Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks

Wajid Hassan[1], Te-Shun Chou[2], Xiaoming Li[3], Patrick Appiah-Kubi[4], Tamer Omar[5]
[1]Indiana State University, United States
[2]East Carolina University, United States
[3,4]University of Maryland University College, United States
[5]California State Polytechnic University, United States

Article Info

Article history:

Received Oct 02, 2019
Revised Nov 13, 2019
Accepted Nov 23, 2019

Keywords:

Cloud computing
Cloud security attacks
Cloud security issues
Cloud security standard
Machine learning
Software defined networking
Virtualization
Virtualized data center security

ABSTRACT

The emergence of cloud computing has changed perception of all regarding software delivery, development models and infrastructure. Cloud computing has a potential of providing elastic, easily manageable, powerful and cost-effective solutions. The rapid transition to cloud computing has fueled concerns on the security issues. The migration of the user's data and applications in a shared environment of a cloud, where there is a collocation of several users increases security related concerns. Several research efforts have been made in evaluating challenges related to security faced by the cloud computing environments, a number of solutions of such problems have also been proposed. Integrated security solutions should be devised to deal with the increasing security risks. In this paper, a detailed cloud computing survey, key services and concepts are being presented. This paper attempts to evaluate various security threats to cloud computing and a number of security solutions have also been discussed. Furthermore, a brief view of the cloud security regulatory bodies and compliance have also been presented. Despite the research efforts in cloud security field, there are still some open research problems and challenges which are discussed in this paper.

Corresponding Author:

Wajid Hassan,
Indiana State University,
200 N 7th St, Terre Haute, IN 47809, United States.
Email: wajidhassan@yahoo.com

1. INTRODUCTION

Although cloud computing environment ensures cost effective solutions and relieves the users from management of infrastructure, it also encounters privacy and security issues [1]. Security is a major issue that hinders the cloud computing growth, data protection and data privacy issues continue to plague the market [2] [3]. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model [4]. In this section we will describe the security risks faced by the cloud computing environment. According to "Cloud Security Alliance" (CSA), the top seven security risks are [5] [6]:

a. Nefarious & Abusive Use of Cloud Computing
b. Insecure Interfaces of Application Programming
c. Malicious Insiders
d. Vulnerabilities due to Shared Technology
e. Data Leakage/Loss
f. Service, Account & Traffic Hijacking
g. Unknown Risk Profile

In recent years IAAS cloud hosting providers have taken a bigger role in the deployment of services. Some well-known Cloud Service Providers are GoGrid Cloud Hosting, Amazon Web Services (AWS), HP

Public Cloud, Microsoft Azure, AT&T's Synaptic cloud storage, Rackspace, SoftLayer's CloudLayer and IBM's SmartCloud. All of these are susceptible to security attacks [7] in-spite of their claim to be built around iron clad security [11].

One of the motivations for this paper are the continuous security attacks, which seem to become bigger and affecting more and more users. In recent years several significant attacks have happened on Cloud through its characteristic of storage, Internet and applications. On July 29, 2017 Equifax had a data breach, which affected 143 million users. The data breach turned out to be 45% of the U.S Population. On November 2, 2017, Uber announced that it had went through a data breach the previous year, hackers had accessed their servers and copied all the data. Having info about payments, they asked for about $100,000 ransom money. The attack affected 57 million Uber drivers and customers. The attackers attacked on their repositories. On May 2017, the WannaCry attack affected 300,000 computers in four days. This attack caused 19,000 appointments of National Health services of the UK to be cancelled, including some surgeries. The vulnerability was discovered by Microsoft on March 14, 2017.

Even Yahoo was not safe from breaches, 2017 was the worst year for yahoo, the cloud-based attack affected 3 billion accounts of users. Due to Cloud Application attack [8] the personal voting information of 200 Million US persons was leaked in June 12, 2017. In late 2016, a hacker with the pseudonym Rasputin hacked several systems of colleges and universities; he is reported to use SQL injection attacks. In June 2017 [9] another cloud application-based attack became the reason 14 million users had their critical information leaked including phone numbers, ID and pins. Last but not the least another attack based on the Cloud characteristic of Internet [10], Infrastructure and Application Point of Sale malware infected 1200 properties of InterContinental Hotels UK in September 2016. Cloud Computing uses internet to deliver internet services, hence cloud inherits the vulnerabilities of internet and the vulnerabilities of computer networks as well as virtualization weaknesses. An IaaS model which is unsecured is vulnerable to MITM, DDOS, Port Scanning, and IP spoofing at minimum for network related security threats.

This survey paper is organized as follows. Section 4 describes the related surveys completed for cloud computing work. Section 5 discusses the cloud computing architectural frame works, Section 6 describes characteristics of Cloud Computing, Section 7 discusses enablers For Cloud Computing, Section 8 discusses various deployment models for cloud, Section 9 discusses cloud computing service models, Section 10 analyses various types of security attacks faced by cloud, Section 11 discusses Cloud Computing Security Framework, Section 12 discusses solutions to cloud computing security threats, Section 13 discusses cloud security regulatory bodies and compliance, Section 14 discusses open research problems and solutions to resolve cloud computing security threats with special focus on Software Defined Network and Machine Learning, Section 15 outlines areas for future work in cloud computing and Section 16 finally concludes the survey paper.

2. RELATED WORK DONE IN THE FIELD OF CLOUD SECURITY

Cloud Security Attacks, Assessment and Solutions are an active area of study for Cloud Computing. Several Survey papers on Cloud Computing have been written to compile the latest issues and solutions to those problems. We list only a few survey papers that we have studied related to security for the purpose of comparison and enhancement to the study on the cloud security threats and solutions.

Table 1. Cloud computing security survey

Paper Title	Authors	Summary of the Paper	Area discussed	Year Published
Cloud Attack and Risk Assessment Taxonomy [11]	(Juliadotter and Choo, 2015)	The authors have provided a comprehensive study on taxonomies, and present different security attacks against cloud computing services.	Attack taxonomy classifiers	2016
Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing [12]	Shameli-Sendi et al., 2015	This research paper studies DDoS attack against Cloud Computing as well as the strategies of mitigation.	DDoS mitigation	2015
A survey of security issues for cloud computing [13]	Minhaj Ahmad Khan, 2016	This research focuses on security risks faced to Cloud Computing environment.	DOS Attacks, Intrusion Detection	2016
Cloud security issues and challenges: A survey [14]	(Ashish Singh and Kakali Chatterjee, 2017)	This paper describes the basic features of the cloud computing, threats, issues related to security and their solutions.	Security Challenges	2017
On cloud security attacks: A taxonomy and intrusion detection and prevention as a service [15]	Salman et al., 2016	In this research paper, Cloud based vulnerabilities and attacks are classified and collected with respect to the models of cloud computing. It also discusses Taxonomy of attacks and their mitigation.	Taxonomy of cloud computing and Security Attacks	2016

Table 1. Cloud computing security survey (Continued)

Paper Title	Authors	Summary of the Paper	Area discussed	Year Published
Security in cloud computing: Opportunities and challenges [16]	Mazhar et al, 2015	The research discusses the security issues that are faced to cloud computing and solutions to counter the security threats and vulnerabilities in the cloud computing environment.	Multi-tenancy, Web Services	2015
An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review [17]	Patel et al., 2013	The survey paper presents a conceptual IDP (Intrusion detection and prevention) architecture for Cloud Computing.	Autonomic computing, ontology, risk management, and fuzzy theory	2013
Cloud Security Challenges: Investigating Policies, Standards and Guidelines in a Fortune 500 Organization [18]	Grispos et al., 2013	The paper describes the case study of Global Fortune 500 organizations and identifies the documentation issues of real-world information security.	Auditing policies, Guidelines and standards Applicable	2013
A Survey on Security Issues & Solutions at Different Layers of Cloud Computing [19]	Modi et al., 2013	The survey paper describes Cloud Computing security issues.	Virtualization, Privacy, Security and Vulnerabilities	2013
Surveying and analyzing security, privacy and trust issues in cloud computing environments [20]	Sun et al., 2011	The authors have surveyed Cloud Computing privacy, security and trust issues.	Presents the solution to analyze and eliminate Potential security, privacy and trust threats.	2011
A Survey on Security Issues in Service Delivery Models of Cloud Computing. [21]	Subashini and Kavitha 2011	The paper classifies Cloud Computing security issues, focusing on SaaS (Software as a Service).	SaaS	2011

3. CLOUD COMPUTING ARCHITECTURAL FRAMEWORK

NIST has developed a Cloud Computing Architectural Framework that essentially explains the several dimension of the ecosystem of cloud computing. The various major components of cloud computing [22] architectural framework [23] are Cloud Consumer, Cloud Broker, Cloud Provider, Cloud Carrier and Cloud Auditor. The Figure 1 shows the different components of the Cloud Computing Architectural Framework.

The discussion of each component of the architectural framework is out of scope of this paper however it has been discussed in detail in the following paper [24].

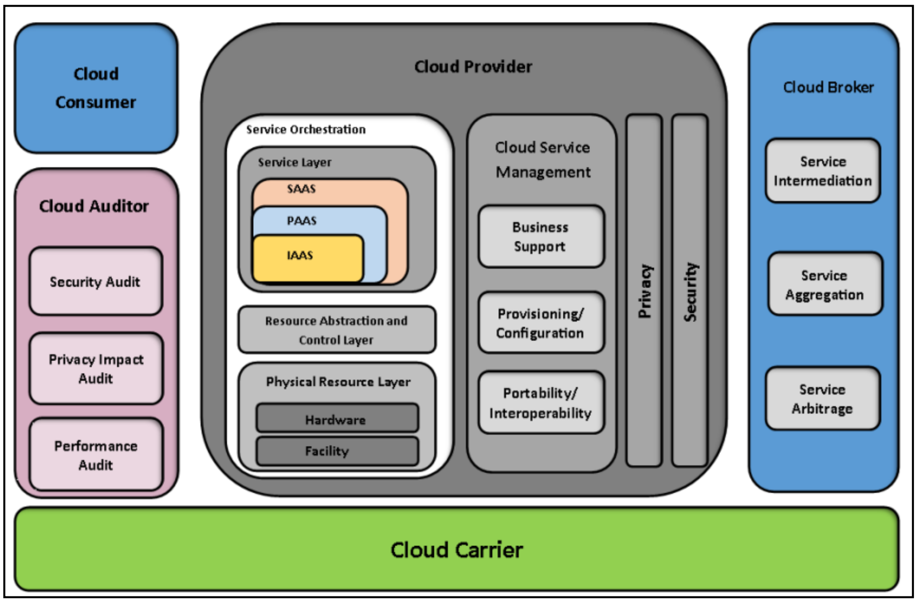

Figure 1. NIST cloud computing reference architecture [25]

4. CHARACTERISTICS OF THE CLOUD

Cloud has several characteristics which make it adaptable and preferable to be used. The defining characteristics of cloud developed by NIST [25] [26] [27] are outlined below:

- On demand self service
  The resources of cloud computing can be provided without the interaction of user with the service provider. The additional computing services can be provided [28] by the manufacturing organization without going through the cloud service provider.
- Broad network access
  Diverse customer platforms can access the cloud computing [29] resources which are available over the internet. Network bandwidth and broad network access are important aspects of cloud computing.
- Resource pooling
  Resource pooling means that same physical resources provide services to multiple customers. The resource pool of providers should be flexible and large enough to service multiple requirements of client.
- Rapid elasticity
  Elasticity is cloud computing's landmark and it implies that any cloud computing resource can be rapidly provisioned and de-provisioned by manufacturing organizations. Cloud computing resources can be scaled up or down rapidly in response to business demands.
- Measured service
  The cloud computing resource usage is metered and the organizations only pay accordingly to what services they use.
- Multi tenancy
  Multi-tenancy is the process in which multiple customers share one same physical infrastructure or the same applications while retaining security and privacy [30] [31] over their own information.

5. ENABLERS OF CLOUD COMPUTING

The key and major technologies that contribute to effective cloud computing are multi-tenant technology, virtualization, web services and less expensive hardware. These technology enablers have made fast growth of cloud computing possible. The main Enablers of Cloud Computing are depicted in Figure 2.

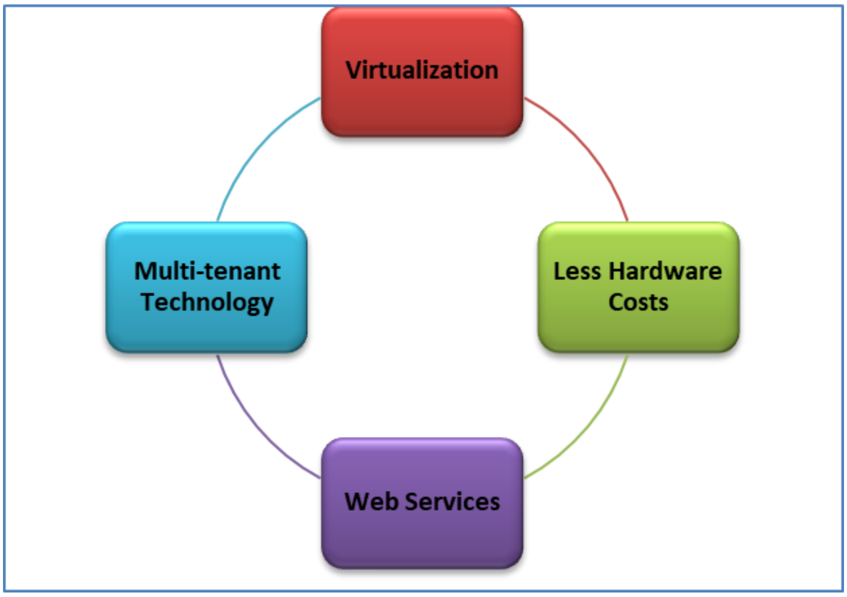

Figure 2. Enablers of cloud computing

- Multi-tenant technology
  Multi-tenancy is a methodology which allows several clients i.e. Virtual Machines (VMs) to share the same resource concurrently without interrupting the data of others. Each client accessing the service is considered as tenant. Multi-tenancy is cost effective as the costs associated with maintenance and software development are shared.

- Virtualization
  Virtualization [32] is the process in which physical system-defined resources are translated into virtual resources. Resources could be anything like power, servers or network. The main advantage linked to virtualization is the flexibility to create multiple VMs between distinct servers.
- Web services
  Web services refer to a software system that allows the communication between two systems connected to a network. All browser and web-based applications are implemented in premises of web Technology e.g. World Wide Web. WWW provides connectivity of IT resources. Its two core majors are web server and web client. To improve scalability and reliability URL, HTML, XML and HTTP play a very important role.
- Less hardware costs
  Hardware costs have been reduced significantly over the last decade while speed and efficiency of the processing has increased dramatically. These technological improvements have paved a way for servers with high density, which pack a large number of computing powers into small area.

6. CLOUD COMPUTING DEPLOYMENT MODELS

There are four cloud computing deployment models according to NIST: Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud. Figure 3 characterizes the NIST cloud computing deployment model definition.

- Private cloud
  As the name indicates, a private cloud [33] is managed within one organization. Also, it is not mandatory that the same organization runs the infrastructure; a third party can also manage it. Geographical location of cloud can also be away from that managing organization. Briefly private cloud serves single organization and is not consumed by other sources or customers.
- Public cloud
  The Public cloud is a shared infrastructure. Its physical infrastructure is embedded in CSP and the public can use it. As resources are shared so the users pay according to consumed resources [34]. The physical structure is out of the location. For instance, VMs, public storage apps. It is a multi-tenant virtualized environment. It refers to the usage of a number of data centers and file replications. It enhances the scalability of different IT resources.
- Community cloud
  A community cloud is cloud computing deployment model that provides cloud computing solution to a limited number of organizations or individuals that is governed, managed and secured commonly by all the organizations availing the services or is managed by the third-party service provider.
- Hybrid cloud
  Just like its name, an amalgam of two or more clouds form a hybrid cloud. The best feature is that the integrity of each model remains intact while serving some combined functionalities and standard technologies. Hybrid cloud [35] shares proprietary technology. Data and applications are shared equally among private and public cloud's amalgam. Hybrid clouds can handle any overflow [36] without giving access to third party datacenters. It is beneficial in scaling resources.

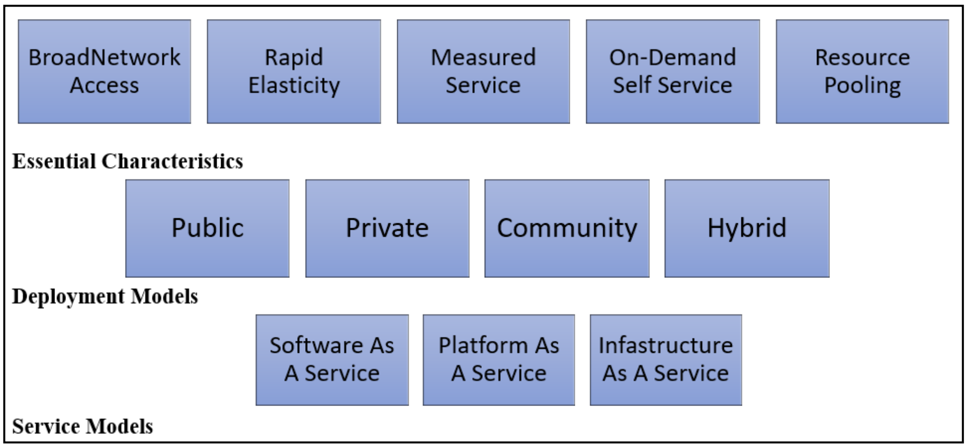

Figure 3. NIST cloud computing definition

7. CLOUD COMPUTING SERVICE MODELS

Cloud Computing Service models represent the different delivery models of cloud that are in use with the deployment models of cloud. The service models of cloud are PaaS (Platform as a Service), SaaS (Software as a Service) and IaaS (Infrastructure as a Service). Figure 4 shows the cloud classifications based on the service models. The example of each of the service model is given in Table 1. Examples for each of the service models is provided in Table 2.

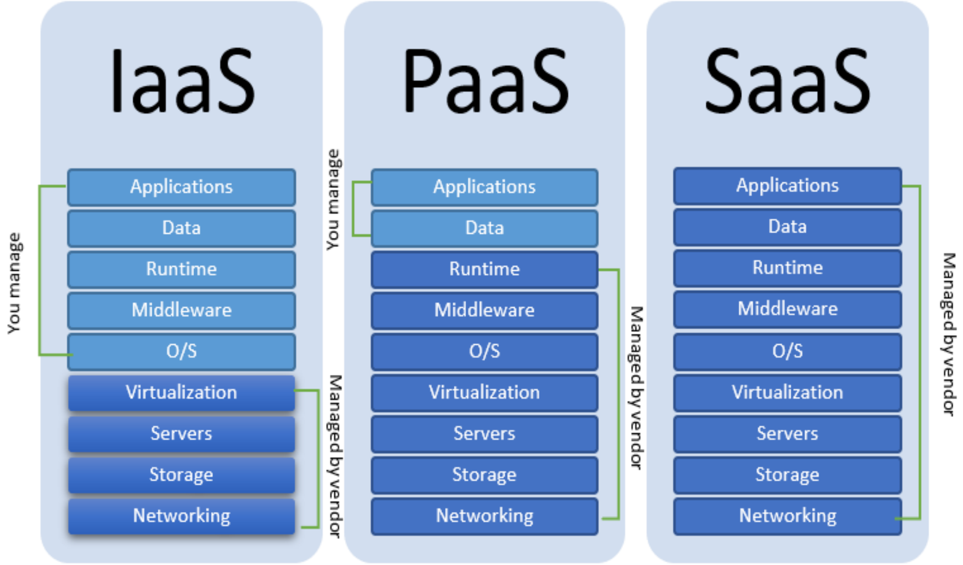

Figure 4. Classification of clouds based on the service model

- Infrastructure as a service (IaaS)
  IaaS is the lowest level of service provided to cloud users with greatest flexibility where the cloud users are provided controlled access to the hardware infrastructure [37] [38] The user can deploy operating system and application software of their choice. The client doesn't really have the control of the Physical hardware but are free to use the virtualized hardware [39] as they please. Client has to manage most of the security aspects of protecting the infrastructure.
- Platform as a service (PaaS)
  In the PaaS service model [40], Platform Software is already installed for the cloud user including Operating System, Storage Drives Controllers, Networking and other required software. User can install the software that they need on top of these infrastructure software. The virtual infrastructure and hardware is controlled by the CSP.
- Software as a service (SaaS)
  SaaS also referred to as 'on demand software'. SaaS is a model of software delivery and licensing where a complete and fully functional model is delivered via web to users on the basis of subscription. The end users access the SaaS offerings typically through web browsers.

Table 2. Example of cloud service provider based on the service model

Infrastructure as a Service (IaaS)	Storage	Desktop as a Service (DaaS)	Software as a Service (SaaS)	Platform as a Service (PaaS)
Microsoft Azure	Google Drive	VMware	Insightly	Heroku
Amazon Web Services	Box	Citrix	Salesforce.com	Red Hat OpenShift

8. TYPES OF CLOUD COMPUTING SECURITY THREATS

The security threats of cloud computing [41] are identified and classified into different categories as shown in the schematic Figure 5 below. It is to be noted that the attacks discussed in this section can also be categorized based on the service models. We have divided the cloud computing security attacks based on 5 categories. Each category is discussed in the subsequent sections.

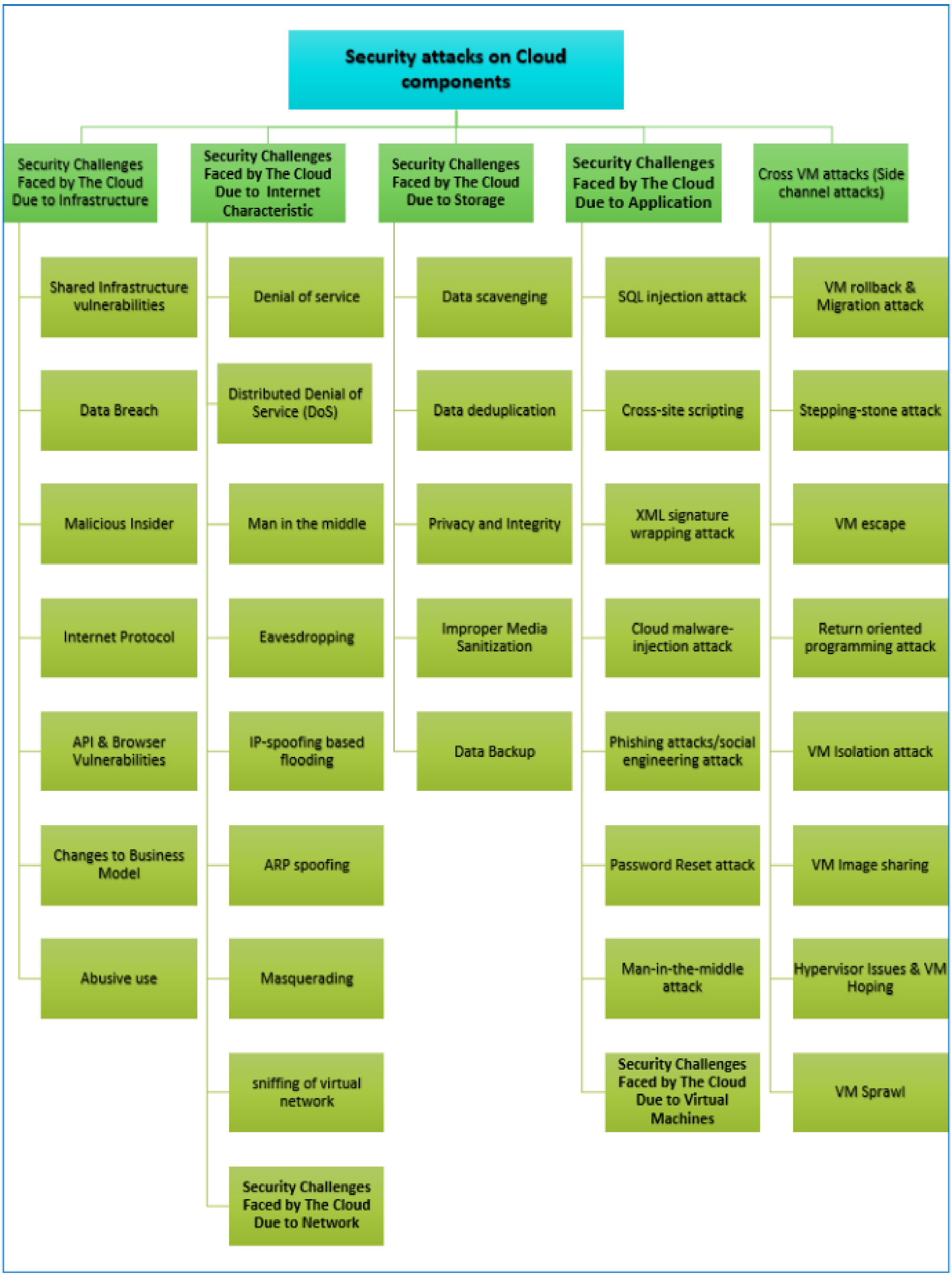
Security attacks on Cloud components
Security Challenges Faced by The Cloud Due to Infrastructure
Security Challenges Faced by The Cloud Due to Internet Characteristic
Security Challenges Faced by The Cloud Due to Storage
Security Challenges Faced by The Cloud Due to Application
Cross VM attacks (Side channel attacks)
Shared Infrastructure vulnerabilities
Data Breach
Malicious Insider
Internet Protocol
API & Browser Vulnerabilities
Changes to Business Model
Abusive use
Denial of service
Distributed Denial of Service (DoS)
Man in the middle
Eavesdropping
IP-spoofing based flooding
ARP spoofing
Masquerading
sniffing of virtual network
Security Challenges Faced by The Cloud Due to Network
Data scavenging
Data deduplication
Privacy and Integrity
Improper Media Sanitization
Data Backup
SQL injection attack
Cross-site scripting
XML signature wrapping attack
Cloud malware-injection attack
Phishing attacks/social engineering attack
Password Reset attack
Man-in-the-middle attack
Security Challenges Faced by The Cloud Due to Virtual Machines
VM rollback & Migration attack
Stepping-stone attack
VM escape
Return oriented programming attack
VM Isolation attack
VM Image sharing
Hypervisor Issues & VM Hoping
VM Sprawl

Figure 5. Classification of security threats to cloud computing

8.1. Cloud computing security challenges due to infrastructure

Infrastructure of cloud causes a number of security issues [42] [43] [44] [45] as mentioned below:

- Shared Infrastructure vulnerabilities
  Multi-tenancy is offered by the cloud computing where multiple customers share different resources of cloud. The underlying infrastructure components which support the installation of the cloud solutions are not good enough in some cases so as to provide isolation properties [46] to get a multi-customer software or multi-tenant structure. This can cause vulnerabilities due to shared technology [47] related to VMs, working methods, supervisor, etc. A misconfiguration or vulnerability in a shared platform can allow the attackers to compromise security of data of many or all customers which results in the data violation.

- Data Breach
  Data breaches are security attacks in which private, sensitive, or confidential data related to an organization or person is copied, sent, or accessed by the unauthorized party. Information breaches have been rated as the number one risk in cloud computing. Data breaches have affected 1.4 billion documents in 2017; many of the breaches included cloud servers as well. One Login, which provided single sign-on and identity management [48] capabilities for cloud services, was hacked in May 2017. Data breaches can occur due to human error, targeted attacks, vulnerabilities of program, or even bad safety practices.
- Malicious Insider
  This is probably the most dangerous threat to cloud computing. A malicious insider could be a system administrator, former worker, business spouse or a third-party contractor. This kind of security threat could be catastrophic [49]. For example, a recent British breach in Sage led to the dropping of organization's share price by 4.3%. Systems which solely depend on the cloud service providers for security providence are at a higher risk. A malicious insider like system administrator can access private info, can access the more crucial methods and may eventually cause an information breach.
- Internet Protocol
  The TCP/IP protocol suite has a vulnerability to a variety of external attack methods which range from IP spoofing, TCP session hijacking, RST and FIN attacks, TCP sequence no. attack, Ping O' Death, TCP session hijacking [49] denial of service and password sniffing. These vulnerabilities can place the internet user at a greater risk.
- API & Browser Vulnerabilities
  Exploiting the API of Cloud may provide the attacker ample accessibility to the resources of the cloud. Cloud Service Providers offer a set of APIs or user interfaces which clients use to socialize with the hosting solutions of cloud. These APIs are used to perform orchestration, provisioning and monitoring of the processes running in a cloud environment. API network can be vulnerable to DOS and DDoS attacks, socket flooding and buffer invasion. DOS (denial of service) and DDoS (distributed denial of service) related attacks in particular can cause severe access problems for user and delay in service pages. To get more substantial safety, cloud APIs ought to be obtained through encoded keys [50], that can be utilized to authenticate the API users. The Anthem Inc. information breach led to cyber offenders getting 80 million records of medical and personal info. This assault had been severe form of stolen consumer credentials. The attackers masquerading as valid users, or programmers can get and alter info or inject malicious applications which seems to arise from a valid origin [10].
- Changes to Business Model
  Businesses have a tendency to gravitate towards the usage of public clouds when expansion is cyclical and dynamic. When companies expect large spikes within their site visitors, or whenever they're on the lookout for more affordable alternatives, public clouds would be the favored option. Obviously, whenever there's not any privacy or sensitive information dilemma, public setup is a wonderful route to take because of its inclination to become less expensive than personal installation. Firms seem more likely to put money into a personal cloud infrastructure whenever there's a demand for high protection or custom-made cloud configurations. On the flip side, the Orthopedic Institute made a decision to benefit from a personal cloud because they needed to comply with rigorous medical insurance Portability and Accountability Act (HIPAA) guidelines for protecting patients' data.
- Abusive use
  Poorly bonded cloud support deployments, completely free cloud support trials, deceptive accounts and sign ups through payment ports expose the cloud computing versions to malicious attacks. Cases of misuse of tools of cloud include things like the launch of DDoS or EDoS strikes, spam e-mail, and other malicious attempts.

8.2. Security challenges to cloud computing due to internet characteristic

Cloud computing is vulnerable to a number of attacks due to its internet characteristic. It can cause a number of issues ranging from eavesdropping to complete system failure. Some of these challenges are discussed below.

- Denial-Of-Service
  The DOS attack takes place when an attacker hinders the authorized users from accessing the network. The impact of this attack is vast on infrastructure which is shared among trillion of users. New security concerns have risen in cloud computing due to increased use of cloud services and virtualized data centers [51]. The innovation in technology has given rise to innovated methods of attack. Botnets are helpful in spreading the DOS attacks quickly. The applications with low bandwidth and requiring more resources are more vulnerable to these attacks e.g. Twitter attack of 2009. SaaS services [16] are also more prone to these attacks because the effects on SaaS services indirectly affect the economy.

- Man-In-The-Middle
  These attacks occur because of the lack of security configuration in the SSL (Secure Socket Layer). The attacker watches for data shared between two parties and try to access it by being active in the middle. The attacker tries to reside and attack in between the communication process between two parties over cloud network.
- Eavesdropping
  In eavesdropping attack, information shared between the sender and receiver is accessed unethically by an attacker [52]. Users use a key to communicate. The attacker replaces that key with his own key and intercept the information.
- Ip-Spoofing Based Flooding
  This method used to obtain illegal access to machines, whereas an attacker illicitly manipulates IP packets. The IP Spoofing entails altering the header of packet using a spoofed (forged) origin IP speech, a checksum and also the purchase value. In IP spoofing-based flooding the normal IP is replaced with forged IP address causing spoofing.
- Masquerading
  A masquerade is a kind of attack in which the attacker pretends to be a legitimate user of a platform so as to acquire access to greater privileges than they're approved for. A masquerade could be attempted via using encoded IDs and passwords through discovering security gaps in applications, or via bypassing the authentication [53] [54] [55] mechanism. The effort may come from inside a company, as an instance, from a worker; or by an external user via a link to the public community.
- Distributed Denial of Service (DDoS)
  The DDoS attack [56] is used to disrupt the normal traffic of a targeted network, server or service by flooding with internet traffic. DDoS attack is similar to a traffic jam which clogs up the network and prevents the regular traffic from arriving at the destination.
- ARP Spoofing
  This is a kind of attack in which an attacker sends the falsified Address Resolution Protocol (ARP) messages over LAN (local area network). This links the MAC address of an attacker with the IP address of an authorized server or computer on the system. A virtual network can also become a victim of the ARP spoofing [4] [57] therefore causing an attacker VM to access the packets of other VMs. The cloud established antivirus or intrusion detection methods can be utilized to deal with such attacks.
- Sniffing of Virtual Network
  Virtual networks come across a lot of obstacles. When a Virtual network is distributed among different VMs spoofing or sniffing of virtual network can happen. The malicious sniffing and spoofing of the virtual network cause the cryptographic keys to become vulnerable to leakage. The data then becomes vulnerable to a lot of risks [58].

8.3. Security challenges faced to cloud computing due to storage

Cloud computing doesn't provide users with complete control over their information. Different to traditional computing method, the cloud computing system enables the service suppliers to exercise management to handle data and servers. The customers can have a certain degree of control just on the VMs [4] [59]. The absence of control over information can contribute to data security [60] risks as compared to traditional computing method. Here we provide a summary of the security challenges confronted to cloud due to storage providers. Icloud, Box, Dropbox, OneDrive, SugarSync, Amazon Cloud Drive, Google drive, Spideroak, Evernote, ADrive, Cubby, Wuala, and Copy [61] are some of the more widely used cloud storage providers.

- Data Scavenging
  When trying to delete information, it is not deleted entirely from documents. Therefore, the eliminated data might be retrieved by attackers and is known as data scavenging.
- Data Deduplication
  The duplicate copies of the redundant data are eliminated by Data Deduplication technique. The technique is used to reduce the bandwidth and for improving storage utilization [62]. Data deduplication [63] faces several security threats such as malicious users who may try to take ownership of files they are not entitled to [64].
- Privacy and Integrity
  Cloud storage is just one of the most cost effective [65] [66] and extremely manageable infrastructure but nevertheless vulnerable to a lot of troubles. The information on the cloud is considerably more vulnerable to dangers concerning ethics, confidentiality, and accessibility compared to the traditional computing model

[67]. Consumers on cloud are growing rapidly. Strike on a single thing can hamper a lot of the users because of the shared platform. Workers of SaaS providers using data could also be a possible threat.

- Improper Media Sanitization

  The process of removing the data irreversibly from media or destroying the media permanently is called media sanitization. There are a number of reasons for carrying out the process of media sanitization e.g., (a) the disc needs to be altered, (b) the information is not required any longer, and (c) the support has to be terminated. If the CSP doesn't sanitize the apparatus correctly, the information could be subjected to dangers. Sometimes the multi-tenancy feature also leads to the dangers associated with media sanitization. It might not be possible to end the life span of the machine completely due to its usage by several users [68].
- Data Backup

  The backup of information is an important problem that is dealt closely. The normal backup of data is necessary at the end of CSP to make sure the recovery and accessibility of information in the cases of accidental and deliberate disasters. In addition, the backup storage should be guarded against tampering and unauthorized access [69].

8.4. Security challenges faced to cloud due to web applications

Cloud computing faces several security threats due to web application's security challenges [70]. Some of them are discussed below:

- SQL injection attack

  The most common threat is the SQL injection attack. A malicious code is inserted in this attack and the user's information is stolen. When data is passed by user, attacker inserts personalized characters in it. It will change the nature of information and query. Resultantly the access to a database is gained by the attacker and can run their own commands of SQL [71] on the database so that it can be used to alter, delete and break into the standard design of database.
- Cross-site scripting

  Cross- site scripting is another technique of hacking. Malicious scripts are injected by attackers into contents of web [72]. The script could be Java or HTML. Cross site scripting attacks are generally targeted to websites complying web 2.0 standards. Secure cloud hosting company blocked 64 million cyber-attacks reportedly in 2012.
- XML signature wrapping attack

  It is possible to sign a portion of a SOAP Web Service request or response at the message level using XML Signature [73]. The message contains a security header with a signature element that references one or more message parts that have been signed. Typically, the message parts are referenced by an ID, and so to validate the signature the recipient must find the element in the request that has the corresponding ID. An XML Signature wrapping attack essentially exploits the fact that the signature element does not convey any information as to where the referenced elements are in the document tree.
- Cloud malware-injection attack

  In these Attacks, harmful code is injected by an attacker [16], which infects the pages of web when browsing is done. It can affect the functionality of cloud server. Attackers hack commands and insert their own.
- Phishing attacks

  Phishing attacks also known as social engineering attacks [74], are conducted by sending malware emails [50] that direct the users to spoofed sites. These attacks are harmful for enterprise as well as user. Attackers manipulate the users to access confidential information.
- Password reset attack

  In this attack, a hacker tries out each and every possible combination of characters to guess the password [75]. By use of tools, even strongly encrypted data can get exposed. This is a commonly practiced attack.
- Man-in-the-middle attack

  Due to lack of Secure Socket Layer (SSL) security configuration this attack occurs [76]. The attacker watches for data shared between two parties and tries to access it by being active in the middle. While communicating at cloud the attacker attacks the source, and in between the process. The actor is between two parties and resides unethically. This attack can be categorized as an application or Internet characteristic attack, hence discussed earlier as well.

8.5. Security challenges faced to cloud computing due to virtual machines

Cloud can face various threats due to VMs such as:

- Cross VM attacks

  The VM based attacks can extract the resource usage information [77], cryptographic keys information and other sensitive information from the targeted VM residing on the same physical machine as that of VM of attacker. These are exploitive for memory and cache. The countermeasures for cross VM attacks include cryptographic algorithms, authentication mechanisms [55], or deterministic execution to deal with the risk of cross VM attacks.

- VM rollback & migration attack
  The VM file contents become vulnerable to different kinds of attacks when an active VM is migrated from host physical machine to some other physical machine. For instance, an execution which is accessible during VM migration. Effective security policies configuration or proper resume/suspend activities may make the VM migration secure.
- Stepping-stone attack
  Although VMs have many benefits, they have some security loopholes. Attackers devise an intermediate host server rather than attacking directly from personal machines. The attack related commands are sent to the victim indirectly through though a series of compromised hosts which act as “stepping stones” in a stepping stone attack. The protection against these types of attacks through firewalls is very difficult because firewalls are only able to protect the network packet’s information.
- VM escape
  In this attack, the attacker runs the code on a VM that breaks out the operating system running within the VM allowing the direct interaction of attacker with hypervisor. Such attack gives the attacker access to all VMs running on that particular host and the host operating system.
- Return oriented programming attack
  This attack is an exploit technique against computer security in which an attacker executes the code against security defenses such as executable space protection and code signing. The program stack control is gained by the attacker who then hijacks the program control flow [78]. Attacker then executes chosen sequences of machine instructions present in the machine’s memory.
- VM isolation attack
  The VM running on the same physical hardware must be isolated from each other. Though logical isolation exists among distinct VMs, the accessibility to the same resources might result in the cross VM strikes and data violation. Isolation isn't just required on storage apparatus but computational and memory hardware also need good isolation of VMs [14].
- VM image sharing
  In VM image sharing, a malicious code is placed inside a VM image which can then get replicated during the creation of VMs. To deal with this, virtual image management system providing scanners and filters for recovering and detecting security violations can be used.
- Hypervisor issues & VM hoping
  Scheduler vulnerabilities may result in theft of service or resource stealing. Modified versions of scheduler can improve hypervisor’s security [79] [80].
- VM sprawl
  When the number of VMs on the host increases and a lot of the VMs remain in idle state then this is called VM Sprawl. This causes the resources to be wasted on a large scale [81].

9. SECURITY FRAMEWORK OF CLOUD COMPUTING

Security framework of cloud computing [82] [83] provides a comprehensive and integration solution for providing security in the Cloud. The framework which is represented in Figure 6. constitutes of the following components.

a. User authentication

Users can access the browser or server installed applications via varied devices such as PDA, notebook, or cellular phone via end user Service Portal by going through multi factor authentication. Multi-factors authentication [84] [85] takes place according to certificate issued by a third party Certification Authority.

b. End user service portal

After user authentication, a Sign-on Access Token can be issued with consumer certificate. The user information related to security policy and verification is shared with other components in cloud service provider and end-user service portal using XACML and KIMP by access control component. User can then use services without restriction of the service providers.

c. Single sign on

Presently, Users can have multiple accounts in different Service Providers using various usernames and distinct password. Thus, there is a tendency that great majority of community users can have the identical password where possible, which pose underlying security risks. The annoyance of numerous authentications [86] not just causes users to eliminate productivity but additionally borrows more administrative overhead. The enterprises now are thinking seriously about the usage of Single Sign on (SSO) technologies to tackle the password burst since they promise to reduce down several application and network passwords into one. To overcome this issue, it's implied to streamline security management and to implement powerful authentication inside the cloud, associations must use Single Sign- on to users that are cloud. This permits a user to get multiple services and applications at the cloud computing environment via one log, thereby enabling strong authentication at the consumer level.

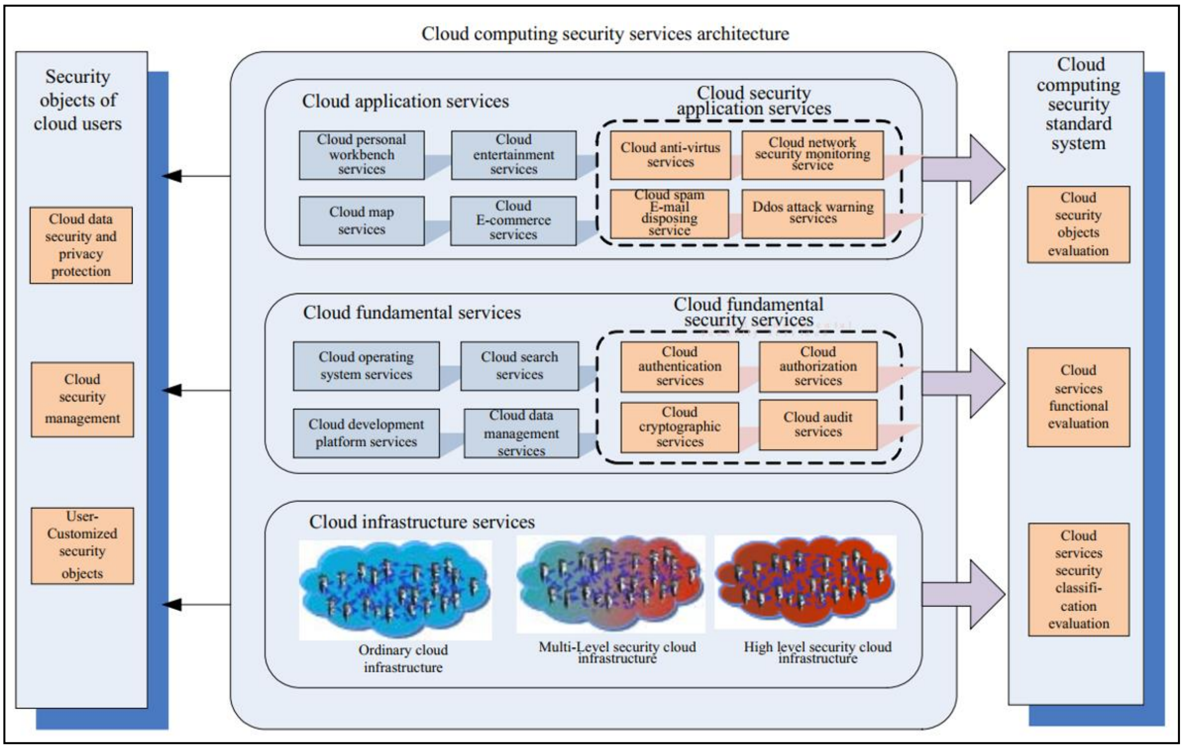
Cloud computing security services architecture
Security objects of cloud users
Cloud data security and privacy protection
Cloud security management
User-Customized security objects
Cloud application services
Cloud security application services
Cloud personal workbench services
Cloud entertainment services
Cloud map services
Cloud E-commerce services
Cloud anti-virtus services
Cloud network security monitoring service
Cloud spam E-mail disposing service
Ddos attack warning services
Cloud fundamental services
Cloud fundamental security services
Cloud operating system services
Cloud search services
Cloud development platform services
Cloud data management services
Cloud authentication services
Cloud authorization services
Cloud cryptographic services
Cloud audit services
Cloud infrastructure services
Ordinary cloud infrastructure
Multi-Level security cloud infrastructure
High level security cloud infrastructure
Cloud computing security standard system
Cloud security objects evaluation
Cloud services functional evaluation
Cloud services security classifi-cation evaluation

Figure 6. Cloud computing security framework [82]

d. Service configuration

The service enabler provides the personalized cloud services by using the user's profile. The user profile is provided to the service management of cloud service provider for interoperation and integration of the service provisioning requests from users. SPML (services provisioning markup language) can be used to share the user's profile. The asset manager requests to Cloud service provider for the personalized resources of the user through user's profile and the service is configured through VPN connection.

e. Security control

The component of security control provides sufficient protection for security policy, access policy and key management against the security threats. The access control module provides support for supplier's needs of access control. Role based access control (RBAC) is widely accepted and is the most efficient control model due to its flexibility, simplicity and support for efficient privilege management. RBAC is policy neutral and can capture a wide array of policies and is best suited for the integration of policies.

f. Security management

The security management element provides privacy and security specification. The authentication and identity control module is responsible for authenticating users and providers according to attributes.

g. Trust management

Due to the service oriented character of the cloud, the trust level [74] [87] should also be integrated with the service. The idea is, the more the services provided by the CSP, the higher the level of trust needs to be built [88] [55]. The trust should be bi-directional; the users should also trust the providers on which they rely on for their services and the providers should also have some trust on users to whom they release their services to. One approach is developing a trust management approach in which generic negotiation parameters of trust are included, integrated with the service and is bi-directional.

h. Service monitoring

This framework facilitates monitoring functionalities deployment for various applications and services within cloud. Online state monitoring is the most common application for Service monitoring, which continuously tracks certain states of networks, applications, instances, systems or any element that may be deployable within the cloud.

10. SOLUTIONS TO SECURITY THREATS OF CLOUD COMPUTING

Here we will discuss some of the solutions that can be employed to reduce the vulnerabilities to the Cloud and provide better security.

- Intrusion detection and prevention systems (IDS/IPS) for automated cloud protection
  An intrusion detection system (IDS) [89] monitors the network traffic for suspicious activities and when a suspicious activity gets discovered, it issues an alert. The reporting and detection of the anomaly are the primary functions of IDS. Some IDS systems are also capable of taking action when anomalous traffic or malicious activity is discovered. They can also block the traffic from suspicious IP addresses in some cases. Intrusion Prevention system (IPS) [89] also monitors the packets of the network traffic. When an IPS detects malicious traffic, it responds by rejecting such malicious traffic packets.
- Cloud Security via tokenization or encryption
  The security problems of cloud computing like privacy maintenance and confidentiality of information can be dealt with tokenization and encryption of the information. The plain text information is transformed into non-readable text called ciphertext by encryption algorithm. [90] The information is decrypted through an encryption key and an algorithm to transfer it back to plain text format. SSL encryption is used commonly to protect transmitted information over internet.
  The meaningful information like account number is turned into a random string of characters called a token which returns no meaningful value if breached. Token is the reference to the original data but cannot be used to guess the original values. Token has no algorithm or key used to derive the original data. Instead, tokenization uses a database 'token vault', to store the relationship between the token and sensitive value. The real data is then secured in the vault via encryption.
- Figure out hash of the files
  A hash is unique value corresponding the file contents. Rather than identifying the file contents by its extension, designation or name, a hash assigns a unique value to the contents of the file. The hash values provide a cryptographically secure way to verify that the contents of the file are not changed. The secure hash algorithm makes it impossible to change the contents of the file either by unauthorized or malicious attempt or by accident and maintain the same hash value. The hash values can be used to determine if the contents of two files are same. If the hash values of two files are same, the file contents are also identical. This method is being employed to secure the file and data transfer over the Cloud Computing.
- The alert correlation, assessment and reaction module-next generation system (ACARM-ng)
  ACARM-ng generates alerts for intrusion detection and correlates attacks. It receives message in IDMEF format which is a standard for communicating with IDF. It has filters, triggers and databases in it to correlate attacks, reacting to attacks and for storing alerts respectively.
- Suricata
  Suricata is a system that monitors the network traffic and prevents the security issues [81]. It alerts the systems if it detects any suspicious activity. Its multithreading feature enhances efficiency. It detects protocols rather than ports making it easy for the users.
- The open source security intrusion prevention system (OSSEC)
  The OSSEC [91] monitors individual hosts. It performs relevant tasks like log forwarding to servers, and generating alerts. Database manager is used by it to generate alerts.
- Snort
  Snort is a widely used open-source, lightweight and free Network Intrusion Detection System (NIDS) which provides protection against packet sniffing, packet logging and analysis. It uses the components pre-processor, packet sniffer [92], logger and detection engine to generate alerts.

- The next generation intrusion detection expert system (NIDES)
  It is a comprehensive real-time monitoring intrusion-detection system. It analyzes the activities of user. It does real time monitoring to suspect activities [93]. It uses rule-based analysis for detecting intrusion. It includes a resolver to detect and mitigate the issues.
- eXpert-BSM
  eXpert-BSM uses knowledge-based intrusion detection system to generate alarm on Sun-Solaris system. It performs audit by interference system for suspicious activities through user ports.
- Bro-IDS
  Bro IDS is now called Zeek. It is a free and open Source software framework for analyzing uses real time network traffic to detect intrusion. It monitors packet streams by using interpreter. It also checks for the IP headers and invalid packets are discarded. Event handling and generating of new notifications is done by interpreter.

11. CLOUD SECURITY REGULATORY BODIES AND COMPLIANCE

Due to the importance of cloud computing and severity of issues related to security, several regulatory bodies and mechanisms have been proposed that cloud service provider/broker and user needs to adhere to for the smooth running of the cloud services and protecting the resources and the users. We will discuss some of such regulations and compliance.

11.1. Privacy acts

Several privacy acts have been enacted in various regions of the world such as USA, Canada and Europe

- PIPEDA
  PIPEDA (personal information protection and Electronic Document Act) is a Canadian law related to the privacy of data [94]. It regulates how private organizations use, collect and disclose personal information in the commercial business. The act also contains provisions to facilitate electronic documents' use. The act requires organizations to obtain consent when they use, collect, or disclose the personal information of individuals.
- GDPR
  General data protection regulation (GDPR) is a European Union Law and covers the data privacy and protection for EU citizens [95]. The GDPR protects the 'personal data', which means information related to biographical data, data relating to physical appearance of individuals, education and work information. If a company collects data, they need to inform the data subjects what's being collected and why it's being collected. Another part of the regulation is that companies must have a lawful reason for collecting and processing any data.
- Data protection directive
  EU data protection directive which is also known as directive 95/46/EC is a regulation adopted by the European Union that regulates personal data use. As a legal guideline and standard, the data protection directive sets various limits on the ways that personal data can be used by third parties. It has generally been replaced by the GDPR adopted in 2016.
- USA patriot act (UPA)
  The USA Patriot Act [96] is an acronym for Strengthening and uniting America by Providing Appropriate Tools Required to Obstruct and intercept Terrorism. The purpose of the USA Patriot Act is to detect and punish the terrorist acts in the USA and worldwide. USA Patriot Act, since amended and reauthorized in 2003, made a lot of modifications to existing reports about the solitude of phone and digital communications, cash laundering, the performance of Foreign Intelligence Surveillance Court, legislation and other regions.
- ECPA
  The Electronic Communications Privacy Act (ECPA) prohibits a third party from disclosing or intercepting information without authorization in United States [97]. The Act was originally passed as an amendment to the Wiretap Act of 1968, applies to both private citizens and government employees. This act protects communications in transit as well as in storage.

11.2. Compliance

Compliance standards have been designed by Cloud Computing bodies [98] for the purpose of regularizing Cloud Computing usage and to define the standards for Cloud Service Providers.

- Common criteria
  This criterion is an international set of specifications and guidelines developed for evaluation of products of information security, in order to ensure they meet an agreed-upon security standard for government deployments. Common Criteria is formally called "Common Criteria for Information Technology Security Evaluation."
- Trusted computing compliance
  For promoting trust and security in computing platforms, a non-profit group of companies “trusted computing group” is formed. They have developed a Trusted Platform Module (TPM). TPM stores encryption keys specific to the host system for hardware authentication.
- Forensics
  Forensics are computer areas working to perform cloud audits [99] [100] [101]. They fight with cybercrimes and identify threats. The data is always dynamic with no physical storage. It keeps on travelling and sharing in cloud so can increase the threat of locality issues. Law of enforcement can solve these issues.
- Privacy ACTS compliance
  Government officials, organizations, private companies and individuals store data on cloud. For legal implications certain rules have been devised for security.
- Privacy of health-related information
  The Health Insurance Portability and Accountability Act (HIPAA) states rules for privacy and confidentiality related to health care. HIPAA states laws related to transmission and protection of health care data from all fronts, HIPAA also include provisions on data backup plans among other regulations and procedures.
- Privacy of electronic data
  The electronic data must be secured. The Electronic Communications Privacy Act (ECPA) states rules and restriction for protection of electronic data. It defines rules of how to access personal or private data. ECPA can give access to personal data if it is for confidential and security purpose.
- Privacy of financial data
  The Fair Credit Reporting Act (FCRA) (states rules to protect credit information of user. Customers save data of credit on cloud so, FCRA compliance is very necessary. Gramm–Leach–Bliley (GLB) Act also ensures data safety and confidentiality.

12. OPEN RESEARCH PROBLEMS AND CHALLENGES

The cloud computing environments have been widely accepted by a large number of organizations, the research in cloud computing security issues still faces some challenges. Moreover, new security challenges continue to get discovered due to the applications by organizations. In the following section some of the key research problems and challenges are discussed.

12.1. Application security

Cloud oriented applications are shared via internet. Any error in cloud apps can harm the cloud application. Behavior and quality of service is highly dependent on security hence the authentication and authorization need to be addressed correctly. Further, APIs ensure more security to cloud services.

12.2. Data access security

Data Access Security is the most difficult challenge to tackle because of data outsourcing. Data access security refrains from unauthorized access to read and write data. Its access is maintained by email authentication. Mostly customers access data through sites. It means they are more vulnerable to attackers. So some resolution is required.

12.3. Protocol vulnerabilities

The protocol is vulnerable to different kinds of threats for example SOAP messages. The protocol is vulnerable to manipulation and affects the cloud security. Similar APIs are reportedly causing various threats to data. A secure process either through encryption is required to mitigate this issue.

12.4. Data center security

Cloud is like a cluster system. It is often times designed just for storage [102]. The applications running on cloud are generally located at provider’s data center; hence upgrading and maintenance of data center software is not possible for the users of cloud. Cloud users use the IaaS API to access the software. The data encryption method can be applied to the data before sending onto cloud. The components of the network are shared between several tenants in cloud computing, making the network layer vulnerable to attacks. Some of famous network layer attacks include Sniffer attacks, DNS attacks, Network sniffing, issues of IP address reuse etc. Access to the network systems and the operating systems is controlled by network security measures in the datacenter. Moreover, the cloud computing model is vulnerable to threats due to virtual shared resource infrastructure. The authentication, backup and encryption are the some of the common ways to secure the data in virtualized data center [103]. SIEM is another approach used for real time events and networks.

Physical security is also very important in cloud-based applications. Physical security can be outsourced to third party data center which can restrict the access to the data center. These third-party data centers are mature enough to make the data secure on their side and require visitor registration, biometric scanner for employee authentication and employee badge access. The Data centers needs to ensure that the security is 99.99% to maintain its tier 4 level which gives it the status of being more secure. Tiers define the strength of security prospects. It is provided with physical security measures when other measures fail to achieve the task. For instance, a private company issues security cards to each of its employee to lock and unlock their chambers and data controls.

12.5. Identity management control

Identity services for organizations and users are managed by the IDM component. It is a core component that protects privacy and security problems in cloud computing. SLA documents provide guidelines on web services security. These guidelines define the standards on making applications communications secure by addressing integrity, confidentiality, and improving authentications. SLA documents also define rules for migrating information across different cloud computing platforms. Customers might lose confidence in a service of cloud due to non-availability status of a particular service or if the quality of the service does not abide by the SLA requirements.

12.6. Authentication

This is a way to verify a subject’s entity on a principal’s behalf. In authentication attacks, attackers prove themselves to be legitimate. Weak passwords [104] and registration process can be harmful for authentication. Strong authentication is necessary for strict privacy.

12.7. Integration

Integration refers to fact that data remains integrated and no third party can access or change it unwillingly. Protection of assets from illegal deletion of data, fabrication and modification should be ensured. Only authorized persons should alter data.

12.8. Multi-tenancy

Multi tenancy means sharing of resources among multiple cloud users. These users among which resources are shared are called tenants. The virtual platform [34] allows multiple running like JVM and .NET. Co-tenancy and co-location attacks can destroy multi tenancy. DoS attacks and illegal accessing of neighbor VMs is another big threat.

12.9. Third party services

Every aspect like cost and framework depends upon interface method. Some very big issues arise when the data is inherited from third party as there remains no control on transparency of data. Security issues can be mitigated by rectifying third party services.

12.10. Vendor lock-in

Issue arising due to lack of standards or SLA is called vendor lock in. Due to this issue transference among platforms is blocked. Sometimes programming languages differ due to migration among platforms as the APIs vary.

12.11. Encryption and key management

As the cloud computing is becoming popular, secure key management and encryption becomes more necessary. The encryption process enables data access control, poor storage and key management can make it vulnerable to threats. When the additional risk of having a third-party controlling logical and physical access is added to the infrastructure, the challenge of keeping the encryption keys secure becomes harder.

12.12. Access control

In cloud, data is outside the premises or boundaries which mean it is difficult for vendors to protect. Further data is mostly kept in same location by vendors making it vulnerable for unauthorized access. The solution to this is to keep the data of one user in segregated databases.

12.13. Defending cloud computing using software defined networking

Cloud services are growing, and the data centers are being converged by organizations in order to take advantage of continuity, quality of service and predictability delivered by the technologies of virtualization. In parallel, high security and energy-efficient networking [105] [106] is of increasing importance. The emergence of software-defined networking as an efficient network technology capable of supporting intelligent applications and the dynamic nature of future network functions has played an important role in defending cloud computing. It has lowered operating costs through simplified software, hardware, and management. In Software Defined Networking [107] [24] [56] [108] [109] the control and forwarding plane for the networking devices is separated. With the use of Network Analytics, the feedback system of the SDN [107] can provide active platform to mitigate security attacks on the Cloud Computing.

It has been shown in literature and somewhat in commercial deployments that software-defined networking can defeat security attacks including DDoS in the cloud environments. A contradictory relationship exists between DDoS attacks and SDN. On one side, the SDN capabilities, including centralized control, software-based traffic analysis, dynamic updating of forwarding rules and global view of the network, make it easier to react and detect the DDoS attacks. On the other side, the SDN security itself remains to be addressed as potential DDoS vulnerabilities also exist across the platforms of SDN.

12.14. Using machine learning to mitigate security threats

Machine learning has been used for text analytics, fraud detection, financial trading face recognition among others. Recent research has been focused on the use of matching learning [15] [110] [111] [112] [110] [113] techniques to identify security threats [83] and has identified issues that can be resolved via Machine Learning and Software Defined Networking solution, however it is suggested in the papers that there are considerable challenges in using Machine Learning for security solutions. The major challenge in these methods is obtaining unbiased and real-time datasets. Many datasets are internal and cannot be shared due to lack of certain statistical characteristics and privacy. As a result of this, researchers prefer to generate datasets for testing and training purpose [114] in the closed or stimulated experimental environments which might lack comprehensiveness. Machine learning models trained with such a single dataset generally result in a semantic gap between application and their results.

12.15. Cloud computing security legal issues

Cloud computing legal issues should be surveyed. Policies on how data is processed, stored and used should also be surveyed. Moreover, various regulations in the disclosure of data like health insurance records, financial data need to be examined. Furthermore, research on cloud security [115] and privacy is a highlighted issue.

12.16. Legal aspect related to SLA

SLA (service level agreement) legal aspect is still an open issue in cloud computing. The issues of service level and auditing are yet to be explored. The delivery of services as per the requirements is facilitated by run-time assurance mechanisms. The auditing mechanisms currently provided by CSP may not be satisfactory options for a number of cloud users. Moreover, usage service pricing depends on the cloud service providers totally. More work done in this area will help the users in the adoption of cloud.

12.17. Integrated security solution

The need to design an integrated and extensive cloud security solution is an important open research challenge. Each researcher focuses on solving a particular security issue and solves the issues in their own way. The research on specific security issue results in multiple security solutions to a specific issue. Employing multiple cloud security solutions could be dangerous. So there is a need to develop a more comprehensive and integrated security solution for easy implementation and management of the security tools.

13. FUTURE WORK

The increase in popularity of cloud computing is promising, and growth is predicted in the coming years. Cloud computing will be more flexible, effective and the technologies of cloud will change the way application platforms are viewed along with infrastructure and software development. Large number of organizations are expected to migrate to cloud environments and will chose hybrid cloud environments. Cloud computing will grow in the coming years with development of innovative solutions using artificial intelligence and machine learning.

Enterprises should educate and instruct their teams about security control features that are provided by cloud service providers. The belief that only CSPs are responsible for the security of their customer’s information shows that enterprises are not addressing properly on how employees should use external applications. Very little security incidents affecting organizations using cloud computing occurred on the CSP's part. Ultimately, it's an organization's duty to apply security control over cloud environments. The public cloud's regulatory compliant procedures require organizations to implement and define clear guidelines on risk acceptance processes of cloud and cloud usage responsibility.

Due to increasing security requirements, access to data centers should be limited. To enter into the secure premises, one should possess an electronic key and should undergo biometric scanning procedure.

The future of cloud computing is extremely promising with a huge opportunity, but it is dependent on the security. Cloud computing will show a powerful impact on the world in the coming years. The awareness of the latest innovations in cloud security technologies is necessary in order to provide secure solutions and to remain competitive.

14. CONCLUSION

In this paper, a survey of virtualization and related technologies are provided first, including virtualized networks and virtualized zdata centers. We discussed some of the characteristics of cloud computing and its services models, deployment models and storage models. Several security threats and challenges to cloud computing have been discussed. Cloud technology has many issues as well like storage issues. Cloud computing is vulnerable to four categories of attacks network related attacks, storage related attacks, application related attacks and VM related attacks. Security framework and several infrastructure challenges have also been investigated in this paper. Various security solutions have also been presented.

There are still many open issues and challenges to security of the cloud environment despite the rigorous research efforts of the research community. The development of integrated and comprehensive security solution for the security challenges faced to cloud computing is needed. The research related activities are focused on resolving these issues or in some cases focus on a solution of a specific security issue. The research focused on specific issue might result in the development of more than one solution which may also cater other security needs as well. Configuration and deployment of multiple security solutions is quite risky, so an integrated security solution should be deployed. An integrated security solution results in an easy management of security tools. Or at the very least, different security solutions should be harmonized to achieve desired security level.

15. ETHICAL STANDARDS COMPLIANCE

- Conflict of Interest: Wajid Hassan declares that he has no conflict of interest.
- Ethical Approval: The authors did not perform any studies with human participants or animals in this article.

This survey paper utilizes the recent published work of various authors and all these papers are listed in the reference section.

REFERENCES

[1] L. H. K. H. R. W. Martin Henze, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Generation Computer Systems,* no. 56, pp. 701-718, 2016.

[2] Alani, Mohammad, "Securing the Cloud: Threats, Attacks and Mitigation Techniques," *Journal of Advanced Computer Science & Technology,* vol. 3, no. 2, 2014.

[3] Aitel, D, 2012.

[4] K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Services App,* vol. 4, no. 1, pp. 1-13, 2013.

[5] T. W. Sriram Natarajan, "Security Issues in Network Virtualization for the Future Internet," University of Massachusetts, Amherst, USA, 2012.

[6] Y.-S. J. H. P. Saurabh Singh, "A survey on cloud computing security: Issues, threats, and solutions," 2016.

[7] T.-S. Chou, "Security Threats on Cloud Computing Vulnerabilities," *International Journal of Computer Science & Information Technology (IJCSIT)* , vol. 5, no. 3, 2013.

[8] D. Chen, H. Zhao, "Data security and privacy protection issues in cloud computing," *International Conference on Computer Science and Electronics Engineering (ICCSEE, IEEE),* vol. 1, pp. 647-651, 2012.

[9] Calyptix, "Biggest Cyber Attacks 2017: How They Happened," 2017.

[10] "Networks and Security for Virtualized Compute Environments," VMWare,Inc, USA.

[11] N. V. Juliadotter and K.-K. R. Choo, "Cloud Attack and Risk Assessment Taxonomy," *IEEE Cloud Computing,* pp. 2(1):14-20, 2015.

[12] A. Shameli-Sendi, M. Pourzandi, M. F. Ahmed and M. Cheriet, "Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing," *Journal of Network and Computer Applications,* vol. 58, pp. 165-179, 2015.

[13] Minhaj Ahmad Khan, "A survey of security issues for cloud computing," Multan, 2016.

[14] K. C. Ashish Singh, "Cloud security issues and challenges: A survey," Bihar, 2016.

[15] Salman iqbal, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *Journal of Network and Computer Applications,* vol. 74, pp. 98-120, 2016.

[16] S. V. Mazhar Ali, "Security in cloud computing: Opportunities and challenges," *Information Sciences,* no. 305, pp. 357-383, 2015.

[17] A. Patel, M. Taghavi, K. Bakhtiyari and J. C. Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *An intrusion detection and prevention system in cloud computing: A systematic review,* vol. 36, no. 1, pp. 25-41, 2013.

[18] G. Grispos and W. Glisson, "Cloud Security Challenges: Investigating Policies, Standards and Guidelinges in a Fortune 500 Organization," in *European Conference on Information Systems (ECIS),* 2013.

[19] C. Modi, D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *The Journal of Supercomputing,* vol. 63, no. 2, pp. 561-592, 2013.

[20] D. Sun, G. Chang, L. Sun and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," *Procedia Engineering,* vol. 15, pp. 2852-2856, 2011.

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

[22] K. K. G. Christos Stergiou, "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems,* no. 78, pp. 964-975, 2018.

[23] Jian Shen,, "A secure cloud-assisted urban data sharing framework for ubiqutous cities," *Pervasive and Mobile Computing,* no. 41, pp. 219-230, 2017.

[24] W. Hassan, "Cloud Computing: Survey on Services, Enhancements and Challenges in the era of Machine Learning and Data Science," 2019.

[25] F. Liu, J. Tong, J. Mao, R. B. Bohn, J. V. Messina, M. L. Badger and D. M. Leaf, "NIST Cloud Computing Reference Architecture," NIST Pubs, 2011.

[26] "NERSC Cyber Security Tutorial," 2012. [Online]. Available: http://www.nersc.gov/users/training/onlinetutorials/cybersecurity-tutorial/.

[27] Ralph and Thomas, "CLOUD PENETRATION TESTING," *International Journal on Cloud Computing: Services and Architecture (IJCCSA,* vol. 2, no. 6, 2012.

[28] M. A. D. A. P. D. A. A. J. B. E. A. …. H. S. Ahronovitz, "Cloud Computing Use Cases A white paper," *Cloud Computing Use Case Discussion Group,* vol. 4, pp. 1-68, 2010.

[29] V. C. a. M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," *IEEE Transactions on Services Computing,* vol. 9, no. 1, 2016.

[30] W.A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," in *44th Hawaii International Conference on System Sciences (HICSS,* 2011, pp. 1-10.

[31] X. C. L. S. W. L. Y. Yinghui Zhang, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences,* no. 379, pp. 42-61, 2017.

[32] S. Z. H. MICHAEL PEARCE, "Virtualization: Issues, Security Threats, and Solutions".

[33] L. Y. D. D. S. D. N. P. D. S. a. D. K. P Aruna, "Private Cloud for Organizations: An Implementation using Open Stack," *International Journal of Scientific & Engineering Research,* vol. 4, no. 10, 2013.

[34] J. G. P. C. Justin Pettit, "Virtual Switching in an Era of Advanced Edges," 2009.

[35] H. L. P. A. V. P. R. M. P. G. J. A. R. D. H. P. C. R. P. S. R. Y. A. Dinkar Sitaram, "Security Infrastructure for Hybrid Clouds and Cloud Federation," *Journal of Internet Technology and Secured Transactions (JITST),* vol. 3, no. 3/4, 2014.

[36] V. Vladimir, "Cloud adoption issues: interoperability and security," in *Cloud adoption issues: interoperability and security,* 2013, pp. 53-65.

[37] I. T. M. Wesam Dawoud, "Infrastructure as a Service Security: Challenges and Solutions," 2010aa.

[38] "Securing virtual desktop infrastructure with NetScaler," Citrix, USA, 2015.

[39] researchgate, "Infrastructure as a Service Security Challenges and Solutions," [Online]. Available: 1. http://www.researchgate.net/publication/234013917_Infrastructure_as_a_Service_Security_Challenges_and_Solutions/file/79e4150e42c3ae7c12.pdf.

[40] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, "A security analysis of amazon's elastic compute cloud service," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, 2012, pp. 1427-1434.

[41] N. K. Dr. R. Sridaran, "A Survey on Security Threats for Cloud Computing".

[42] M. f. A. S. I. R. K. S. Syed Asad Hussain, "Multilevel classification of security concerns in cloud Computing," *Applied Computing and Informatics,* vol. 13, pp. 57-65, 2017.

[43] Ahmed Khalid Salih, "A survey of Cloud Computing Security challenges and solutions," 2016.

[44] G. H. Cooper, "Providing Avirtual Security Appliance Architecture to Virtual Cloud Infrastructure". USA Patent US 9,571,507 B2 , 14 Feb 2017.

[45] J. L. M. Rodrigo Romana, "Mobile edge computing, Fog et al.: A survey and analysis of security,threats and challenges," *Future Generation Computer Systems,* vol. 78, pp. 680-698, 2018.

[46] Y.-H. K. R. Victor Chang, "Cloud computing adoption framework: A security framework for business clouds," *Future Generation Computer Systems,* no. 57, pp. 24-41, 2016.

[47] Godefroid, P., Molnar, D, "Fuzzing in The Cloud (Position Statement)," 2010.

[48] Rion Dutta, *"Planning for Single SignOn.*

[49] Z. C. X. D. a. A. V. V. Jun Zhou, "Security and Privacy for Cloud-Based IoT:Challenges, Countermeasures, and Future Directions," *Impact of Next-Generation Mobile Technologies on IoT: Cloud Convergence.*

[50] N.-u.-h. S. A. K. M. M. D. H. Michael R. Watson, "Malware Detection in Cloud Computing Infrastructures," *IEEE Transactions on Dependable and Secure Computing,* vol. 13, no. 2, 2016.

[51] K.S. Rao, P.S. Thilagam, "Heuristics based server consolidation with residual resource defragmentation in cloud data centres," *Future Gener. Comput.Syst.,* 2014.

[52] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilako, "Security and privacy for storage and computation in cloud computing," pp. 371-386, 2014.

[53] J. M. a. F. W. Qi Jiang, "On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Computing Services," *IEEE Systems Journal,* vol. 12, no. 2, 2018.

[54] John Rohton, "The Identity Component Keystone," 11 Dec 2013. [Online]. Available: http://www.ibm.com/developerworks/cloud/library/cl-openstack-keystone/.

[55] K. Munshi, *openstack keystone identity service,* CTO,Atpira, Oct17,2012.

[56] Qiao Yan, F. Richard Yu, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," *IEEE Communications Surveys & Tutorials,,* vol. 18, no. 1, 2016.

[57] W. P. R. W. Andre van Cleeff, "Security Implications of Virtualization:A Literature Study," 2009.

[58] W. A. Sultan Aldossary, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 7, no. 4, 2016.

[59] V. F. V. S. M. M. P. M. H. D. H. M. D. Z. Peter Schoo, "Challenges for Cloud Networking Security," 2010.

[60] W. Liu, S. Peng, W. Du, W. Wang, G.S. Zeng, "Security-aware intermediate data placement strategy in scientific cloud workflows," *Knowl. Inform. Syst,* vol. 41, no. 2, pp. 423-447, 2014.

[61] Brandon Batler, "Cloud Computing Gartner Top 10 Cloud Storage Providers," 3 Jan 2013. [Online]. Available: http://www.networkworld.com/article/2162466/cloud-computing/gartner-top-10-cloud-storage-providers.html.

[62] N. Gonzalez, C. Miers, F. Redgolo, M. Simplcio, T. Carvalho, M. Nslund, M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud Computing," *J. Cloud Comput,* vol. 1, no. 1, pp. 1-18, 2012.

[63] W. D. X. Y. H. Z. H. D. F. Zheng Yan, "Deduplication on Encrypted Big Data in Cloud," *IEEE TRANSACTIONS ON BIG DATA,* vol. 2, no. 2, 2016.

[64] V. R. P. a. D. B. P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," *IJIRST –International Journal for Innovative Research in Science & Technology|* , vol. 2, no. 9, 2016.

[65] "Chapter 1, "Ethernet-to-the-Factory Solution Overview."," in *Ethernet-to-the-Factory 1.2 Design and Implementation Guide*.

[66] M. I. X. W. L. Z. Z. Q. Zhihua Xia, "A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," *EEE Transactions on Information Forensics and Security,* vol. 11, no. 11, 2016.

[67] S. R. R. B. Syam Kumar Pasupuleti, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *Journal of Network and Computer Applications,* no. 64, pp. 12-22, 2016.

[68] O. C. L. R. L. B. JUN TANG, "Ensuring Security and Privacy Preservation for Cloud Data Services".

[69] K. L. W. S. J. L. Y. X. Joseph K. Liu, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," *IEEE Transactions on Computers,* vol. 65, no. 6, 2016.

[70] D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, "Security issues in cloud environments: a survey," *Int. J. Inform. Sec,* vol. 13, no. 2, pp. 113-170, 2014.

[71] *OASIS, “Service Provisioning Markup Language(SPML)”.*

[72] "OASIS, “Key Management Interoperability Protocol (KMIP)”".

[73] "OASIS, “eXtensible Access Control Markup Language(XACML)".

[74] Matt Blaze, Sampath Kannan, Insup Lee, Oleg Sokolsky, Jonathan M. Smith, Angelos D, "Dynamic Trust Management," *IEEE Computer,* pp. 44-51, 2009.

[75] Miller, B., Fredriksen, L. & So, B, "An empirical study of the reliability of unix utilities,Communications of the ACM," vol. 33, no. 12, pp. 32-44, 1990.

[76] Graham, R. D, "Ferret & Hamster Sidejacking Tools," 2012. [Online]. Available: http://www.erratasec.com/sidejacking.zip.

[77] R. K. a. R. S. Yun Zhang, "Secure Information and Resource Sharing in Cloud".

[78] J. G. a. I. M. Mohamed Al Morsy, "An Analysis of the Cloud Computing Security Problem," Australia, 2016.

[79] M. G. a. S. K. G. Nancy Arya, "Hypervisor Security - A Major Concern," *International Journal of Information and Computation Technology,* vol. 3, no. 6, pp. 533-538, 2013.

[80] Ramaswamy Chandramouli, "Security Assurance Requirements for Hypervisor Deployment Features".

[81] "Principles of Network and System Administration," Oslo University, Norway.

[82] F. DG, Z. M, Z. Y and X. Z, "Study on cloud computing security," *Journal of Software,* vol. 22, no. 1, pp. 71-83, 2011.

[83] S. N. G. Srujan Das Kotikela, "Virtualization Based Security Framework (vBASE)".

[84] Bartek Kupidura, "understanding openstack authentication: keystone KPI," 10 July 2013. [Online]. Available: https://www.mirantis.com/blog/understanding-openstack-authentication-keystone-pki/.

[85] A. F. T. Allan Edwin Wetter, "cloud service authentication". USA Patent US 9.418,216 B2 , 16 Aug 2016.

[86] M. E.-K. B. K. a. H. S. Ismail Butun, "Cloud-Centric Multi-Level Authentication as a Service for Secure Public Safety Device Networks," *Critical Communications and Public Safety Networks.*

[87] Dongwan Shin and Gail-J. Ahn, "Role-based Privilege and Trust Man- agement," *Computer Systems Science and Engineering Journal,* vol. 4, no. 6, 2005.

[88] M. K. E. S. Z. W. W. Dan GonzalesJeremy, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," *IEEE Transactions on Cloud Computing,* vol. 5, no. 3, 2017.

[89] Jason Dablow, "Layered Cloud Security with IPS & IDS," 19 Jan 2017. [Online]. Available: https://www.trendmicro.com/aws/ips-ids/.

[90] G. S. V. A. S. Akashdeep Bhardwaja, "Security Algorithms for Cloud Computing," *International Conference on Computational Modeling and Security,* no. 85, pp. 535-542, 2016.

[91] Asif Imran,Kazi Saqib, "Web Data Amalgamation for Security Engineering: Digital Forensic Investigation of Open Source Cloud," *Journal of Universal Computer Science,* vol. 22, no. 4, pp. 494-520, 2016.

[92] Satish Kumar Garg, "Wireless Network Security Threats," haryana, 2011.

[93] A. A. J. Shadi A. Aljawarneh, "Cloud security engineering: Early stages of SDLC," *Future Generation Computer Systems,* no. 74, pp. 385-392, 2017.

[94] "Office of The Privacy Commissioner of Canada," Jan 2018. [Online].

[95] Nate Lord, "What is the Data Protection Directive? The Predecessor to the GDPR," 12 Sep 2018. [Online]. Available: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

[96] Brian Duignan, "USA Patriot Act," 20 DEC 2018. [Online]. Available: https://www.britannica.com/topic/USA-PATRIOT-Act.

[97] "Electronic Communications Privacy Act of 1986 (ECPA)," [Online].

[98] R. R.Kalaiprasath, "Cloud Security and Compliance - a Semantic Approach in End to End Security," *International Journal on Smart Sensing And Intelligent Systems Special Issue,* 2017.

[99] A. T. S. Josiah Dykstra, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Digital Investigation,* pp. 87-95, 2013.

[100] M. A. K. A. Muhammad Baqer Mollah, "Security and privacy challenges in mobile cloud computing: Survey and way," *Journal of Network and Computer Applications,* no. 84, pp. 38-54, 2017.

[101] W. B. g. Y.-K. R. C. Nurul Hidayah Ab Rahman, "Forensic-by-Design Framework for Cyber Physical Cloud Systems," *Digital Forensics.*

[102] N. D. W. C.-K. R. C. Nurul Hidayah Ab Rahman, "Cloud incident handling and forensic-by-design: cloud storage as a Case Study," 2016.

[103] X. W. X. S. Zhihua Xia, "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems,* vol. 27, no. 2, 2016.

[104] A. M. G. S. H. P. Yiannis Verginadis, "PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services," 2017.

[105] "Network Functions Virtualization, An Introduction, Benefits, Enablers, Challenges & Call for Action - ETSI".

[106] Y. D. W. Y. Hanqian Wu, "Network Security for Virtual Machine in Cloud Computing".

[107] Mohammad R. Abbasi, "Traffic Engineering in Software Defined Networks: A Survey," 2016.

[108] J. L. H. L. G. M. C. Ping Li, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems,* no. 74, pp. 76-85, 2017.

[109] W. Hassan, "Future Controller Design and Implementation Trends in Software Defined Networking.," *Journal of Communications,* vol. 13, no. 5, pp. 209-217, 2018.

[110] C. T. V. K. Gunasekaran Manogaran, "MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing," *4th International Conference on Recent Trends in Computer Science & Engineering,* no. 87, pp. 128-133, 2016.

[111] P. Z. V. V. Zheng Yan, "A security and trust framework for virtualized networks and software-defined networking," *Security and Communication Networks,* vol. 9, pp. 3059-3069, 2016.

[112] M. P. Z. Tommy Koorevaar, "Elasticenforcement Layer for Cloud Security Using Sdn". USA Patent US 9,304.801 B2 , 5 April 2016.

[113] A. Sathi, M. Thomas, J. Radadia, K. Kralick and R. Lanahan, "Support your business requirements using big data and advanced analytics," IBM, 24 September 2013. [Online]. Available: https://www.ibm.com/developerworks/library/ba-adv-analytics-platform1/index.html. [Accessed 10 November 2018].

[114] K. Hanford, "Automatic generation of test cases," *IBM Systems Journal,* vol. 9, no. 4, pp. 242-257, 1970.

[115] A. A. H. C. Arwa Alrawais, "Fog Computing for the Internet of Things: Security and Privacy Issues," *Fog Computing.*