of packet, attacker sends very large number of ICMP "Echo request" packet to the victim. In this packet's destination IP address is a special broadcast address of the network, while the source IP address is the address of the victim. Resulting from them victim send "Echo reply" message from each host on its network. This type of attack is referred as a Smurf attack.

Another type of attack known as the DDoS attack. A distributed DoS attack is much more complex and harder to detect compared to a DoS attack. In a DDoS attack, the attacker called a controller, first scan the whole network and list out all the defenseless hosts called handlers and settlement with. Each handler creates or recruit many agents called zombies to launch the attack.

5.4.2. Service injection attack

Cloud system provides the services to its user. When a user wants to access a service first he sends a request to the cloud and cloud system is responsible for providing free to use the resources of the requested service. The new allocated resource to a requested user may be assigned to the other requesting user at some later point of time. An attacker makes a new malicious image of the assigned resource and every time he tries to inject the malicious resource, service or new virtual machine into the cloud environment. When a legitimate user request for a service the malicious service serve as a cloud service. This may affect the cloud actual functionalities. To protect this type of attack a service integrity module should be implemented.

5.4.3. Attack on virtualization

The virtualization attack in the cloud are performed two different types first is VM escape and another is rootkit in hypervisor. In virtualization attack, control of the virtual machine in the virtual environment will be captured. Zero day attack is one of the method. Another attack includes backdoor channel attack, VMs modification, storage allocation and multi-tenancy.

5.4.4. User to root attack

In this attack, the attacker on intruder acquires limitless access to the whole system by seizing the account and password of an authorized user. This type of attack is executed through overflowed data in which excessive data sent to a statically defined buffer.

5.4.5. Port scanning

Port scanning is used to identify open, closed and filtered parts of a system. In port scanning, intruders use open ports like services, IP and MAC address that belong to a connection to seize information. The most common port scanning attack includes TCP, UDP, SYN/FIN/ACK and window scanning. The actual attack is executed by attackers after scanning the port.

5.4.6. Man-in-the-middle attack

The man-in-the-middle attack refers an attack in which an attacker is active in the middle and access the data those are passed between two parties. This attack is possible due to lack of security configuration in a Secure Socket Layer (SSL). The two parties, including providers communicate with each other in the cloud, at this time an attacker is residing in the middle and capable to access the data, if communication channel are not secure.

5.4.7. Metadata spoofing attack

The service functionality and detail are stored in the WSDL file. In this type of attack, an attacker wants to access this type of file and perform modification or deletion operation on the file. For accessing the file attacker wait until service delivery time and at the delivery time he succeeds to interrupt the service invocation code in the WSDL file. The solution of this attack information about service functionality and other details should be kept in encrypted form. Strong authentication should be required to access this type of file.

5.4.8. Phishing attack

Phishing attack is performed for manipulating a web link. Resulting from the attack a legitimate user is redirected to a fake web page and he thinks the open web page is a secure page and he enter his credentials (user-name and password). After that, the attacker can access his credentials.

5.4.9. Backdoor channel attack

The backdoor channel attack permits the attackers to access remote computer program that control the victim resources. It is a passive attack. A programmer may sometimes deploy zombies so, that the zombies can be performed DDoS attack. However, attackers often use back doors channels for control the victim resources. It can breach the privacy and confidentiality of the data.

5.5. Data center security

The cloud system resembles cluster systems, not only for combining together computing resources while have a common achievement. The cloud system design a room for storage and protect her equipments. The cloud data center is the very strong physical foundation such as grid redundancy. Cloud providers assure that the cloud is fully fault tolerance and efficiency of the services is very high reaching 99.99%, thus achieving the tier 4 level in every situation. The tier level defines the data center quality, being the lowest level is 1 and highest level quality of data is 4. The cloud service provider aim is achieving high availability of data and highly reliable services in term of uptime and elasticity. In fact, IT researcher, research on cooling factor in data center and specially design a cool IT room.

The provider provides a physical security throughout a data center. Other security measures are unnecessary if this physical security does not fulfill all criteria. The data center must be well secured in order to prevent other physical equipments. Each computational server, storage server, and network equipment are under the physical security. Any user wants to access the service first he clear the security clearance. For example, the private identity card is assigned to each user in private organizations that is used to open door locks and access restricted area of the facilities. The provider takes higher price to its customer and give some higher level of security options (access right).

The internal network of the cloud computing environment consists of a number of service driven networks, storage area networks, and computation and storage related hardware. Hence, if any, other enterprise network is deployed, first fulfill the security requirements to analyze network traffic and safeguard data. Firewalls and IPSec is

some network security protocols that help to prevent the network system. IPSec is used to alert malicious intrusion attack. Honeypots are another approach to create a distraction for attacker and learn their movements. Typically, a Security Operations Center (SOC) is established within the infrastructure to monitor the network health and detect the anonymous packet. A Computer Security Incident Response Team (CSIRT) is placed within the SOC, collaborates with other CSIRTs team to share the security intelligence. For achieving high level network security, Security Information and Event Management (SIEM) are another approach. SIEM is used to correlate real time events, triggered by the network, learn what is normal and abnormal behavior of the network by the security agents. Hewlett-Packard (HP) ArcSight are such example that perform event correlation. Security agents establish SIEM to share their alert messages and event message. Kufel (2013) compared all the available SIEM platform. Several cloud Intrusion Detection Systems (IDS) platforms are available in the market. The paper (Modi et al., 2013b) describe IDS and Intrusion Prevention Systems (IPS) role in the cloud to gain high level security and performance to next generation networks.

The paper (Kant, 2009) presents a four layered model for data centers. The lower level consists of physical infrastructure in the form of clusters. Then the next upper layer is a virtual infrastructure layer, enables to run co-resident VMs to make a virtual data center. A single data center can be owned by a single user, so that he manages the VMs. The virtual infrastructure coordination layer is the third layer of this model. It makes an agreement between the virtual data center and cross-geographic location deployment. This layer enables all the scattered virtual data center mount in a single unit which can be served as a distributed virtual data center. In the top layer all applications run in a SaaS manner. This layer is made for the service provider.

Nowadays, a new dimension of the data center is emerging, in which data center is not just for storing the data, also with some new network connectivity concepts. Resulting from them, new security complication is arise in the inter-clouds. The Google Spanner Database (GSD) is made for public share own data across five data centers. The paper (Zissis and Lekkas, 2012) identified some security issue and attack include flooding attack, hardware interruption, theft, modification, infrastructure misuse and natural disasters in the data center.

6. Cloud security issues

In this section, work is mainly focusing on several categorized security issues and their solutions. First, the work presents a brief introduction about security issue in cloud computing then presents their solutions. A security issue is something happening in any assets-attacks, misconfiguration, fault, damage, loopholes, and weakness in the system. There is much difference between cloud specific issue and general issue. The cloud related issue is generated due to the characteristics of cloud computing, defined by NIST and it is much more difficult to implement security solutions in cloud environment.

The survey categorized security issue in eight parts as data storage and computing security issues, virtualization security issues, Internet and services related security issues, network security issues, access control issues, software security issues, trust management issues, and compliance and legal aspects. 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.

6.1. Data storage and computing security issues

Data is a vital part of cloud computing. Data stored in the cloud is isolated and inscrutable to the customers. Customers on the first hand are either reluctant in providing their information or are in constant fear of losing their data in bad hands, unfavorable consequences that can arise during manipulations and processing. Thus, their data should be consistent during computation, confidential at every stage of processing and perpetually stored to update the records.

In the remote storage or third party storage the main problem is that the user does not know what happen after the storage of the data in the cloud. The data owner does not aware the locality of the cloud storage center, security services and security mechanisms used for securing the cloud data. The quality of service is the important aspect in the cloud storage. A cloud storage provider needs a proper technique and mechanisms to store efficiently and reliability data in the cloud. There are two situations before the computation and after the computation of data. There are various security issues and their solutions related to data storage, un-trusted computing, data and service availability, cryptography mechanisms, cloud data recycling, and several malware that affects the cloud storage system as seen in Table 4. The research needs a system that frequently, efficiently and securely store the data in the cloud. So, that people store their data on the trusted environment.

6.1.1. Data storage

In the data storage issue loss of control is a major issue in cloud computing model because it does not provides full control over the data and it is harder to check data integrity and confidentiality. The customer of the cloud computing is physically separated from their data, storage and computing server. The cloud computing provides a server pool that store the cloud data. The location of the server pool is unknown and it is control and manage by the cloud service provider. The abstracting of the virtual layer makes harder to find the actual location of the storage server. The user allows a certain level of control only on the VMs. The characteristics of the cloud computing like multi-tenancy and virtualization make more possibilities for the attacker to perform the attack.

The user data are stored in the cloud data centers. Many big player provides cloud storage at very cheap competitive cost. This distributed data is highly redundant and stored at different physical locations. The electrical source redundancy and efficient cooling ensure that the data is highly available. By the help of proper space allocation mechanism, cloud space can be reused efficiently. The data redundancy provides a mechanism in which data is backuped to another cloud server for ensuring high availability of data. In case of one data center is completely failure, provider use backup data server. Google and Amazon have different data servers in different countries. These organizations store their data on the basis of multi-location feature that can bring new security threats and legal problems, as the data stored across the world have different policies.

6.1.2. Un-trusted computing

Many security service goal is to implement the front end interface for SaaS application, which is come when user request to a web service or an HTML page. Such applications is changeable or adjust with a pattern of behavior. This pattern of behavior composed with the session state manager, other service and reference data that may be called by the request. A service tree is generated when an application called another application or service, simply the request is turned from one service to another service and so on. A computing framework that computes large data sets in distributed system may produce the unwanted, inaccurate, and dishonest result due to mis-configuration and malicious servers. It is hard to find an honest and accurate computation server that gives an accurate and honest result.

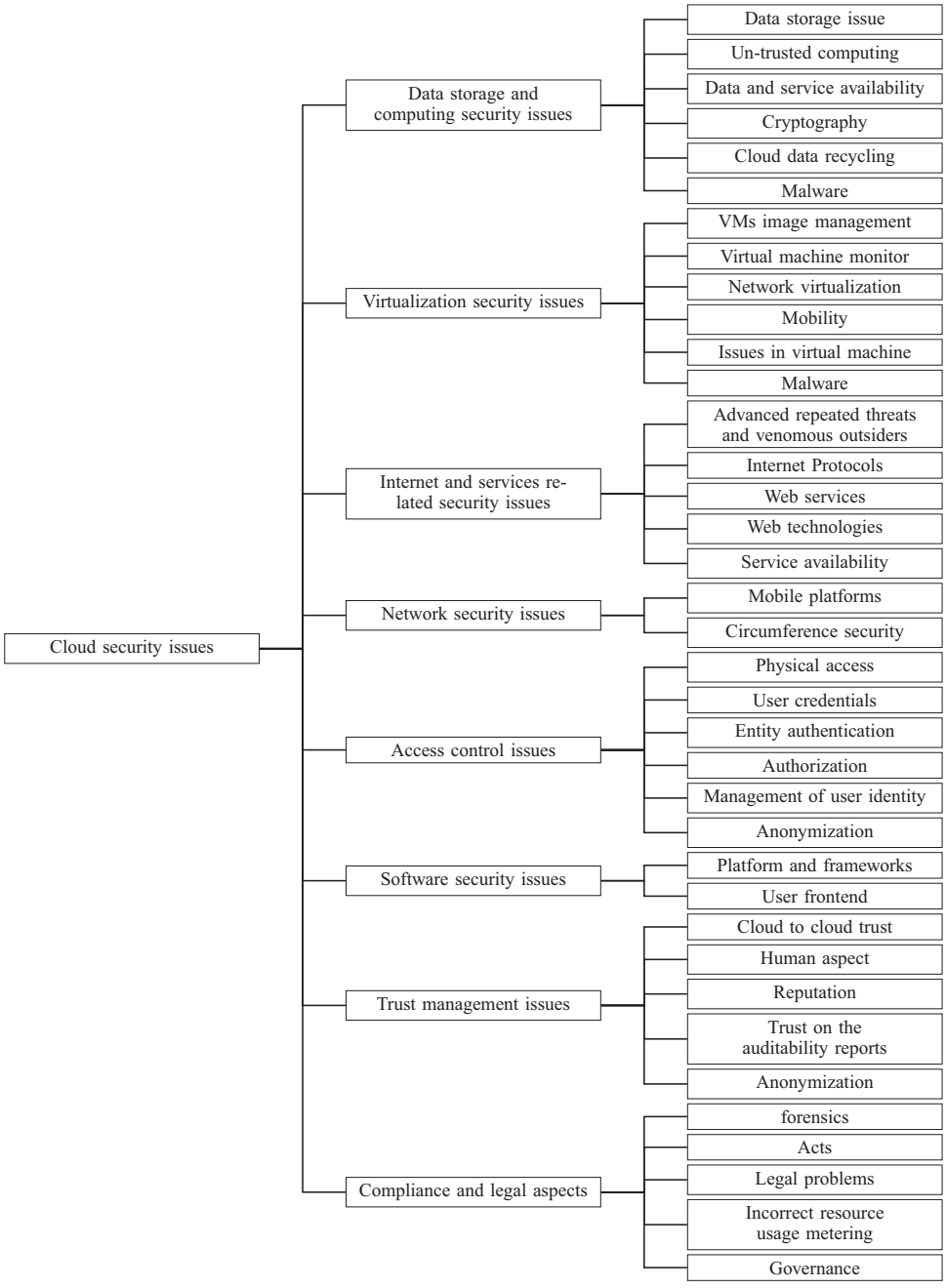

Fig. 2. A summary of the cloud computing security issues.

6.1.3. Data and service availability

The physical and virtual resources (database and processing servers) of the cloud are highly available. For achieving high availability and scalability of services and data require architectural changes are made in the application and infrastructure level. One solution is running application are alive multiple server. This approach enables the DoS attacks. The benefits of this approach is, if one application server is crashing then another same application server is present to ensure data and service availability. It is also possible that the server has a highly demanding application task and he consumes more power, occupy available resources, take more time to process the task. Resulting from this it may possible that the application availability and other computation cost is increasing. The SLA is used to depict the availability of data, speed of memory, and quantity of resources. A hardware availability is another issue in cloud computing. A single fault can lead the partial or complete failure of the system, result from this system failure, the availability of data and services are affected. Unavailability of hardware resources can lead to cloud outages hampering the entire online business fraternity causing distress.

6.1.4. Cryptography

Cryptographic mechanisms are used to secure the cloud information and data. It is a straight forward idea to achieve the security of the cloud. It converts plain text data into another form of text called cipher text. The idea based on the assumption that it is unfeasible to calculate the value of the plain text data, if a cipher text is available. So, they require carefully and strong implementation of cryptography methods because the whole security depends upon the key that is used as an encryption key. The prime factorization of large number gives more security to the Rivest Shamir Adleman (RSA) based encryption. They are impossible to calculate in discrete logarithm time. The bad implementation of the algorithm or uses weak key in the encryption

Table 4
A comprehensive study on data storage and computing security issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
Data storage	Remote data storage	Syam Kumar and Subramanian (2011)	
	Loss of control	Xiao and Xiao (2013)	Better security scheme for resident data Sood (2012)
	Data pooling, data locality	Sengupta et al. (2011) Xiao and Xiao (2013)	File Assured Deletion (FADE) scheme for data security Tang et al. (2012)
	Multi-location	Zhou et al. (2010)	SecCloud protocol for secure storage Wei et al. (2014)
	Complex model for integrity checking	Subashini and Kavitha (2011)	
Un-trusted computing	Top down SLAs		
	Malicious users, downtimes, slowdowns	Helland (2013)	A non-interactive solution Gennaro et al. (2010)
	Dishonest computing, root level error in backups, migration and restoring problem	Xu et al. (2011), Xiao and Xiao (2013), Rong et al. (2013)	A lightweight and low-cost solution for e-banking Li et al. (2012)
	Weak security solutions for computing models		
Data and service availability	Counterfeit resource usage	–	A solution for data availability Wang et al. (2012)
	Cloud interruption	Ahuja and Komathukattil (2012), Armbrust et al. (2010), Rimal et al. (2011)	Proxy re-encryption scheme based on time-based
	Hardware availability issue (hardware fault)		Liu et al. (2014)
Cryptography	Insecure cryptography mechanism, poor key management	Grobauer et al. (2011)	
	faulty cryptography algorithms	Yu et al. (2012)	Order-preserving encryption Boldyreva et al. (2011)
	Brute force and Dictionary attack	Sood (2012), Thorsheim (2015)	Cryptography in cloud computing Jaber et al. (2013)
Cloud data recycling	Deficient implementation of data devastation policies	Boampong and Wahsheh (2012)	
	Un-used hard discard	Armbrust et al. (2010)	
	Hard disk multi-tenant usage	Grobauer et al. (2011), Pearson (2013)	Secure data deletion Reardon et al. (2013)
	Resource recycling	Casale (2013)	
Malware	Failure of signature based anti-viruses	Li and Clark (2013), Websense (2013)	Detecting malware Oyama et al. (2012), Xing et al. (2013)
	Cloud malware syncing	–	

increase possibility of attack. The most common attack in cryptography is brute force attack, match all possible keys with the encryption key in a known range. There is a great need to protect massive databases using Advanced Encryption Standard (AES) and Message Authentication Code (MAC). The MAC is used to ensure the integrity of the message and the data origin authentication. Encryption method AES uses 128 bit key to encrypt the 128 bit plain text. The digital signature is used to verify the sender identity. In this process, signing algorithm use sender private key to generate a signature. At the receiver side verifying algorithm use sender public key to verify the signature.

6.1.5. Cloud data recycling

It was a wise proposal to reuse the cloud space once the data has been properly utilized and sent to garbage. But, it must be ensured that the data used by the previous user is not available for the next user. The process of cleaning or removing certain piece of data from a resource is known as sanitization. After the sanitization refreshed data are available for people as distributed manner. The data sanitization is a critical task in the distributed system in order to properly dispose of data and select the data which is sent to the garbage. The improper sanitization gives data leakage and data loss results, because the hard disk might be deleting some data that is important.

6.1.6. Data backup

In the cloud computing another important issue is cloud data backup. There is need of a regular data backup mechanism to ensure the availability of data. This data backup procedure is done at the service provider side and provides data recovery in case of natural or accidental disasters. The most common threats like unauthorized access and data tempering may be destroying the backup storage. So, the data backup time people also consider this type of threats.

6.1.7. Data recovery

Cloud computing has resource pooling and elasticity feature. This feature provides the ability to cloud to allocate dynamic and on demand resources for the requested user. Due to this feature, there may be possible that data recovery and confidentiality are broken. The resources that are allocated to a requested user, it may possible that the allocated resources is assigned to another user at some later point of time. The malicious user can be able to use data recovery mechanism and find the previous user data. This can be generated many serious harms for the sensitive user data.

6.1.8. Privacy and integrity

Although the cloud computing has a model of computing network provides cost economy and efficient infrastructure services. The infrastructure management activity is free from user's involvement. This enables the several security issues. In the cloud, number of user and application is increasing, this can lead to enhanced security risk in term of data privacy and integrity. In the shared environment, there are malicious user collect the user information that can breach the privacy and integrity of the user, but also non malicious (insecure entity) user can breach the data. A successful violation of integrity may affect the multi-tenants nature of the cloud computing.

6.1.9. Malware

The advance threat report presented in 2012 says that malware is active and perform actions in every 3 min at a single organization on average. The MediaFire and SugarSync is an online data storage provider creates one specific security issue related to cloud based system is they capture or inherit the functionality and data property of several devices. The main problem behind that is, if one system contain malware then due to inheritance the malware is spread across the cloud. Additionally, malware is very harmful to cloud devices because it can able to delete or corrupt the cloud data. Suppose, protection of such

type of devices, assign anti-virus agents. When the malware enters in the system, first anti-virus agents match the malware signature and by chance if the signature is matched, but probability of happening such thing is very low, then the malware enters the system and he may delete the data, change the data or do anything with the data. This is the worst situation. If the agent will find such malware first time, then it is good otherwise surely the malware create more serious issues. So, people required one monitoring system that is able to detect and show such malware. Malware spreads to all the files which are synchronized with the file it attaches to. The malware even after cleaned by anti-virus at the end-point of agent program clings to the device in cloud environment. So, there is readily need to deal with dynamic malwares.

6.2. Virtualization security issues

The reason behind the wide adoption of cloud computing in the industry is the virtualized cloud computing. Development of cloud service for business purpose, cloud provider require trust on VM. In the cloud environments, the virtualization is the primary requirements of any service. The multi-tenancy and virtualization concept provides more profit, but this concept is not free from threats and attacks. Many attacker perform co-location attack to access the services. Day by day people do research in this field to achieve proper logical and virtual isolation. The virtualization software is used to create virtualized services and images, contain several types of virus that may damage or break the virtualized code. The virtualization security issues and their solutions widely cover in this section. The section discusses several topics related to virtualization security issues, including VMs image management, virtual machines monitor, network virtualization, mobility, issues in virtual machine, and malware as seen in Table 5.

6.2.1. VMs image management

The dynamic nature of the cloud allows the provider to create, modify and copy VM images. This is possible due to the service oriented and elasticity features of the cloud. The cloud environment are a volatile environment, according to the situation the state will change. This feature can bring new issues in the cloud. The VM images are kept in the database repository. They can be easily turned off, on or suspended and save their current working state. The dynamic nature allows to user to create her own VM images or use a previously created image. One possible workaround for VM is a malicious user can upload the corrupted images that contain malware, in the repository or can find the code of the image to look for probable attack point. However, this can bring several issues in the cloud. The risk included hosting, distributing and manage VM images. On the other hand the malicious VM image observes the user activity or data resulting from them data theft or breach the user privacy. If the VM image is not properly managed then it create more serious harm to the system in the form of exposing the user confidentiality. The improper management of the VM can break the administrator password or decrease the efficiency of the VM in the form of VM sprawl. It is a situation where the numbers of VMs are continuously increasing on the host system, but previously installed VMs are in an idle state. This situation can lead resource wasted on the host machine and make complicated VMs management.

6.2.2. Virtual machine monitor (VMM)

The VMMs is well known term in the virtualization that are not germ free. It is a software component regulate all the virtual machines and their connection with the hardware. The core responsibility of the VMM is the management and isolation of each running VMs. The VMM is also responsible for the creation and management of each virtual resources. The paper (Perez-Botero et al., 2013) discuss the hypervisor vulnerabilities, along with breaking the security of the Xen and KVM. The interconnection complexities and more entry point in the VMM can promote a large number of attack vectors. The guest user required to trust on the underlying virtual hardware and VMMs. On the VMM, VMM-based rootkits attacks are possible due to the transparency of the VMM. The attack can compromise the trust model, which identify the single point of failure or malicious users on the VMM. The lack of monotonicity is another security issue in the VMM due to wrong or non linear execution path of the VMs. This issue can break the linear program execution running within the virtual machine. For example, restoring the VM or some snapshots can lose the database information, log files, monitoring data, and application setting. The separation of data from the snapshoting process can also create a security issue of data storage. The isolation, interposition, and inspection are three concerning areas in the VMMs. An attack named VM escape is referring to a situation in which the control of the VMM or hypervisor is under the attacker. The attacker can monitor other virtual machines, access the shared infrastructure, monitor the CPU utilization or can bring the VMM shutting down. Such attacks include BLUEPILL (Bahram et al., 2010), SubVirt and Direct Kernel Structure Manipulation (DKSM). The computational overhead on the VMM, VM diversity, execute malicious code, and zero day vulnerabilities are some other concerning issues yet not to be solved.

6.2.3. Network virtualization

In a real scenario, the management of physical Ethernet networks or radio networks are hard due to abundant interruption or anomalies. The traffic in the networks can produce security issues. In the virtualized network layer due to high traffic the tried-and-tested network security solutions might not work. When people move to virtualized network in the cloud environment the security of such network are down. In the virtual infrastructure the security of the Virtual Local Area Networks (VLANs) and firewalls are reduced. Many security provider provides their security service in the virtualization form. For example, Cisco Virtual Security Gateway for Nexus 1000 V series switch used as a virtual appliance on VMware.

The paper (Wang and Ng, 2010) discusses the network performance of Amazon EC2 due to virtualization. They presents the reason for the unstable network characteristic, abnormal packet delay, and unstable TCP and UDP throughput. Such abnormal nature of the network brings network holes named network tailoring and limited administrative access issue in the cloud. The above security issue and loopholes promote the attacker to attack on a sensitive portion of the virtual infrastructure and might be access the sensitive information related to users or providers.

Amazon EC2 provides their virtual machines to publicly access through a unique identifier named IP address of the user. The bridged adapter is responsible for sending, receiving and listening of incoming and outgoing network packets from the host. For checking firewalls rules, Network Address translation (NAT) modifications, and checking MAC address the bridged adapter takes some time. The above scenario creates an issue named promiscuous mode where running VM checks all the network packets that are not addressed to them. Another security issue such as packet sniffing, spoofing, and network based VM attack present in the virtualized networking.

6.2.4. Mobility

The VM cloning or template image cloning is a process of coping or moved VM into other servers. This can be sometimes create a problem because several running VMs copies of the same images and they trust on same software and initial state. This copying process propagates several errors, misconfiguration or even worst. During the copying of images contains secret key and other private information of the owner, that to be leaked to another VM. There are multiple copies of VM across the network. If an attacker takes one copy of the VM and perform attacks, it might be possible that the attacker can read the data and break the administrative password. The mobility of the VM provides the facility for quick development of VM images. This can also bring new security issues and challenges. So, people required to concern all security issues during transfer time. To solve these problems several

Table 5
A comprehensive study on virtualization security issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
VMs image management	Cryptographic overhead due to large size images	Vaquero et al. (2011)	
	VMs theft and malicious code injection	Almorsy et al. (2010)	
	Overlooked image repository	Wei et al. (2009)	A VM image management system Wei et al. (2009)
	Virtual machine transience, infected VMs	Wei et al. (2009)	VM image privacy and integrity Kazim et al. (2013)
	Virtual machine sprawl	Luo et al. (2011)	
Virtual machine monitor	Hypervisor failure, single point od failure, un-trusted VMM components, transparency of VMM, lack of monitor GUI, VMM separation, inspection, and interposition	Pearce et al. (2013) Subashini and Kavitha (2011)	HyperCheck Wang et al. (2013) DeHype Wu et al. (2013)
	VM escape	Grobauer et al. (2011)	HyperLock Wang et al. (2012)
	VM diversity, Load balancing in VMM	Vaquero et al. (2011)	SplitVisor Pan et al. (2012)
	VMM zero day vulnerabilities	Tang et al. (2012)	NoHype Szefer et al. (2011)
Network virtualization	Twofold traffic, limited network access, inapplicability of standard security mechanisms	Grobauer et al. (2011)	
	Effectiveness of network security devices in virtual network	Grobauer et al. (2011) Vaquero et al. (2011) Wang and Ng (2010)	
	Dynamic network property	Pearce et al. (2013)	Virtual network security Lombardi and Di Pietro (2011) Li et al. (2012) Wu et al. (2010) He et al. (2014)
	Packet sniffing and spoofing	Almorsy et al. (2010)	
	Virtual devices software exposure	Pfaff et al. (2009)	
	Virtualized communication medium		
Mobility	VM cloning	Duncan et al. (2012) Grobauer et al. (2011) Pearce et al. (2013)	
	VM mobility	Tsai et al. (2011)	Protocol for vTPM based VM migration Wan et al. (2012)
	Generation of untruth configurations	Jasti et al. (2010)	Live VM migration Anala et al. (2013)
	Live VM migration, man-in-the middle attack	Sood (2012)	Security framework for VM migration Tavakoli et al. (2012)
	Replay attack	Sood (2012)	
Issues in virtual machine	Vm hopping, Cross-VM attack	Jasti et al. (2010) Xiao and Xiao (2013)	
	Side-channel attack	Aviram et al. (2010) Ristenpart et al. (2009) Zhang et al. (2012)	
	Covert-channel attack	Bugiel et al. (2011) Okamura and Oyama (2010)	Secure run time environment Gonzalez et al. (2012)
	VM data exfiltration attack	Rocha and Correia (2011)	CloudVisor, secure run time environment Zhang et al. (2011)
	Memory deduplication issues	Suzaki et al. (2011)	Hypercoffer, secure run time environment Xia et al. (2013)
	Malware injection	Jensen et al. (2009)	CloudSec, detect and prevent memory based kernel rootkits Ibrahim et al. (2011)
	Entropy generation strength	Kerrigan and Chen (2012) Becherer et al. (2009) Taylor and Cox (2011)	
	Entropy depletion	Amazon Web Services Discussion Forums (2015) Carriço (2015) Patel (2015)	Exterior, a dual VM architecture Fu and Lin (2013)
	VM reset problem, consistency, re-usage	Yilek (2010)	
	VM rollback	Basak et al. (2010)	
Malware	Avoidance of malware	Chen et al. (2008) Shinotsuka (2012) Sood and Enbody (2013)	
	Spreading of malware onto VMs	Websense (2013) Katsuki (2012)	Intrusion prevention system Xing et al. (2013)
	Metamorphic engines	Staten (2012)	

security solutions (Tavakoli et al., 2012; Wan et al., 2012), and (Anala et al., 2013) are present and applied them at the VM transferring and deploying time.

6.2.5. Issues in virtual machine

The VMs in the IaaS infrastructure is the essential for each customer. But, they can create several potential threats. The VMs contains malicious accesses to different VMs related to different users by introducing the VMs to VMs or VMs to VMMs attacks. The cross VM attack (Xiao and Xiao, 2013) is implemented using two VMs on the same physical host. The attacker knows the logical address of the victim with standard capabilities. The successful attack gives various security issues, possible to check the resource usage, altered the configuration of the system and files or leak sensitive data. The author (Ristenpart et al., 2009) and (Bugiel et al., 2011) describes cross-VM side channel and covert-channel attacks in Amazon EC2. The side channel attack technique passively observes data flowing between sender to receiver without interfering. In contrast of, the covert channel attack actively observes the data flowing between sender to receiver. The attacker injects some bit in the data flow for gaining useful information. The attacker requires a square and multiply algorithm, co-residing VM and a machine learning algorithm. The square and multiply algorithm stored in L1 instruction cache. The machine learning algorithm is used to be trained to decrypt the ElGamal cipher text by using LIBGCRYPT V.1.5.0. The covert channel attack exploited the L2 cache by using CPU load. This attack allows to attacker to encode the information and gain some sensitive information such as a private key. A new attack named timing side-channels are a security challenge for researchers because they are hard to control and steal the sensitive data. Moreover, the paper (Rocha and Correia, 2011) presents a number of malicious

Table 6
A comprehensive study on Internet and service related security issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
Advanced repeated threats and venomous outsiders	Information collection, scan publicly available information	Sood and Enbody (2013)	
	Doxing	Goodrich (2013)	Property hidden
	Data exfiltration, cyber activity	Mandiant (2015)	Strong privacy laws
Internet protocols	Susceptible communication protocols, network-based cross-tenant attacks	Almorsy et al. (2010) Panah et al. (2012)	Use Secure Flag for security of the cookies
	Session hijacking	Grobauer et al. (2011) Hunt (2015)	OpenSSL Yarom and Benger (2014)
	Mixed HTTP and HTTPS data streams	Hunt (2015) Prandini et al. (2010)	Network Security Services (NSS) Shin and Gu (2012)
	Weak cryptographic key usages	Heninger et al. (2012)	Secure the server operators private keys
	Cookie theft, cookie poisoning, impersonation attacks	Panah et al. (2012)	
	TLS attack, cookie theft	AlFardan et al. (2015) Marlinspike (2015)	Use secure HTTP protocol Bormann et al. (2012)
Web services	HTTP stateless protocol, API transaction support for integrity	Subashini and Kavitha (2011)	Signed SAML assertions
	Metadata spoofing attacks, improper WSDL documents	Jensen et al. (2009) Jensen et al. (2009)	XML Encryption Saravanaguru et al. (2013)
	XML injection, SOAP wrapping attacks	Rocha and Correia (2011) Jensen et al. (2009)	XML Signature Saravanaguru et al. (2013)
	Incorrect inspection WSDL documents	Doroodchi et al. (2009) Jensen et al. (2009)	Encoding of binary tokens Chandrasekar et al. (2013)
Web technologies	Increases infected web sites	Websense (2013) Microsoft (2015)	
	XSS explosure	HP (2015) OSVDB (2015) OWASP (2015)	
	Session management, authentication break, code injection	OWASP (2015)	Real-time security updates
	HTML hidden field manipulation attack	OWASP (2015) OWASP (2015)	Video controls
	Watering hole attacks, Faulty plugin and browser	Oyama et al. (2012) Symantec (2015)	Network port monitoring Shin and Gu (2012)
	MitB attacks	Bin Mat Nor et al. (2012) Dougan and Curran (2012) Rauti and Leppänen (2012)	Web Security and Filtering
Service availability	Bandwidth under provisioning, VPSes	Cisco (2015b) Cisco (2015a)	
	Resource consumption attacks	Jensen et al. (2008) Jensen and Schwenk (2009)	Database mirroring
	UDP uplink flood attack	Liu (2010)	SANless clusters
	Direct/indirect DoS attack	Jensen et al. (2009) Jensen and Meyer (2011)	Shared storage clustering
	XML flooding attacks	Wang et al. (2012)	Use Storage Area Network (SAN)
	DNS reflection and amplification attack	Prince (2013)	Use load balancers Ferris et al. (2014)
	Exhaustion of mobile API	O'Neill (2013)	

insider attacks on the VMs. The attacker use simple plain text passwords, private key and arbitrary commands for getting the data backup copy of the VMs. The VM relocation mechanism can make possible tampering in the data. In the shared environment, another VM level security issue named memory deduplication mechanism reduces physical memory usage. This issue are oppressed in the form of memory disclosure allowing to a user can find number of file and application reside on other VMs. The cloud malware injection attack allows to eavesdroppers to insert either malicious codes into the PaaS and SaaS service models or malicious VMs into the IaaS cloud model. After inserting the malicious code, cloud execute malicious services on the virtual machine. Resulting from malicious code execution an authentic user redirect to a malicious site, which can adjust with the overall cloud VM security.

The side channel attack on the VM is a critical issue in the VM cloud. But, as pointed out this attack is not easy to perform on the VM and hard to implement by an average skilled attacker. The cloud suffers from this type of attack. The cloud security expert gives a number of solutions. But, the cloud provider does not properly implement the security solutions in their services. The practical implementation of these security solutions is not easy because it requires a number of skilled and knowledgeable security solution developers.

The VM resetting is another security issue in the VM cloud, perform on the VMware and VirtualBox. This can exploit by reusing or randomness repetition of the previous VM instances. It is initiated by compromising the Transport Layer Security (TLS) sessions and getting the secret Data Signature Algorithm (DSA) authentication key by attacker malicious executions.

6.2.6. *Malware*

The transformation of IT infrastructure into the cloud infrastructure promotes different types of malware. The virtualization and sandboxing technique in the cloud provides various advantages, but this is the open door for malware. The malware named Conficker version. B is combined with the Store Local Descriptor Table (SLDT) instruction, which can handle the VM deletion. Malware attack on the VM is hard. But, anyhow, if the attack is successful, it could have a serious harm into the trustworthiness of the VM. The growth of the malware for hypervisor in the cloud promotes the attacker to find new more easy way for an attack on the target hypervisor. However, for security of the VMs security experts provides a high level of authentication and access control mechanism. It could be possible that the hypervisor is compromised, these types of malware are still virtualization security concerns that are likely to be solved in the future. Other malware attacks on the hypervisor is possible due to the platform they run on. Many hypervisor runs on the top of windows like Virtual-PC, Microsoft Hyper-V and certain versions of VMware and some hypervisors run on top of Linux-based systems. The malware attack is possible if the security of the Linux or Windows based server is compromised. Prevention of this type of malware security experts present in IBM and North Carolina State University provides security solutions includes the hypervisor management interface is isolated from one another. It is necessary a valid and trusted system is connected to the hypervisor, the running code on the hypervisor is trusted and purify such as the

running code provided by the hypervisor providers and the use software is up to date. These solutions ensure that malware can not easily execute attacks on the hypervisor.

6.3. Internet and services related security issues

The cloud Infrastructure is not only composed with many services and resources, but also required a carrier that is transmitting the data between sender to receiver. The Internet is a carrier, transmit the large number of packets from source to destination in the form of digital data. The data are passed through a number of nodes, so it is not safe. Due to an inherited problem with the Web 2.0 many new types of threats emerged. The Internet exploits many security issues like MitM attacks, IP spoofing, port scanning, malware injections, and packet sniffing. The cloud services is accessed and managed over the web and standard web browser, that is not a safe solution to the end users. There are many security solutions are available but still people assume that transferred data through the Internet is not safe. The following issues and corrective solutions are discussed in this subsection that is summarized in Table 6.

6.3.1. Advanced repeated threats and venomous outsiders

The Advanced Repeated Threats (ART) belonging to an attack model consist three phases: The first phase says about the method and procedure for information gathering. In this phase, the attacker finds all the related information about the target server. The attacker uses public or private intelligent source for information gathering, known as Open Source Intelligence (OSINT) gathering. The second phase known as the threats modeling phase. In this phase, an attacker maps the target server and finds the best way or technique for the attack. Finally, in the last phase attacker performs her attack on the target server.

The above discussion clearly says that the information gathering phase is the most important phase for a successful attack. It is important for the attacker, she knows where and how the attack is performed. Thus, it is a concerning point for the business people what type and how much information is provided publicly. Sood and Enbody (2013) presents the conditions in which the AWS security is compromised.

6.3.2. Internet protocols

The web based cloud infrastructure used different protocols and standard stacks such as the TCP/IP stacks for the communication in the Internet. The Domain Name Server (DNS), Internet Protocol (IP) and Dynamic Host Configuration Protocol (DHCP) are the well know vulnerable protocol used in the Internet, that may create different types of network based attacks. For example, the botnets used fast flux technique in DNS to hide the IP addresses of phishing or malware delivery sites behind a constantly-changing network of compromised hosts acting as proxies.

The delivery protocol HTTP is a stateless protocol and does not provides any guarantee for delivery of service. The HTTP protocol and many web applications use session handling technique for secure communication. The session riding and session hijacking is such vulnerabilities happening inside when people handle session technique. Most of the website implements HTTPS in the wrong way. For example, sites implement HTTPS only for sensitive information such as login form and remaining whole session implement over HTTP. Such sites do not give guarantee security at all because the session can be hijacked during HTTP communication, known as the mixed content. A session cookie is used for creating cookie poisoning and impersonation attacks. The HyperText Transfer Protocol Strict Transport Security (HSTS) is an enhancement of ForceHTTPS, define under Request For Comments (RFC) 6797. It give instruction or restrict to its web users to interact with the web sites under secure connections.

The PaaS web service and APIs use another delivery model like SOAP (Aihkisalo and Paaso, 2012), REST, Remote Procedure Call (RPCs). But, All the web service delivery models have some security issue that is still a challenge for researchers.

6.3.3. Web services

In the distributed system, the main problem is data integrity. But, in the cloud computing due to Service Oriented Architecture (SOA) approach the problem of the data integrity can be solved. The cloud computing web service normally use XML and APIs to enhance own functionality. Most of the SaaS vendors deliver their web services through insecure APIs. These APIs do not provides any transaction report. This can increase the data integrity issue across multiple cloud services. The functionality of the web service is describe by the WSDL language. The language specifies how to call them, what parameter to pass as input and what is the result. This re-engineering meta data information can create various issues such as metadata spoofing attacks and man in the middle attacks. In the clouds, the WSDL documents are accessible dynamic and spread over the network, resulting from that the attacker performs a successful attack. So, required a attention when web service provider combined cloud technologies with the web services. In the paper (McIntosh and Austel, 2005), describe XML based Signature wrapping attacks or rewriting attacks with their solutions. The wrapping attacks are referring to the process in which eavesdropper captures the SOAP messages and inject false or forged messages in the XML field to access the web resources. In 2009 Amazon suffers from wrapping attacks. The authorized SOAP messages is captured by the eavesdropper and he/she put own signature and the signature is correct. Resulting this attacks the eavesdropper access multiple Amazon EC2 services. SOAPAction spoofing modifies the HTTP header and XML injection attacks are such issues that can to be solved in the future.

6.3.4. Web technologies

Most of the cloud application and services are accessed by the web based agents (e.g., web browser). The malicious web links and web sites continuously increase malware in the cloud web environment. In the web, day by day number of connected people and devices has increased. This can attract to the attacker for the attack vector. The most general web vulnerabilities in the Open Source Vulnerability database (OSVDB) websites over the years. In 2012 HP says that Cross-Site Scripting (XSS) attack is the most happening attack in the web.

The Open Web Application Security Project (OWASP) is an organization provides security guidelines to web developers for building a secure web application. The OWASP (2015) describes most happening critical web application risk in 2010. According to this report, the code injection is the top most risk and XSS is the second. Later, in 2013 OWASP presented security risk report. In this report, the code injection issue is the top most issue, broken authentication and session management is the second and third issue respectively. The Structured Query Language Injection (SQLi) known as blind SQLi contains the injection threats. Another web technology issue is cookie theft and hidden field manipulation attack. The hidden field manipulation attack allows the attacker to change HTML hidden field according to own needs. The HTML hidden field is used for exchanging and control data from a web page to web server.

Generally, the company employee browses social network sites, personal email accounts, and other application site during work time. This extra browsing may produce risk for the enterprise because it is the entering point for the malware into the enterprise through the web browsing. In this scheme, suppose user login into the cloud for access cloud services after few minute he do some other extra browsing activity. This activity can breach the privacy of the user. The Man-in-the-Browser (MitB) attacks another security issue related with browsers and plugins. URL-zone, Torping and Zeus are some malware related to the MitB attacks. The phishing attacks, Zero-day vulnerabilities, and watering hole attack (Symantec Security Response, 2012) are most common issues during accessing the SaaS applications.

6.3.5. Service availability

Nowadays DoS attack is very commonly seen in the organizations. For example, the Blue security organization opens new anti-spam security service called Blue Frog after coming DoS attacks. The data center has a large number of connected data server and other resources. Hence, to support large amounts of network traffic, it is required a proper bandwidth and network security. The Cisco company found the bandwidth under provisioning is one of the main issue in the data center. They identify in the data center the large server cluster is implemented with factor 2.5:1 to 8:1. The factor compares the network capacity of the data center with whole capacity in the data center due to several loads. The cloud is the backbone of the data for many organizations, suffers from different types of issue like bandwidth under provisioning and flooding attacks, can supply a massive impact in an organization.

The flooding attack directly affect the available network bandwidth, memory and processing power. In the case of botnet, an attacker can send millions of TCP SYN packets in a successive and quick manner to the target server. This situation creates DDoS attack. The DoS attack can be possible in three scenarios. In the first case, the target server process either large number of requests or process a single malicious request. In the second case, the attacker fully captures or hack the network link, sending many bogus requests. This bogus requests captures the whole network bandwidth. In the third type of DoS attack, the number of immediate routers process large number of bits.

The paper (Liu, 2010) propose a new type of cloud DoS attack. The author found an uplink bottleneck in the network topology with minimal cost. Before the attack the attacker gains the topology information and other host related information to maximize the attack effectiveness. The attacker uploads many UDP packets for captures the network traffic.

In the cloud resource exhaustion is another form of attack on the web services. The oversize payload attack aim is to increase the memory consumption of parsing XML objects into memory Document Object Model (DOM) objects. The name-space vulnerabilities named coercive parsing is aiming to consume more CPU during XML parsing. The obfuscation attack, over-sized cryptographic attack, and WS-addressing spoofing attack increases overhead on the CPU and consume more memory usage during execution of business process.

Another service related issue is the API consumption by mobile device applications. The cloud user consumes many services by mobile applications via cloud API. If a target server API suffers from DoS attack, the application user unaware of this attack. The result of the application running on the mobile device is either slow or give different errors such as HTTP 404.

6.4. Network security issues

The network is the basic component of the cloud computing. So, issues are not only present in the VM, service, or application level, but also alive in the network level. The network level issues can directly affect the cloud system. The cloud network nature is dynamic, so the issue is considered both internal and external networks. Any user can perform a DoS attack to affect the availability of the service. This can also affect the network bandwidth and increase the congestion in the network. For connectivity of the user and the service, the network perimeter is changed. The network protocol will also change like it can move from Routing Information Protocol (RIP) to Dynamic Routing Protocol (DRP). Hence, in the current context of network security need to adopt new trends. This can be enhanced in mobile based device and virtualized networking. The dynamic nature and new trends of network enhance the many security issues that can be categorized as mobile platforms and circumference security as shown in Table 7.

6.4.1. Mobile platforms

The concept of Bringing Your Own Device (BYOD) is sometimes is harmful for companies. The company employee uses their own device to access the enterprise applications. This concept is helpful from a productivity viewpoint, but arise security threats. Many cloud users use smart-phones for accessing the SaaS cloud applications and services. This mobile devices not only produce harmful malware, but also vulnerabilities. The HP presented a report in 2012 states that mobile platforms are the major area that produce several malware. The rooting or jailbreaking smart-phones, further enhance the security threats because this type of threats can easily access kernel parts. This rooting facility in smart-phones permits the users to install fancy applications. In the installing process application can access other parts of the operating system. Hence, a harmful application can access the sensitive components of the operating system including protected data. Furthermore, after factory resetting the data left in the mobile phone arises data leakage issue. The phone recycling concept not only leak the user private data, but also company data. So, the company does not support the BYOD paradigm. Accessing the cloud services using a mobile device raise a security issue that has been unsolved.

6.4.2. Circumference security

In the cloud computing, the perimeter security is a combination of static security controls. The dynamic network security is composed with network security devices are placed in network traffic entering point and on the gateway. This security approach assumes that the network infrastructure is static, but nowadays this not possible. The BYOD concept is changing the security requirements of the network and require an open boundary-less connectivity for cloud services and applications. The VMs use Internet for delivery of services, migrate one place to another place whenever required. The big issue in the cloud is to achieve sufficient security in the dynamic network. There are provided some standards and control mechanisms, but this does not fulfill all security requirements. There are many obstacles arise during the design of cloud network security. For example, a TCP connection table that hold all TCP connections is handled by a firewall. Now suppose, VMs is outside of the firewall and access by an external customer. If the VM is migrating to another place in the cloud, which changes the routing path or firewall security. The security firewall did not know the connection might drop and requires a connection for security purposes. In this case, malware can spread itself from one network to another network in multi-tenant clouds.

6.5. Access control issues

The access control security is refers to the protection from unauthorized read/write permissions. The access security is maintained by authentication with combination of an Email ID or username and password. In the multi-tenant cloud environment have a large number of customers. Each customer's access cloud services using websites or front-end interface. The web technology or websites are an attack door. So, people required some access control mechanisms. To solve this issue, it is important to separate and provide different authorization to each component either logical or physical from one another. The issues and corrective solutions related to access control is summarized in Table 8.

6.5.1. Physical access

Data centers is a database house whose contains a huge amount of data in a single point. The actual owner of the data center is some other business organizations that gives data center on rent basis to the provider for their business profits. Due to the access security issues in the cloud data centers any organization does not give full physical security. The security issue is explored in the form of data leakage in the data center. The data center developer considers all aspects when they develop data center to achieve proper security and protect information for the long term. The security issue does not derive only by outsider person, but also insider person can create more serious

Table 7
A comprehensive study on network security issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
Mobile platforms	Generation of mobile malware	Cisco (2015a)	
	Extension of mobile vulnerabilities	HP (2015) Li and Clark (2013)	Intrusion detection system to protect mobile platforms Yazji et al. (2014)
	Rooting and jailbreaking, rootkits, openness of privilege	–	Mobile security Li and Clark (2013)
	Cloud syncing mobile applications vulnerabilities	Grispos et al. (2013)	
Circumference security	Immobile network infrastructure		
	Open network perimeter	–	
	DMZ assumption	–	Network security for virtual machine
	Firewalls limitation, limited mobile connection	Shin and Gu (2012)	Cloud network security using tree-rule firewall
	VMM network sniffing and spoofing	Prolexic (2015)	He et al. (2014)
	Security threats in logging, insufficient monitoring system	Grobauer et al. (2011)	Security for dynamic cloud network Shin and Gu (2012)

harm called the malicious insider, can access or control the internal physical security. A malicious insider, unpleasant person, ex-employees or malicious system admins can access very sensitive information stored in the data center and leak this sensitive information to breach the user privacy. There are more serious attack in term of cold boot attacks and hardware tampering. Henceforth, to secure the data center it is mandatory to deploy security mechanisms along with Access Control List (ACLs).

6.5.2. User credentials

Large companies use Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory (AD) technology for management of user credentials, authentication and authorization purpose. This access management server can be placed either within the cloud provider organization or outside the organization using a firewall. In a large application user management overhead is increasing because there are a large number of users and each time required to add, delete, modify, activate and deactivate user accounts. Each new time a new credentials are added in the directory so management of user credentials is a complex task. This can give results in the form of loss of control. The security of the directory is also an important task. The weak password recovery mechanism and credentials reset is another issue in the accessible directory. Service provider always concern about the security of user credentials because if the user credentials are stolen, then attacker can access all the credits and sensitive information. If any company loss her employee credentials, then it is possible to monitor or manipulate employee data. The replay sessions and malicious redirects are some issue that has most likely happened.

Table 8
A comprehensive study on access control issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
Physical access	Malicious insiders	Yu et al. (2012),Zou and Zhang (2011)	Use eXtensible Access Control Markup Language (XACML) expressing access policies
	Malicious system admin	Kandukuri et al. (2009),Santos et al. (2009)	
	Cold boot attack,hardware tempering	HP (2015)	Secure data access Sanka et al. (2010)
User credentials	Load on IT management,LDAP and AD servers location	Subashini and Kavitha (2011)	
	Weak credential reset methods	Grobauer et al. (2011)	Attribute based encryption Wan et al. (2012)
	Phishing attack,key-logger attack,man-in-the-middle attack,replay attack,sessions hijacking,	Behl (2011)	Use Heirarchical Attribute Set Based Encryption Wan et al. (2012)
	User to root attack	Modi et al. (2013)	
Entity authentication	Archaic static password	Hart (2009)	
	Inapplicability of alternative password schemes	Dinesha and Agrawal (2012)	Hierarchy identity based cryptography
	SAML explosure	Baier et al. (2010)	ID management framework
	XML SAML wrapping attacks	Baier et al. (2010)Somorovsky et al. (2012)	Decentralized access control for cloud storage
	QA explosure	Grosse and Upadhyay (2013)	SMS based password recovery
	Account lockout	Grobauer et al. (2011)	
Authorization	Data mashups, inapplicability on centralized access control	Chow et al. (2009)	
	malicious third-party applications	Chow et al. (2009)	Role based multi-tenancy access control Mon and Naing (2011)
	Insufficient or wrong authorization assignment	Grobauer et al. (2011)	Multi-tenancy authorization model for collaborative clouds Tang et al. (2013)
	URL guessing attack	Grobauer et al. (2011) OWASP (2015), OWASP (2015)	
Management of user identity	Synchronization leakage, federation IDM trust and validation	Subashini and Kavitha (2011)	Claim based identity management system Singh and Chatterjee (2015)
	Complex and fine grain synchronization	Sengupta et al. (2011)	Use trusted third party as an identity provider, identity management framework
	Distinct identity token and negotiation protocols	Baier et al. (2010)	Digital identity management Chow et al. (2012) User Managed Access (UMA) protocol Dhungana et al. (2013)
Anonymization	Hidden identity of adversaries	Xiao and Xiao (2013)	Use a strong and secure anonymization technique that is not easily de-anonymized
	De-anonymization attacks	Backstrom et al. (2007), Narayanan and Shmatikov (2009)	

6.5.3. Entity authentication

In the cloud require authentication technique to achieve a secure access to cloud applications. A weak authentication mechanisms make cloud attacks such as brute-force and dictionary attacks. The cloud service provider provides different authentication technique such as simple text based passwords, one time password, graphical password, third party authentication, 3D object password, and biometric password. The provided authentication technique has some security faults. They are not provides complete and secure authentication. Each cloud customers owned different cloud service. For accessing different services require different logins. Resulting from that poses many security challenges. In this scenario, it is more difficult to implementation of a strong user authentication technique as user requirement. The management and creation of multi-level authentication technique for different cloud services to different users is a more complex task. The Single Sign On (SSO) provides solution to these types of issue. The Advancement of Structured Information Standards (OASIS) provides an open standard Security Assertion Markup Language (SAML) for making SSO authentication technique. The provided open standard allows two people to exchange the authentication and authorization parameter. Google provides a shared XML based authentication technique, provide authentication across different services running on different servers without re-authentication. But, this technique creates different attacks such as impersonate and wrapping attacks. Most of the authentication technique has password reset and account ownership proof phase. In this case, for resetting the password require a finite number of answers and if the answer matches the user account is hijacked. To address this issue a Short Message Service (SMS) based password recovery is a better solution.

6.5.4. Authorization

Authorization is the process of granting or denying permissions to a person or system. In centralized system, it is very easy to handle and have several advantages. But, in multi-user computer system, the scenario is a complex task. The large number of data and users can create security implications in term of data leakage. In the cloud, the deployment of authorization mechanism for each user is a complex task. The malicious application can access the resources that are prohibited and perform malicious activity. A third party may be access the cloud based services. Suppose, one can authorized to third party to access cloud based services. For example, Facebook does not have facility to verify the outside applications that use Facebook uploaded data. This scenario is very harmful to cloud, but many social networks are based on this scenario. It is easier to access the privileges and intelligence. This has happened due to insufficient or faulty authorization checks.

6.5.5. Management of user identity

The Identity Management (IDM) is a mechanism to identify and manage the user identity, cloud objects, organizations account and provide access authority for the resources according to the administrative policies. The identity management system supports three different models, namely the independent IDM stacks, credential synchronization, and Federated IDM. The independent IDM stacks is highly configurable and secure used for storing the user credentials and other user related information. The credential synchronization maintains replicating user account information and access control ability to the provider. This model creates many threats such as account information leakage during storage and replicate the data to the provider side. The Federated IDM is a concept of SSO authentication allows to users to link one account to multiple IDM system for authentication. But, this can create trust, validation and interoperability issue that happen from using different identity token and protocols.

6.5.6. Anonymization

The anonymization is a technique of destroying tracks, or the electronic trail, on the data. An electronic trail is the information about the sender when he sends data over the network. This procedure cuts the semantic links of the data to their original origin. This can be increased the user privacy. In criminal cases, expert tracks the data origin and find the information of the actual sender. So, required to implement a layer of security into the database. There are many techniques in the cloud for achieving the privacy using anonymization techniques. There are required to implement an anonymization system that ensures the privacy of the user. The anonymization system provides facility-identity information of the cloud customer should be hidden and not be disclosed in front of any other person. There are de-anonymization attack, active attack, and passive attack those can breach user privacy on the basis of user origin knowledge. It is proved that anonymization data can reveal the identity of the user. So, this is an important security issue that still not to be solved.

6.6. Software security issues

Software security is the very concerning point in the current situation. Nowadays, people write each software program in own ideas and use different programming language, such software program have thousand or millions of lines of code. So, that is the reason people unable to measure the software security in the system. Even developer follows the set of rule and constraint, a single bug can be counter a security problem. The survey categorized the system software issue in two subcategories. First is the platform and frameworks related

Table 9
A comprehensive study on software security issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
Platforms and frameworks	Isolation between platforms, safe thread termination, resource monitoring	Rodero-Merino et al. (2012)	
	Uncertain system calls and imperfect memory isolation	Almorsy et al. (2010)	Multi-tenant software platform security Rodero-Merino et al. (2012)
	Bad SDLC mechanisms	Martin (2013)	
User frontend	Exposure of frontend interfaces	Ahuja and Komathukattil (2012) Grobauer et al. (2011) Pearson (2013) Tripathi and Mishra (2011)	
	Imperfect configurations, unauthorized access	Grobauer et al. (2011)	
	Application drawbacks, masked code injection	Subashini and Kavitha (2011)	
	VMM management consoles exposure	Wu et al. (2010)	Lightweight intrusion detection Azmandian et al. (2011)
	Trust on programmers	Staten (2012)	Implementing malware solutions King and Chen (2006)
	Open-source software, reverse engineering procedure	–	

security issue and second is the user interfaces. The survey is summarized in Table 9. The tabular analysis shows several issues and their solutions related to user interface and platforms.

6.6.1. Platforms and frameworks

In this section, provides a deep study regarding PaaS. The PaaS provides a sharing based platform for deploying the cloud application and support various languages that is helpful for developing the cloud application. Each platform has some security issue like resource metering, platform isolation problem, and safe thread termination. Java implementation developer use sandbox provides program isolation, byte code integrity, and encrypted secure communication. The most meaningful way to create isolation is to use individual JVM for each program, but this way the memory is much more consuming and another problem is it is not secure or providing security is a complex thing. Another way to implement the isolation is to use standard Java capabilities- a security control manager that control one class loader per application. This approach isolates one class from another, but problem behind that it does not prevent leakage of data information and safe thread termination. So, researcher finds more secure isolation software and platform. The multi-tasking virtual machine, isolation based KaffeOS, I-JVM, and heap based protection some contribution that provide the isolation. In terms of resource accounting no such language provides this type of facilities. The .NET Common Language Runtime (CLR) phenomena provides a more secure isolation between two different application domain.

6.6.2. User front-end

A consumer access the IaaS and SaaS services by the use of standard user interface through the Internet. The user front-end has capabilities that manage and monitor the usage services. According to user authorization the interface may be changed. For example, administrative purpose interface is only accessible by only a privileged administrators person. In the cloud environments, an interface is by default is a gateway access through the Internet. It is an attractive door to enter in the cloud. This interface used by the attacker to perform their attacks. Imperfect configurations, deficient applications, unauthorized access, and injecting masked code is such issues that break the system security firewalls and barriers. The front-end interface is deployed for administrators, used for management of VM and VMMs. Such console can bring injection and cross site scripting attack due to remotely access.

6.7. Trust management issues

Trust is a non measurable parameter in cloud computing. It must be present in between the customer and the cloud provider for outsource their business and data. In addition, the trust also related to the resources those are used, including storage device, web based access, computational algorithms, virtualization mechanisms, etc. There are many reasons for an unsuccessful trust established between two parties. The trust plays an important role for any system. It is not only for a cloud system, but also required in distributed networks, peer to peer networks and sensor networks. The Table 10 summarized trust security issues and their solutions related to the cloud security system.

6.7.1. Cloud to cloud trust

In the cloud infrastructure, trust is an important aspect for the security of the business related application and service. Day by day cloud technology is improved. So, for improvement of the technologies, trust is an important parameter those are considered at the improvement time of the cloud. The cloud computing services, business applications, communication technologies is very dynamic. It changes according to the user and provider requirements. This is the characteristic of the cloud computing. But, this creates trust breaching and other issues. So, people required a more trustworthy model in the cloud. Many technologies such as Virtual Private Network (VPN) allow to its remote user to access internal resources for other external places. This kind of approach the application and other resources required a strong trust mechanisms.

The above discussion clearly says that in the cloud business model, if trust are broken down it create serious harm to the system. Many organizations design a restricted secure network in its location. But, if any user proof the validity and truth for the system then the provider network allow to user to connect to the network and give permission to access number of applications, services and other instances of the network. This can generates trust issue related to storage, computation and access to cloud instances, known as the malicious insider.

6.7.2. Human aspect

The generator of all problems, threats and issues are human. Human design and implement each application and services according to own requirements. The result from this human nature create some faulty result and serious harm in the system. In the cloud computing model, the data and information are travel from one location to another location. For this still required a defensive trust model. For organizational point of view the important thing is organizations trust on their employees. For completion of their duty employee access number of resources. But, in this approach organization can not filter human nature. In a data center number of assets is maintained by employee. The employee nature leads number of problems because they create an error or negligence. The user password is an important factor for care of user private data and services. But, due to heavy load most of the user trust on co-worker or friends and they share her/his password with them. Due to this trust approach if the password is open or disclose then the whole system security is broken. The social engineering is another issue in the trust model. The understanding of social engineering is change person to person. If a security expert gets phishing email, then based on their subjective knowledge and past experiences they can find phishing emails. But, a normal Internet user can not find phishing emails and he/she easily phished.

6.7.3. Reputation

The different cloud customer uses different VMs, but they are hosted by the same machine. Single hardware assets are shared among multiple users. Thus, different user activity and behavior can affect each other reputation. There is an issue known as reputation isolation and fate sharing. The cloud system may affect the user services and resources, if the cloud system is corrupted. Additionally, all malicious people get benefits from the services and resources. If any spammers or malicious activity disturbs the cloud system, the cloud provider have facility to block the activity. Many cloud customers suffer from the reputation isolation issue and faced different challenges, if they do not know about malicious activity.

6.7.4. Trust on the auditability reports

In the cloud environments, the virtualized guest OS allows to third party auditors perform a number of tests to find the health status of the assets. The auditability is hard cause of the cloud provider may not provide the complete information of their assets. The audit technique provides the complete information about service conditions, check all access and events, record and maintain logs, and monitor intrusions. The auditability makes easy to user or provider to identify the status of the service. The user and provider give this auditability responsibility to other trusted third party auditors. Suppose, a user trust on auditability reports and if the auditor compromised with the service provider, produce wrong reports. For the complete security of the service trust on the audit reports is not sufficient.

6.7.5. Anonymization

In the cloud infrastructure, it is required for the customers to trust on their service providers. The service provider security control devices

Table 10
A comprehensive study on trust management issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
Cloud to cloud trust	Invalid enterprise trust model	Amoroso (2013)	Cloud Trust Authority provides security of the cloud services from multiple providers Habib et al. (2011)
	Cloud environment openness	Gharehchopogh and Hashemi (2012)	Use different trust models Xu et al. (2015)
	Un-trusted employees		
	Password sharing	–	
Human aspect	Password strength and commonness	Townsend (2009)	Public Key Infrastructure based trust model
	Social engineering	Doel (2013)	Evidence based trust model
	Phishing attack	FireEye (2015) Lineberry (2007)	
Reputation	Isolation of reputation	ENISA (2015) Monfared and Jaatun (2011)	Reputation based trust model
	Fate-sharing	Chen et al. (2010) Roberts and Al-Hamdani (2011)	SLA verification based trust model
			Evidence based trust model
	Providers reports truthfulness		Policy based trust
Trust on the audit-ability reports	Jurisdictional audits, court system	Gonzalez et al. (2012)	Use cloud auditor's assessment
	Data locality	Chen et al. (2010) Zhou et al. (2010)	Accreditation by Auditing Standards Board of AICPA
	Lack of privacy capable audits techniques	Roberts and Al-Hamdani (2011)	
Anonymization	logs anonymization	–	LKC privacy model Mohammed et al. (2009) Data Anonymization Sedayao (2012)

record each activity and produce logs. Based on the trust user think the provider does not disclose these logs and logs cannot be compromised with other malicious user. But, if the logs are compromised or unclosed by the service provider. Then these logs can produce useful information to the other malicious user, such as the VM location of a particular user can produce various attacks on the VM. So, in the trust model require an additional layer of security.

6.8. Compliance and legal security issues

The SLA is a document plays an important role in the cloud business model. It contains an agreement between the two communicating parties, all service related information, and terms and conditions of the service. The SLA is signed by the both parties to show they are agree with this agreement. The Table 11 shows some compliance and legal security issues and their solutions. The issues arise when people disagree or break the agreement.

6.8.1. Forensics

In the recent years, the digital forensics is a form of computer forensics emerged in the cloud computing for making the auditing tasks. The aim of development of this field to identify the potential digital threats and fight with cyber crimes by use of digital analysis techniques. The applicability of digital forensics in the cloud infrastructure is a complex task due to the dynamic nature of the cloud. The cloud data is moved from one place to another place, rather than stored in a physical storage. This issue does not provides isolation of a particular resource, known as the data locality issues.

From the consumer point of view, data seizing and data disclosure issue compromised user privacy and confidentiality. The web browser history and cache, presents different forensics issue in the cloud. The BYOD concept also brings new threats because they sense user private data or business data. The cross-platform SaaS application concept is a barrier for the development of an appropriate and applicable platform for cloud devices. The barrier defines in terms of data collection, resemblance, and data verification. A malicious user can use digital forensic techniques to find out the complete history of the virtual machine including user services, user credentials, IP addresses, and security protocols runs on the VM.

The issue hardware confiscation arises due to law of enforcement. The security experts concern number of issues in the clouds forensics part such issues are unsound forensic data in the virtualized environment, lack of validation for disk images due to computational overhead or lack of cryptographic mechanisms, and evidence acquisition.

6.8.2. Acts

The cloud technology is a new technology, the used cyberlaws and acts does not completely secure the cloud systems. From the cloud user's point of view, the old and outdated cyberlaws may breach the user privacy. The cloud data migrate from one country to another country and the different country follows different rules and laws, may create a clash between rules. For example, the cyberlaws named Personal Information Protection and Electronic Document Act (PIPEDA) in Canada and Data Protection Directive in Europe clash with cyberlaw of USA named USA PATRIOT Act (UPA). Other concerning example includes older privacy acts, old regulation, out of date and inapplicable rules affect and leak the user and business information in the new cloud scenario. The classical acts like Electronic Communication Privacy Act (ECPA) of 1986 and UPA of 2001 are failing to protect the user private data. This old act has an impact on cloud business model because it is required each entity work legally.

6.8.3. Legal problems

The dishonest or malicious operations in the cloud promote the legal agreement issues. The multi-location is a characteristic of the cloud computing allows to cloud providers to spread the data and resources in all over the world to provide the high availability of the services and information. But, this paradigm creates various issues because many countries do not allow data and information goes outside their boundaries. In some cases, during data transfer, it cannot identify the which country administration the data decline. In Some scenario, if some accident takes place, it is hard to identify which party is responsible.

The SLA is a contract between consumer and provider specify a list of requirements for the entire duration of the service. Both parties agreed with level and quality of the services. Accidental resource allocation, availability issues, dishonest computing, and data loss are critical issues raised when people do not follow the SLA rules and regulations. Solutions of such issue are hard to find for both consumer and provider.

In the services usage context, the different interest between different cloud users arise new security issues. The transitive issue affects the SLA consistency between different cloud providers. Thus, the cloud user is unable to find legal or trusted service providers.

Table 11
A comprehensive study on compliance and legal security issues and solutions.

Security topic	Security issues	Studies/survey	Security solutions
	Cross platform forensic techniques, public cloud, data locality, legal authority	Taylor et al. (2011)	
	Data collection and verification	Chung et al. (2012) Taylor et al. (2011)	
	E-discovery, Data seizing and confiscation	Gonzalez et al. (2012) Taylor et al. (2011)	
Forensics	Forensic data unsoundness rendering due to virtualization	Chung et al. (2012)	Use Oruta (one ring to rule them all) approach Wang et al. (2012)
	Lack of validation for disk images, weak encryption scheme	Dykstra and Sherman (2012)	
	Evidence acquisition	Dykstra and Sherman (2012) Taylor et al. (2011)	
Acts	Outdated acts	Zhou et al. (2010)	Asia Pacific Economic Cooperation (APEC) privacy framework
	Privacy breaking acts	–	
	Data jurisdictional borders	Chow et al. (2009) Kaufman (2009) Monfared and Jaatun (2011)	
	SLA breach	Pearson (2013)	
Legal problems	Providers compliance evidences	Khan and Malluhi (2010) Xiao and Xiao (2013)	
	Providers and customers have different interests	ENISA (2015)	Need an appropriate SLA for data privacy
	SLA consistency and truthfulness	Chow et al. (2009) Pearson (2013)	SecAgreement Hale and Gamble (2012)
	Blocked lawful data	Habib et al. (2011) Monfared and Jaatun (2011)	
	Attack on QoS property	Jensen and Schwenk (2009)	
Incorrect resource usages metering	FRC and EDoS attacks	Idziorek and Tannian (2011) Idziorek et al. (2011) Xiao and Xiao (2013)	
	Un-trusted computing, break protocol	Aguiar et al. (2014)	Trust model based on QoS Manuel (2015)
	Randomly billing	Sekar and Maniatis (2011)	
	Vendor lock-in	ENISA (2015)	
Governance	Data migration, price growth, security and reliability problem, service termination, provider termination	Armbrust et al. (2010) Gonzalez et al. (2012)	Need to frame unified regulatory compliance
	Race-to-the-bottom	Armbrust et al. (2010)	

6.8.4. Incorrect resource usages metering

The business model allows for its customer to rent the bandwidth, service and resource usage on the basis of pay as you go manner. The cloud customer takes number of resources on the rent. This can arise flooding and resource exhaustion attack. The billing and accountability issue of the target running services continually increase in the cloud. A more profound and ambiguous attack called Fraudulent Resource Consumption (FRC) is a pattern of an Economic Denial of Sustainability (EDoS) attack. It increases the price of the services or possible financial loss of the consumers. The attacker sends large number of request for consuming the bandwidth. The FRC packets are hard to identify and classify. To achieve the measured services it is required the accounting of the bandwidth, storage and computing is correctly. They follow three properties named identity binding, execution verification and tamper-evident logs. The unreliable computing disagrees the SLA conditions, encourage wrong accountability systems. The wrong resource consumption metering produces an inaccurate bill or charge additional cost. Thus, the customer point of view it is hard to find the produce bill is correct or wrong.

6.8.5. Governance

The governance issue is the last and the more subjective issue in the cloud. In this issue, the cloud user looses the administrative power, operational, and security control over the cloud system. The vendor lock-in issue is another issue in the governance. The different government policy between different cloud still faces security, privacy and standardization issue. The interoperability in the cloud infrastructure creates protocol, data format and API related security issue. The data migration, service quality, service validity, government policy, price increasing, reliability, provider business termination and race to the bottom is some governance issue that still a challenging issue in the cloud.

7. Discussion and open issues

The previous section describes security issues related to the cloud. It enables to understand the cloud have not only some security issues, but also have a large number of security issues that may arise due to adoption of new cloud technologies. The security issues related to cloud communication, network, data privacy, application, and web services are some traditional issues that are present at the beginning of cloud computing. Security issues that emerge due to multi-tenancy, Virtualization, and shared pool resources are innovative security issues. In a cloud computing environment, several services and resources are available, but security level of the resources depends upon the sensitivity and value level of the resource. For example, the data security of the cloud computing is more important and it is difficult to deal because of the data owner loses the control over the data, when data are transferred/stored to the cloud.

There are several research gives her effort to solve the security problems in a cloud environment. But, still there are many open issues are present that is needed to be solved for providing a secure cloud infrastructure. The first and more important open issue is to design an extensive and integrated security solution that may fulfill all major security requirements in the cloud. Each researcher focuses on a particular security issue and solve the issues in its own way. The research on specific issue and solve the issue may result multiple security solution to a specific issue. In a real scenario, it is not feasible to implement multiple security solutions for a single issue. Employment and arrangement of several security solutions itself may be dangerous. A common and more integrated security solution is more secure and easy to implement in the security tools.

Multi-tenancy provides a sharing environment in cloud computing enable the sharing of the resources among multiple users. The sharing environment in cloud computing may pose new security threats. Security and privacy of the multi-tenancy in cloud is still one of the

most open security issue. The research finds the number of solutions in this area, but the solution is not sufficient to solve all the issues.

The concept of a shared pool of computing resources, design a reliable access control system. The access control system restricts the illegitimate access to the cloud resources. The heterogeneity of the services and dynamic allocation of the resources makes an access control system to be more complex. Management of user identity and credentials is a challenging issue in the cloud. The transformation of business identities to cloud specific identities and the transformation time in this process is a key factor that affects the efficiency of the cloud system. Moreover, future enhancement is to compose assurance and auditing tool to ensure better identity management and access control system.

The privacy of the computation is another open issue in cloud computing. In the storage most of the data are in an encrypted form. But, in the storage all the operation are not performed over the encrypted data. Most of the operation required plain text data during computation. The memory is assigned to the within or outside processor used for storing temporary data may be the target of attack. Therefore, research endeavors in this respect to find a broad solution that provides privacy during computation time.

Due to many security and other reasons the cloud customer migrates their assets to other cloud. The migration of the assets to other cloud is not an easy task. For migration there is a need of some standard protocol and standardized formats those support cloud format and help to the customer to migrate their data and application to other cloud.

The cloud computing also needs a security solution against insider threat. There are many solutions are available and still applicable to the cloud. But, the available solutions are not sufficient to solve the insider threat. In these phenomena identification of the insider attack in cloud computing is an open area of research. In this scenario, develop an indicator that help to find the insider attacks. This indicator will increase the potential of securing the cloud system. Similarly, another open issue is to identify who is the normal user and who is the malicious user, still have a problem in a cloud environment.

Lastly, the legal aspect related to SLA is still an open unsettles issue in cloud computing. The issue of auditing, the service level is met as was promised in SLA or not, needs to be explored. Run time assurance mechanisms provides a facility to deliver the services as per requirement. The current auditing mechanisms provided by the CSP itself might not be a satisfactory option for many cloud users. Moreover, the pricing of the usage service totally depends upon the CSP. The work in this area will greatly help the user to adoption of the cloud.

8. 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. The cloud computing utilizes many traditional as well as novel technologies. This emerging technologies can create many cloud specific security issues. Multi-tenancy and virtualization feature of the cloud give its user to access the same physical resources from different locations. The absence of proper isolation between VMs can hamper the security of the system.

In this paper, we have discussed about the basic features of the cloud computing as well as the security issues that originate due to the virtualized, distributed, shared and public nature of the cloud. Subsequently, the paper presented different counter measures to address the security issues at different area in the cloud. The tabular presentation of the security attacks, threats, issues and its solution will greatly help to the readers. At the last of the paper, the discussion of some open issues in the cloud will motivate the researcher and academia to focus on the subject.

References

Abbas, A., Khan, S.U., 2014. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE J. Biomed. Health Inform. 18 (4), 1431–1441.

Aguiar, E., Zhang, Y., Blanton, M., 2014. An overview of issues and recent developments in cloud computing and storage security. InHigh Performance Cloud Auditing and Applications. Jan 1 pp. 3–33. Springer New York.

Ahuja, S.P., Komathukattil, D., 2012. A survey of the state of cloud security. Netw. Commun. Technol. 1 (2), 66–75.

Aihkisalo, T., Paaso, T., 2012. Latencies of service invocation and processing of the REST and SOAP web service interfaces. InServices (SERVICES), 2012 IEEE Eighth World Congress on. Jun 24. IEEE. pp. 100–107.

AlFardan, N., Bernstein, D., Paterson, K., Poettering, B., Schuldt, J. 2005. On the Security of RC4 in TLS. ⟨http://www.isg.rhul.ac.uk/tls/index.html(2013)⟩. Accessed December.

Ali, M., Khan, S.U., Vasilakos, A.V., 2015. Security in cloud computing: opportunities and challenges. Inf. Sci. 305, 357–383.

Almorsy, M., Grundy, J., Müller, I., 2010. An analysis of the cloud computing security problem. In: Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov.

Amazon Web Services Discussion Forums: Low Entropy on EC2 Instances Problem for Anything Related to Security. 2015. ⟨https://forums.aws.amazon.com/thread.jspa?MessageID=249079(2011)⟩. Accessed November.

Amazon: Amazon Web Services: Overview of Security Processes, 2015. ⟨http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf(2011)⟩. White Paper. Accessed November.

Amazon: Amazon Elastic Compute Cloud (Amazon EC2), 2015. ⟨https://aws.amazon.com/ec2/(2012)⟩. Accessed November.

Amazon: Amazon Virtual Private Cloud (Amazon VPC), 2015. ⟨http://aws.amazon.com/vpc/(2012)⟩. Accessed November.

Amoroso, E.G., 2013. From the enterprise perimeter to a mobility-enabled secure cloud. IEEE Secur. Priv. 11 (1), 23–31.

Anala, M.R., Shetty, J., Shobha, G., 2013. A framework for secure live migration of virtual machines. InAdvances in Computing, Communications and Informatics (ICACCI). 2013 International Conference on, Aug 22. IEEE. pp. 243–248.

Armbrust, M., Fox, O., Griffith, R., Joseph, A.D., Katz, Y., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2009. Above the clouds: a Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28. Electrical Engineering and Computer Sciences University of California.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58, (Apr 1).

Aviram, A., Hu, S., Ford, B., Gummadi, R., 2010. Determinating timing channels in compute clouds. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop. Oct 8. ACM. pp. 103–108.

Azmandian, F., Moffie, M., Alshawabkeh, M., Dy, J., Aslam, J., Kaeli, D., 2011. Virtual machine monitor-based lightweight intrusion detection. ACM SIGOPS Oper. Syst. Rev. 45 (2), 38–53.

Backstrom, L., Dwork, C., Kleinberg, J., 2007. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of the 16th international conference on World Wide Web. May 8. ACM. pp. 181–190.

Bahram, S., Jiang, X., Wang, Z., Grace, M., Li, J., Srinivasan, D., Rhee, J., Xu, D., 2010. Dksm: Subverting virtual machine introspection for fun and profit. InReliable Distributed Systems. 2010 In: Proceedings of the 29th IEEE Symposium on. Oct 31. IEEE. pp. 82–91

Baier, D., Bertocci, V., Brown, K., Woloski, M., Pace, E.A., 2010. Guide to Claims-Based Identity and Access Control: patterns & Practices. Microsoft Press.

Basak, D., Toshniwal, R., Maskalik, S., Sequeira, A., 2010. Virtualizing networking and security in the cloud. ACM SIGOPS Oper. Syst. Rev. 44 (4), 86–94.

Becherer, A., Stamos, A., Wilcox, N., 2009. Cloud Computing Security: Raining on the Trendy new Parade. BlackHat, USA.

Begum, S., Khan, M.K., 2011. Potential of cloud computing architecture. InInformation and Communication Technologies (ICICT), 2011 International Conference on . Jul 23. IEEE. pp. 1–5.

Behl, A., 2011. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. InInformation and Communication Technologies (WICT), 2011 World Congress on. Dec 11. IEEE. pp. 217–222.

Bin Mat Nor, F., Jalil, K.A., Manan, J.L., 2012. An enhanced remote authentication scheme to mitigate man-in-the-browser attacks. InCyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. Jun 26. IEEE. pp. 271–276.

Boampong, P.A., Wahsheh, L.A., 2012. Different facets of security in the cloud. In: Proceedings of the 15th Communications and Networking Simulation Symposium. Mar 26. Society for Computer Simulation International. (p. 5).

Boldyreva, A., Chenette, N., O'Neill, A., 2011. Order-preserving encryption revisited: Improved security analysis and alternative solutions. InAdvances in Cryptology-

CRYPTO 2011. Jan 1. Springer Berlin Heidelberg. pp. 578–595.
Bormann, C., Castellani, A.P., Shelby, Z., 2012. Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Comput. 16 (2), 62.
Bugiel, S., Nürnberger, S., Pöppelmann, T., Sadeghi, A.R., Schneider, T., 2011. AmazonIA: when elasticity snaps back. In: Proceedings of the 18th ACM conference on Computer and communications security. Oct 17. ACM. pp. 389–400.
Carriço, P., 2015. Low entropy on VMs.⟨http://blog.pedrocarrico.net/post/17026199379/low-entropy-on-vms(2012)⟩. Accessed November.
Casale, A., 2013. The Dangers of Recycling in the Cloud. TheMakegood.
Chandrasekar, S., Zhang, N., Idicula, S., Agarwal, N., 2013. inventors; Oracle International Corporation, assignee. Fast extraction of scalar values from binary encoded XML. United States patent US 8,429,196. Apr 23.
Chen, X., Andersen, J., Mao, Z.M., Bailey, M., Nazario, J., 2008. Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware. InDependable Systems and Networks With FTCS and DCC, 2008. DSN 2008. IEEE International Conference on. Jun 24. IEEE. pp. 177–186.
Chen, Y., Paxson, V., Katz, RH., 2010. What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January. Jan 20;20(2010):2010-5.
Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J., 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on Cloud computing security. Nov 13. ACM. pp. 85–90.
Chow, S.M.S., He, Y., Hui, L.C.K., Yiu, S.M., 2012. Spicesimple privacy-preserving identity-management for cloud environment, In: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, pp. 526–543.
Chung, H., Park, J., Lee, S., Kang, C., 2012. Digital forensic investigation of cloud storage services. Digit. Investig. 9 (2), 81–95.
Cisco: Cisco Annual Security Report, 2015. ⟨http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html⟩ (2013). Accessed November.
Cisco: Cisco Data Center Infrastructure 2.5 Design Guide, 2015. ⟨http://www.cisco.com/univercd/cc/td/doc/solution/dcidg21.pdf⟩ (2007). Accessed November.
Dhungana, R.D., Mohammad, A., Sharma, A., Schoen, I., 2013. Identity management framework for cloud networking infrastructure, In: IEEE International Conference on Innovations in Information Technology (IIT), pp. 13–17.
Dinesha, H.A., Agrawal, V.K., 2012. Multi-level authentication technique for accessing cloud services. InComputing, Communication and Applications (ICCCA), 2012 International Conference on. Feb 22. IEEE. pp. 1–4.
Doel, K., 2013. Scary logins: Worst passwords of 2012 and how to fix them. Retrieved 1/21.
Doroodchi, M., Iranmehr, A., Pouriyeh, SA., 2009. An investigation on integrating XML-based security into Web services. InGCC Conference & Exhibition, 2009 5th IEEE. Mar 17. IEEE. pp. 1–5.
Dougan, T., Curran, K., 2012. Man in the browser attacks. Int. J. Ambient Comput. Intell. (IJACI) 4 (1), 29–39.
Duncan, A., Creese, S., Goldsmith, M., 2012. Insider attacks in cloud computing. InTrust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE Proceedings of the 11th International Conference on. Jun 25. IEEE. pp. 857–862.
Dykstra, J., Sherman, A.T., 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. Digit. Investig. 9, 90–98.
ENISA: Cloud Computing: Benefits, Risks and Recommendations for Information Security, 2015. ⟨http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computingrisk-assessment(2009)⟩. Accessed August.
Fan, K., Mao, D., Lu, Z., Wu, J., 2013. OPS: Offline Patching Scheme for the Images Management in a Secure Cloud Environment. InServices Computing (SCC), 2013 IEEE International Conference on. Jun 28. IEEE. pp. 587–594.
Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R., 2014. Security issues in cloud environments: a survey. Int. J. Inf. Secur. 13 (2), 113–170.
Ferris, J.M., 2014. inventor; Red Hat, Inc., assignee. Load balancing in cloud-based networks. United States patent US 8,849,971. Sep 30.
FireEye: FireEye Advanced Threat Report2H 2012, 2015. ⟨http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf(2013)⟩. Accessed October.
Fu, Y., Lin, Z., 2013. Exterior: using a dual-vm based external shell for guest-os introspection, configuration, and recovery. ACM SIGPLAN Not. 48 (7), 97–110.
Gennaro, R., Gentry, C., Parno, B., 2010. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. InAdvances in Cryptology-CRYPTO 2010. Jan 1. Springer Berlin Heidelberg. pp. 465–482.
Gharehchopogh, Farhad Soleimanian, Hashemi, Sajjad, 2012. Security challenges in cloud computing with more emphasis on trust and privacy. Int. J. Sci. Technol. Res. 1 (6), 2277–8616.
Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., Pourzandi, M., 2012. A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput. 1 (1), 1–8.
Goodrich, R., 2013. What Is Doxing?. TechNewsDaily.
Google: Google App Engine, 2015. https://developers.google.com/developers.google.com/appengine/(2013)⟩. Accessed August.
Grispos, G., Glisson, W.B., Storer, T., 2013. Using smartphones as a proxy for forensic evidence contained in cloud storage services. In: System Sciences (HICSS), 2013 Proceedings of the 46th Hawaii International Conference on. Jan 7. IEEE. pp. 4910–4919
Grobauer, B., Walloschek, T., Stöcker, E., 2011. Understanding cloud computing vulnerabilities. Ieee. Secur. Priv. 9 (2), 50–57.
Grosse, E., Upadhyay, M., 2013. Authentication at scale. Ieee. Secur. Priv. 11 (1), 15–22.
Habib, S.M., Ries, S., Mühlhäuser, M., 2011. Towards a trust management system for cloud computing. InTrust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE Proceedings of the 10th International Conference on. Nov 16. IEEE. pp. 933–939.
Habib, Sheikh Mahbub, Sebastian Ries, Max Muhlhauser, 2011. Towards a trust management system for cloud computing. In: 2011 IEEE Proceedings of the 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 933–939. IEEE, 2011.
Hale, M.L., Gamble, R., 2012. Secagreement: advancing security risk calculations in cloud services, In: IEEE Eighth World Congress on Services (SERVICES), 2012, pp. 133–140.
Hart, J., 2009. Remote working: managing the balancing act between network access and data security. Comput. Fraud Secur. 2009 (11), 14–17.
Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B., 2013. An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4 (1), 1–3.
He, X., Chomsiri, T., Nanda, P., Tan, Z., 2014. Improving cloud network security using the Tree-Rule firewall. Future Gener. Comput. Syst. 30, 116–126.
Helland, P., 2013. Condos and clouds. Commun. ACM 56 (1), 50–59.
Heninger, N., Durumeric, Z., Wustrow, E., Halderman, J.A., 2012. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. InUSENIX Security Symposium. Aug 8 pp. 205–220.
HP: HP 2012 Cyber Risk Report. 2015. http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0213.pdf(2013)⟩. Accessed September.
Hubbard, D., Sutton, M., 2010. Top threats to cloud computing v1.0. Cloud Security Alliance.
Hunt, T., 2015. 5 Ways to Implement HTTPS in an Insufficient Manner (and leak sensitive data). ⟨http://www.troyhunt.com/2013/04/5-ways-to-implement-https-in.html(2013)⟩. Accessed September.
Ibrahim, A.S., Hamlyn-Harris, J., Grundy, J., Almorsy, M., 2011. CloudSec: a security monitoring appliance for Virtual Machines in the IaaS cloud model. In: Network and System Security (NSS), 2011 Proceedings of the 5th International Conference on. Sep 6. IEEE. pp. 113–120
Idziorek, J., Tannian, M., 2011. Exploiting cloud utility models for profit and ruin. InCloud Computing (CLOUD), 2011 IEEE International Conference on. Jul 4. IEEE. pp. 33–40.
Idziorek, J., Tannian, M., Jacobson, D., 2011. Detecting fraudulent use of cloud resources. In: Proceedings of the 3rd ACM workshop on Cloud computing security workshop. Oct 21. ACM. pp. 61–72.
Jaber, A.N., Zolkipli, B., Fadli, M., 2013. Use of cryptography in cloud computing. InControl System, Computing and Engineering (ICCSCE), 2013 IEEE International Conference on Nov 29. IEEE. pp. 179–184
Jasti, A., Shah, P., Nagaraj, R., Pendse, R., 2010. Security in multi-tenancy cloud. InSecurity Technology (ICCST), 2010 IEEE International Carnahan Conference on. Oct 5. IEEE. pp. 35–41
Jensen, M., Meyer, C., 2011. Expressiveness considerations of XML signatures. InComputer Software and Applications Conference Workshops (COMPSACW), 2011 IEEE 35th Annual. Jul 18. IEEE. pp. 392–397.
Jensen, M., Schwenk J. The accountability problem of flooding attacks in service-oriented architectures. InAvailability, Reliability and Security, 2009. ARES'09. International Conference on 2009 Mar 16 pp. 25–32. IEEE.
Jensen, M., Gruschka, N., Luttenberger, N., 2008. The impact of flooding attacks on network-based services. InAvailability, Reliability and Security, 2008. ARES 08. In: Proceedings of the Third International Conference on. Mar 4. IEEE. pp. 509–513.
Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L., 2009. On technical security issues in cloud computing. InCloud Computing, 2009. CLOUD'09. IEEE International Conference on. Sep 21. IEEE. pp. 109–116
Jensen, M., Gruschka, N., Herkenhöner, R., 2009. A survey of attacks on web services. Comput. Sci. Res. Dev. 24 (4), 185–197.
Kandukuri, B.R., Paturi, V.R., Rakshit, A., 2009. Cloud security issues. InServices Computing, 2009. SCC'09. IEEE International Conference on, Sep 21. IEEE. pp. 517–520.
Kant, K., 2009. Data center evolution: a tutorial on state of the art, issues, and challenges. Comput. Netw. 53 (17), 2939–2965.
Katsuki, T., 2012. Crisis for windows sneaks onto virtual machines. Symantec Blog.
Kaufman, L.M., 2009. Data security in the world of cloud computing. Ieee. Secur. Priv. 7 (4), 61–64.
Kazim, M., Masood, R., Shibli, MA., 2013. Securing the virtual machine images in cloud computing. In: Proceedings of the 6th International Conference on Security of Information and Networks. Nov 26. ACM. pp. 425–428.
Kerrigan, B., Chen, Y., 2012. A study of entropy sources in cloud computers: random number generation on cloud hosts. Springer Berlin Heidelberg; Jan 1.
Khan, K.M., Malluhi, Q., 2010. Establishing trust in cloud computing. IT Prof. 12 (5), 20–27.
King, S.T., Chen, P.M., 2006. SubVirt: Implementing malware with virtual machines. InSecurity and Privacy, 2006 IEEE Symposium on. May 21. IEEE.
Kufel, L., 2013. Security event monitoring in a distributed systems environment. IEEE Secur. Priv. 11 (1), 36–43.
Kulkarni, G., Waghmare, R., Palwe, R., Waykule. V., Bankar. H., Koli, K., 2012. Cloud storage architecture. In: Telecommunication Systems, Services, and Applications (TSSA), 2012 Proceedings of the 7th International Conference on. Oct 30. IEEE. pp. 76–81.
Leopando, J., 2013. World backup day: the 3-2-1 rule. Trend Micro Trend..
Li, Q., Clark, G., 2013. Mobile security: a look ahead. Ieee. Secur. Priv. 11 (1), 78–81.
Li, C., Raghunathan, A., Jha, N.K., 2012. A trusted virtual machine in an untrusted management environment. IEEE Trans. Serv. Comput. 5 (4), 472–483.
Li, S., Sadeghi, A.R., Heisrath, S., Schmitz, R., Ahmad, J.J., 2012. hPIN/hTAN: A lightweight and low-cost e-banking solution against untrusted computers.

InFinancial Cryptography and Data Security. Jan 1. Springer Berlin Heidelberg. pp. 235–249.
Lineberry, S., 2007. The human element: the weakest link in information security. J. Account. 204 (5), 44.
Liu, Q., Wang, G., Wu, J., 2014. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Inform. Sci. 258, 355–370.
Liu, H., 2010. A new form of DOS attack in a cloud and its avoidance mechanism. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop.Oct 8 pp. 65–76. ACM.
Lombardi, F., Di Pietro, R., 2011. Secure virtualization for cloud computing. J. Netw. Comput. Appl. 34 (4), 1113–1122.
Luo, S., Lin, Z., Chen, X., Yang, Z., Chen, J., 2011. Virtualization security for cloud computing service. InCloud and Service Computing (CSC), 2011 International Conference on. Dec 12. IEEE. pp. 174–179.
Mandiant: APT1: Exposing One of China's Cyber Espionage Units. 2015. ⟨http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf(2013)⟩. Accessed September.
Manuel, Paul, 2015. A trust model of cloud computing based on quality of service. Ann. Oper. Res. 233 (1), 281–292.
Marlinspike, M., 2015. New tricks for defeating SSL in practice. ⟨https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf⟩ (2009). Accessed September.
Martin, D., 2013. Implementing effective controls in a mobile, agile, cloud-enabled enterprise. IEEE Secur. Priv. 1 (1), 13–24.
McIntosh, M, Austel, P., 2005. XML signature element wrapping attacks and countermeasures. In: Proceedings of the 2005 workshop on Secure web services, Nov 11. ACM. pp. 20–27.
Microsoft: Microsoft Security Intelligence Report: Volume 14. 2015 http://www.microsoft.com/security/sir/default.aspx⟩ (2013). Accessed September.
Modi, C., Patel, D., Borisaniya, B., Patel, A., Rajarajan, M., 2013a. A survey on security issues and solutions at different layers of Cloud computing. J. Supercomput. 63 (2), 561–592.
Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M., 2013b. A survey of intrusion detection techniques in cloud. J. Netw. Comput. Appl. 36 (1), 42–57.
Mohammed, N., Fung, B., Hung, P.C., Lee, C.K., 2009. Anonymizing healthcare data: a case study on the blood transfusion service. In: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. Jun 28. ACM. pp. 1285–1294.
Mon, E.E., Naing, T.T., 2011. The privacy-aware access control system using attribute- and role-based access control in private cloud. In: Broadband Network and Multimedia Technology (IC-BNMT), 2011 Proceedings of the 4th IEEE International Conference on. Oct 28. IEEE. pp. 447–451.
Monfared, A.T., Jaatun, M.G., 2011. Monitoring intrusions and security breaches in highly distributed cloud environments. In: 2011 Proceedings of the Third IEEE International Conference on Coud Computing Technology and Science. Nov 29. IEEE. pp. 772–777.
Narayanan, A., Shmatikov, V. 2009. De-anonymizing social networks. In: Security and Privacy, 2009 Proceedings of the 30th IEEE Symposium on. May 17. IEEE. pp. 173–187.
NIST: The NIST Definition of Cloud Computing. ⟨http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf⟩(2011). Accessed September.
O'Neill, M., 2013. Cloud APIsthe next battleground for denial-of-service attacks. CSA Blog.
Okamura, K., Oyama, Y., 2010. Load-based covert channels between Xen virtual machines. In: Proceedings of the 2010 ACM Symposium on Applied Computing. Mar 22. ACM. pp. 173–180.
Oktay, U., Sahingoz, O.K., 2013. Attack types and intrusion detection systems in cloud computing. In: Proceedings of the 6th International Information Security & Cryptology Conference. Sep pp. 71–76.
OSVDB: The Open Source Vulnerability Database Website, 2015. ⟨http://www.osvdb.org/(2013)⟩. Accessed October.
OWASP: The Then Most Critical Web Application Security Risks, 2015. ⟨http://owasptop10.googlecode.com/files/OWASP(2010)⟩. Accessed July.
OWASP: The Then Most Critical Web Application Security Risks, 2015. ⟨https://www.owasp.org/index.php/Top_10_2013⟩(2013). Accessed July.
Oyama, Y., Giang, T.T., Chubachi, Y., Shinagawa. T., Kato, K., 2012. Detecting malware signatures in a thin hypervisor. In: Proceedings of the 27th Annual ACM Symposium on Applied Computing. Mar 26. ACM. pp. 1807–1814.
Pan, W., Zhang, Y., Yu, M., Jing, J., 2012. Improving virtualization security by splitting hypervisor into smaller components. InIFIP Annual Conference on Data and Applications Security and Privacy. Jul 11. Springer Berlin Heidelberg. pp. 298–313.
Panah, A., Panah, A., Panah, O., Fallahpour, S., 2012. Challenges of security issues in cloud computing layers. Rep. Opin. 4 (10), 25–29.
Patel, P., 2015. Solution: FUTEX_WAIT hangs Java on Linux/Ubuntu in vmware or virtual box. ⟨http://www.springone2gx.com/blog/pratik_patel/2010/01/solution_futex_wait_hangs_java_on_linux_ubuntu_in_vmware_or_virtual_box(2010)⟩. Accessed September.
Pearce, M., Zeadally, S., Hunt, R., 2013. Virtualization: issues, security threats, and solutions. ACM Comput. Surv. (CSUR) 45 (2), 17.
Pearson, S., 2013. Privacy, security and trust in cloud computing. InPrivacy and Security for Cloud Computing. Jan 1. Springer London. pp. 3–42.
Perez-Botero, D., Szefer, J., Lee, R.B., 2013. Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 international workshop on Security in cloud computing. May 8. ACM. pp. 3–10.
Pfaff, B., Pettit, J., Amidon, K., Casado, M., Koponen, T., Shenker, S., 2009. Extending networking into the virtualization layer. InHotnets.
Prandini, M., Ramilli, M., Cerroni, W., Callegati, F., 2010. Splitting the HTTPS stream to attack secure web connections. IEEE Secur. Priv. 1 (6), 80–84.
Prince, M., 2013. The ddos that knocked spamhaus offline (and how we mitigated it). Cloudflare Blog 20 (March), 3.
Prolexic: Prolexic Quarterly Global DDoS Attack Report Q1 2013, 2015.⟨https://www.prolexic.com/knowledge-center-ddos-attackreport-2013-q1.html(2013)⟩. Accessed September.
Rauti, S., Leppänen, V., 2012. Browser extension-based man-in-the-browser attacks against Ajax applications with countermeasures. In: Proceedings of the 13th International Conference on Computer Systems and Technologies. Jun 22. ACM. pp. 251–258.
Reardon, J., Basin, D., Capkun, S., 2013. Sok: Secure data deletion. InSecurity and Privacy (SP), 2013 IEEE Symposium on May 19. IEEE. pp. 301–315
Rimal, B.P., Jukan, A., Katsaros, D., Goeleven, Y., 2011. Architectural requirements for cloud computing systems: an enterprise cloud approach. J. Grid Comput. 9 (1), 3–26.
Ristenpart, T., Tromer, E., Shacham, H., Savage, S., 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security. Nov 9. ACM. pp. 199–212
Roberts II, J.C., Al-Hamdani, W., 2011. Who can you trust in the cloud?: a review of security issues within cloud computing. In: Proceedings of the 2011 Information Security Curriculum Development Conference. Sep 30. ACM. pp. 15–19.
Rocha, F., Correia, M., 2011. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In: Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP Proceedings of the 41st International Conference on. Jun 27. IEEE. pp. 129–134.
Rodero-Merino, L., Vaquero, L.M., Caron, E., Muresan, A., Desprez, F., 2012. Building safe PaaS clouds: a survey on security in multitenant software platforms. Comput. Secur. 31 (1), 96–108.
Rong, C., Nguyen, S.T., Jaatun, M.G., 2013. Beyond lightning: a survey on security challenges in cloud computing. Comput. Electr. Eng. 39 (1), 47–54.
Sanka, Sunil, Chittaranjan, Hota, Muttukrishnan, Rajarajan, 2010. Secure data access in cloud computing. In: Internet Multimedia Services Architecture and Application (IMSAA), 2010 IEEE Proceedings of the 4th International Conference on, pp. 1–6. IEEE.
Santos, N., Gummadi, K.P., Rodrigues, R., 2009. Towards trusted cloud computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing. Jun 15 pp. 1–5.
Saravanaguru, R.A., Abraham, G., Ventakasubramanian, K., Borasia, K., 2013. Securing Web Services Using XML Signature and XML Encryption. arXiv preprint arXiv:1303.0910. Mar 5.
Sedayao, Jeff., 2012. Enhancing cloud security using data anonymization. White Paper, Intel Coporation.
Sekar, V., Maniatis, P., 2011. Verifiable resource accounting for cloud computing services. In: Proceedings of the 3rd ACM workshop on Cloud computing security workshop. Oct 21. ACM. pp. 21–26.
Sengupta, S., Kaulgud, V., Sharma, V.S., 2011. Cloud computing security–trends and research directions. InServices (SERVICES), 2011 IEEE World Congress on. Jul 4. IEEE. pp. 524–531
Shin, S., Gu, G., 2012. CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?). In: Network Protocols (ICNP), 2012 Proceedings of the 20th IEEE International Conference on. Oct 30. IEEE. pp. 1–6.
Shinotsuka, H., 2012. Malware authors using new techniques to evade automated threat analysis systems. Symantec Blog (October).
Singh, A., Chatterjee, K., 2015. Identity Management in Cloud Computing through Claim-Based Solution. In: Advanced Computing & Communication Technologies (ACCT), 2015 Proceedings of the Fifth International Conference on. Feb 21. IEEE. pp. 524–529
Somorovsky, J., Mayer, A., Schwenk, J., Kampmann, M., Jensen, M., On Breaking SAML: Be Whoever You Want to Be. InUSENIX Security Symposium. Aug 8 pp. 397–412.
Sood, A.K., Enbody, R.J., 2013. Targeted cyberattacks: a superset of advanced persistent threats. IEEE Secur. Priv. 1 (1), 54–61.
Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. J. Netw. Comput. Appl. 35 (6), 1831–1838.
Stanoevska-Slabeva, K., Wozniak, T., Ristol, S., editors. Grid and cloud computing: a business perspective on technology and applications. Springer Science & Business Media. Nov 4.
Staten, J., 2012. Cloud predictions: we'll finally get real about cloud. Forrester Blog.
Subashini, S., Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 34 (1), 1–11.
Suzaki, K., Iijima, K., Yagi, T., Artho, C., 2011. Software side channel attack on memory deduplication. SOSP POSTER.
Syam Kumar, P., Subramanian, R., 2011. An efficient and secure protocol for ensuring data storage security in Cloud Computing. IJCSI Int. J. Comput. Sci. Issues 8 (6), 8.
Symantec Security Response: Internet Explorer Zero-Day Used in Watering Hole Attack: Q & A. Symantec Blog, 2012.
Symantec: Internet Security Threat Report, 2015. ⟨https://www.symantec.com/security_response/publications/threatreport.jsp⟩(2013). Accessed September.
Szefer, J., Keller, E., Lee, R.B., Rexford, J., 2011. Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM conference on Computer and communications security. Oct 17. ACM. pp. 401–412
Takabi, H., Joshi, J.B., Ahn, G.-J., 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. 6, 24–31.
Tang, Y., Lee, P.P., Lui, J., Perlman, R., 2012. Secure overlay cloud storage with access

control and assured deletion. IEEE Trans. Dependable Secur. Comput. 9 (6), 903–916.
Tang, M., Lv, Q., Lu, Z., Zhao, Q., Song, Y., 2012. Dynamic virtual switch protocol using Openflow. In: Software Engineering, Artificial Intelligence, Networking and Parallel & Distributed Computing (SNPD), 2012 Proceedings of the 13th ACIS International Conference on. Aug 8. IEEE. pp. 603–608
Tang, B., Sandhu, R., Li, Q., 2013. Multi-tenancy authorization models for collaborative cloud services. In: Proceedings of the 14th International Conference on Collaboration Technologies and Systems (CTS), IEEE, San Diego, California, USA. pp. 132–138
Tari, Z., Yi, X., Premarathne, U.S., Bertok, P., Khalil, I., 2015. Security and privacy in cloud computing: vision, trends, and challenges. IEEE Cloud Comput. 2 (2), 30–38.
Tavakoli, Z., Meier, S., Vensmer, A., 2012. A framework for security context migration in a firewall secured virtual machine environment. InInformation and Communication Technologies. Jan 1. Springer Berlin Heidelberg. pp. 41–51.
Taylor, G., Cox, G., 2011. Digital randomness. Ieee. Spectr. 48 (9), 32–58.
Taylor, M., Haggerty, J., Gresty, D., Lamb, D., 2011. Forensic investigation of cloud computing systems. Netw. Secur. 2011 (3), 4–10.
Thorsheim, P., 2015. The Final Word on the LinkedIn Leak. ⟨http://securitynirvana.blogspot.pt/2012/06/final-word-on-linkedinleak.html(2012)⟩.(accessed September 2015).
Townsend, M., 2009. Managing a security program in a cloud computing environment. In2009 Information Security Curriculum Development Conference. Sep 25. ACM. pp. 128–133
Tripathi, A., Mishra, A., 2011. Cloud computing security considerations. InSignal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on. Sep 14 pp. 1–5. IEEE.
Tsai, H.Y., Siebenhaar, M., Miede, A., Huang, Y.L., Steinmetz, R., 2011. Threat as a service?: virtualization's impact on cloud security. IT Prof. 14 (1), 32–37.
Vaquero, L.M., Rodero-Merino, L., Morán, D., 2011. Locking the sky: a survey on IaaS cloud security. Computing 91 (1), 93–118.
Wan, Z., Liu, J.E., Deng, R.H., 2012. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans. Inf. Forensics Secur. 7 (2), 743–754.
Wan, X., Zhang, X., Chen, L., Zhu, J., 2012. An improved vTPM migration protocol based trusted channel. InSystems and Informatics (ICSAI), 2012 International Conference on. May 19. IEEE. pp. 870–875.
Wang, G., Ng, T.E., 2010. The impact of virtualization on network performance of amazon ec2 data center. InINFOCOM, 2010 Proceedings IEEE. Mar 14. IEEE. pp. 1–9
Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W., 2012. Toward secure and dependable storage services in cloud computing. Serv. Comput., Trans. IEEE 5 (2), 220–232.
Wang, Z., Wu, C., Grace, M., Jiang, X., 2012. Isolating commodity hosted hypervisors with hyperlock. In: Proceedings of the 7th ACM european conference on Computer Systems. Apr 10 pp. 127–140. ACM.
Wang, Boyang, Baochun, Li, Hui, Li, 2012. Oruta: Privacy-preserving public auditing for shared data in the cloud. In: Cloud Computing (CLOUD), 2012 IEEE Proceedings of the 5th International Conference on, IEEE, pp. 295–302.
Wang, R., Chen, S., Wang, X., 2012. Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. InSecurity and Privacy (SP), 2012 IEEE Symposium on. May 20. IEEE. pp. 365–379.
Wang, J., Stavron, A., Ghosh, A., 2013. Autonomic Recovery: HyperCheck: A Hardware-Assisted Integrity Monitor. GEORGE MASON UNIV FAIRFAX VA CENTER FOR SECURE INFORMATION SYSTEMS; Aug.
Websense: 2013 Threat Report, 2015. https://www.websense.com/content/websense-2013-threat-report.aspx⟩ (2013). Accessed September.
Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P., 2009. Managing security of virtual machine images in a cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud computing security. Nov 13. ACM. pp. 91–96.
Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., Vasilakos, A.V., 2014. Security and privacy for storage and computation in cloud computing. Inf. Sci. 258, 371–386.
Wu, H., Ding, Y., Winer, C., Yao, L., 2010. Network security for virtual machine in cloud computing. In: Computer Sciences and Convergence Information Technology (ICCIT), 2010 Proceedings of the 5th International Conference on. Nov 30. IEEE. pp. 18–21.
Wu, C., Wang, Z., Jiang, X., 2013. Taming hosted hypervisors with (mostly) deprivileged execution. InNDSS (February).
Xia, Y., Liu, Y., Chen, H., 2013. Architecture support for guest-transparent vm protection from untrusted hypervisor and physical attacks. In: High Performance Computer Architecture (HPCA2013), 2013 IEEE Proceedings of the 19th International Symposium on. Feb 23. IEEE. pp. 246–257.
Xiao, Z., Xiao, Y., 2013. Security and privacy in cloud computing. Ieee. Commun. Surv. Tutor. 15 (2), 843–859.
Xing, T., Huang, D., Xu, L., Chung, C.J., Khatkar, P., 2013. Snortflow: A openflow-based intrusion prevention system in cloud environment. InResearch and Educational Experiment Workshop (GREE), 2013 Second GENI. Mar 20. IEEE. pp. 89–92.
Xu, Y., Bailey, M., Jahanian, F., Joshi, K., Hiltunen, M., Schlichting, R., 2011. An exploration of L2 cache covert channels in virtualized environments. In: Proceedings of the 3rd ACM workshop on Cloud computing security workshop. Oct 21. ACM. pp. 29–40.
Xu, Jun, Feng, Xu, Wenna, Chang, Haiguang, Lai. 2015. Research and Development of Trust Mechanism in Cloud Computing. In: International Conference on Cloud Computing and Security, Springer International Publishing, 2015. pp. 218–229
Yarom, Y., Benger, N., 2014. Recovering OpenSSL ecdsa nonces using the flush+ reload cache side-channel attack. IACR Cryptol. EPrint Arch. 2014, 140.
Yazji, S., Scheuermann, P., Dick, R.P., Trajcevski, G., Jin, R., 2014. Efficient location aware intrusion detection to protect mobile devices. Pers. Ubiquitous Comput. 18 (1), 143–162.
Yilek, S., 2010. Resettable public-key encryption: How to encrypt on a virtual machine. InTopics in Cryptology-CT-RSA. Jan 1. Springer Berlin Heidelberg. pp. 41–56.
Yu, H., Powell, N., Stembridge, D., Yuan, X., 2012. Cloud computing and security challenges. In: Proceedings of the 50th Annual Southeast Regional Conference. Mar 29. ACM. pp. 298–302.
Zhang, F., Chen, J., Chen, H., Zang, B., 2011. CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In: Twenty-Proceedings of the Third ACM Symposium on Operating Systems Principles. Oct 23. ACM. pp. 203–216.
Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T., 2012. Cross-VM side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security. Oct 16. ACM. pp. 305–316.
Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, A., 2010. Security and privacy in cloud computing: A survey. In: Semantics Knowledge and Grid (SKG), 2010 Proceedings of the Sixth International Conference on. Nov 1 pp. 105–112. IEEE.
Zissis, D., Lekkas, D., 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst. 28 (3), 583–592.
Zou, B., Zhang, H., 2011. Toward enhancing trust in cloud computing enviroment. In: 2011 Proceedings of the 2nd International Conference on Control, Instrumentation and Automation (ICCIA) pp. 364–366.