DE GRUYTER OPEN

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **17**, No 4
Sofia • 2017 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2017-0039

Exploring Security Issues and Solutions in Cloud Computing Services – A Survey

P. Ravi Kumar[1], *P. Herbert Raj*[2], *P. Jelciana*[3]

[1]*School of ICT, IBTE JB Campus, MOE, Kuala Belait, Brunei*
[2]*School of ICT, IBTE SB Campus, MOE, Seria, Brunei*
[3]*Laksamana College of Business, Bandar Seri Begawan, Brunei*
E-mails: ravi.patchmuthu@ibte.edu.bn herbert.raj@ibte.edu.bn jelciana@yahoo.com

Abstract**:** *Cloud computing is emerging as one of the powerful computing technologies in the field of Information Technology due to its flexibility and cost reduction. This paper provides a detailed survey on security issues of the services provided by cloud computing and solutions to mitigate them. The main objective of this paper is to empower a new researcher to figure out the concepts of cloud computing, the services provided by them, and the security issues in the services. It also provides solutions to avoid or mitigate the different security issues which occur in the services provided by cloud computing. Additionally, it provides insight into the cloud computing model proposed by the National Institute of Standards and Technology* (*NIST*)*, data stages and data security basics in a multi-tenant environment. This paper explores the different security methods proposed by different researchers and analyzes them.*

Keywords**:** *Cloud computing, cloud services, cloud computing model, cloud security, cloud security solutions.*

1. Introduction

According to National Institute of Standards and Technology (NIST), cloud computing is defined as "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources* (*e.g., networks, servers, storage, applications and services*) *that can be rapidly provisioned and released with minimal management effort and or service provider interaction.*" [1]. Cloud computing is evolving as one of the ubiquitous paradigms in computing where computing infrastructure and solutions are delivered as a service. Most of us are using cloud computing without realizing it like Gmail, Office 365, Dropbox, etc. According to a recent report from Forbes says that worldwide public cloud revenue will increase from $80B in 2015 to $167B in 2020 [2].

Cloud computing provides numerous benefits like less investment and faster access to infrastructure, anytime, anywhere accessibility and better geographic coverage at a faster time. Also cloud computing take care of the software upgrades, licenses and maintenance from customers thus by minimizing the user involvement [3]. Because of the above benefits, many small and medium-sized companies are already migrated or in the process of migrating to cloud computing. The migration process empowers the companies to focus on their core business process to increase profitability rather than focus on the IT infrastructure [8]. There are also certain significant issues concerned with cloud computing, which makes it difficult for certain companies and government agencies to migrate to the cloud. The major cloud problems are with the security and privacy of the data stored in the cloud and the lack of resources and expertise. This paper focuses on the cloud security. The cloud security turns out to be more vulnerable due to its architectural foundation-elements such as heterogeneity, resource sharing, multi-tenancy, virtualization, mobile cloud computing and Service Level Agreement (SLA).

As more and more companies are embracing the cloud computing, the security issues are escalating due to the accumulation of digital assets [3]. Traditional security measures will not be effective in cloud computing because the cloud operating environments (multi-tenant, heterogeneity, virtualization, etc.) are totally different from traditional computing. In the traditional computing, there is a clear distinction between insiders and outsiders and the security administrator takes the sole responsibility for the security policies and protection of data and assets. In cloud computing, the gap between insiders and outsiders are very ambiguous and in certain cases, the outsiders become insiders. Cloud computing is very susceptible to malicious inside attackers due to multi-tenancy and side attack from outsiders. So cloud computing should have multi-tiered security procedure based on the service delivery models and deployment models.

Many researches have been conducted on security issues in cloud computing with various aspects. A survey of security issues in service delivery models are done in [4, 5] wherein the former [4] gave a special attention to Software as a Service (SaaS) model. A survey of security issues in the deployment models are done in [6, 7] and the authors provided mitigation techniques also. In [4, 6, 8], the authors did a survey on data security and privacy issues in cloud computing. Other authors [9, 10] did a survey on security issues related to Network and Infrastructure. Multi-tenancy and virtualization security issues are highlighted by authors in [7, 8, 11]. This paper uses a unique approach in bringing the security issues in cloud computing by using the services provided by them and also provided solutions to avoid or mitigate the security issues.

This paper is organized as follows. In Section 2, evolution of cloud computing is described briefly using a diagram. Section 3 describes the cloud computing model using the standard NIST model which includes the essential characteristics, deployment model and service delivery model of cloud computing with the nine services provided by cloud computing. Section 4 starts with data security fundamentals, followed by data stages and the later part of Section 4 is dedicated to security issues in the services provided by cloud computing and solutions to thwart

security issues. Section 5 concludes this paper by providing new developments and their challenges in the cloud computing.

2. Evolution of cloud computing

Cloud computing has evolved through a number of stages. Fig. 1 shows the evolution of cloud computing [12]. It started off with Utility Computing and then evolved to Cluster Computing. Cluster Computing has evolved into Grid Computing and then to Cloud Computing and it has not stopped there. Mobile Cloud Computing (MCC) is evolved from Cloud Computing.

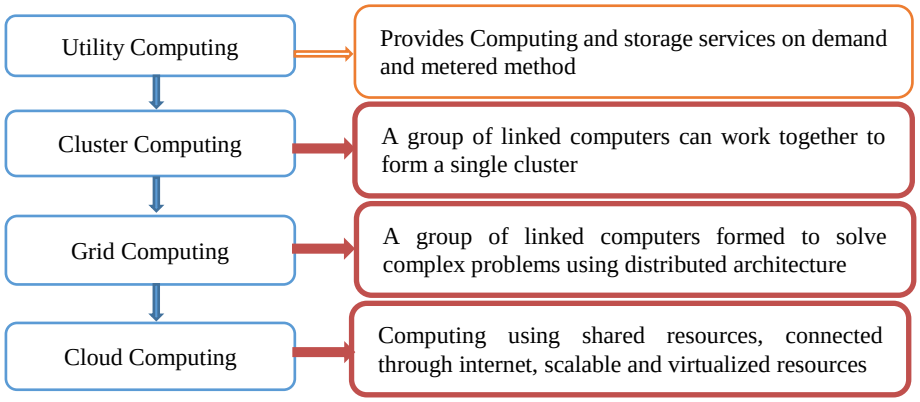

Fig. 1. Evolution of cloud computing

3. Cloud computing model

According to H o g a n and S o k o l [1], there are five entities associated with cloud computing based on the participation. The first entity is Cloud Service Provider (CSP) who provides the cloud services to customers. The second one is Cloud Service Customer (CSC) who consumes the cloud facilities provided by the provider. The third one is a Cloud Auditor (CA) who conducts an independent assessment of cloud services, operations, performance and security of the cloud implementation. The fourth one is a Cloud Broker (CB) who manages the use, performance and delivery of cloud services and negotiates relationship between CSP and CSC. The fifth entity is a Cloud Carrier (CC) who provides connectivity and transport of cloud services from CSP to CSC. A cloud computing model consists [1] of three cloud service delivery models and four cloud deployment models and five essential characteristics as shown in Fig. 2.

Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are the three service delivery models. Public, Private, Hybrid and Community are the four cloud deployment models. The five key essential characteristics are *Rapid Elasticity*, *Measured Service*, *Resource Pooling*, *Broad*

Network Access and *On-Demand Self Service*. The above five characteristics are important in the design and development of cloud models.

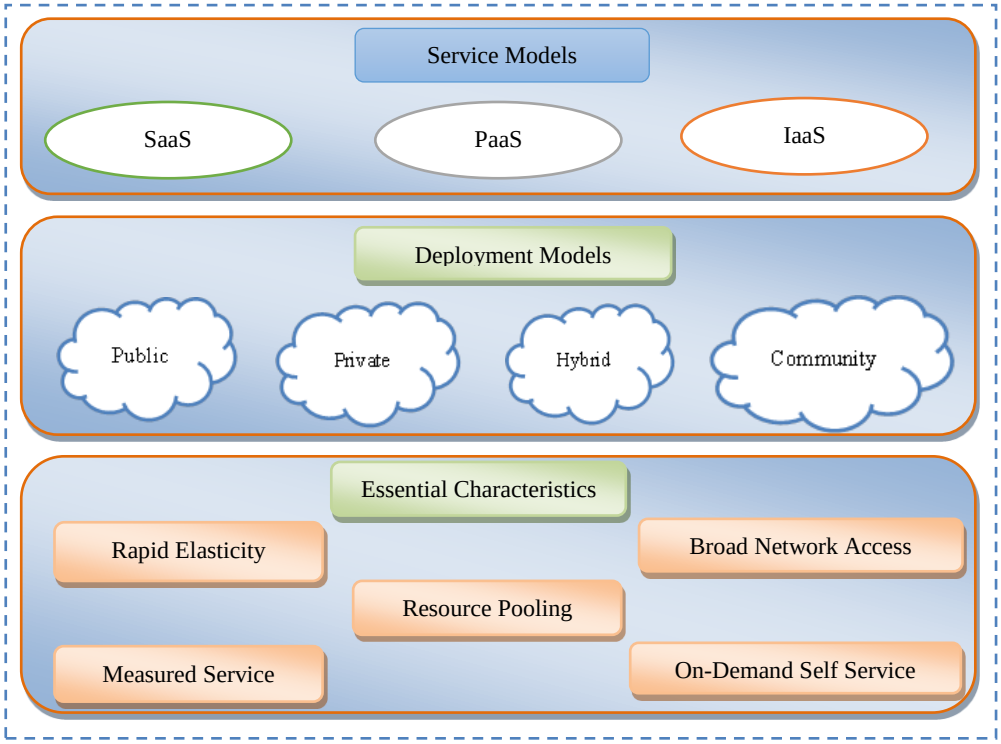

Fig. 2. NIST based cloud computing model

3.1. Cloud computing characteristics

Rapid Elasticity, *Measured Service*, *Resource Pooling*, *Broad Network Access* and *On-Demand Self Service* are considered as essential characteristics by many researchers [13, 14]. But other researchers [8, 9, 15] insist that *multi-tenancy* is an important element of cloud computing. They are described briefly below:

- *Rapid Elasticity* – defines that resources can be dynamically increased or decreased according to the need.
- *Measured Service* – tells how much resources are used by a customer and then bill the customer accordingly. It can also be called as pay-per-use or metered service.
- *Resource Pooling* – tells that resources can be pooled centrally and those resources will be consumed by multi-tenants. The resources include physical resources such as storage, processing, memory, network and virtual resources like virtual machines. These resources can be dynamically allocated and reallocated according to CSC demands.
- *Broad Network Access* – tells that CSC can access the resources from anywhere through internet.

- *On-demand Self Service* – tells that CSC can access the cloud services automatically without human intervention.
- *Multi-tenancy* – is an architecture in which a single instance of a software application serves to multiple customers or tenants. Multi-tenancy applies to all the three service models IaaS, PaaS and SaaS. It has many advantages and also has some challenges. The advantages are: cost savings on scaling IT resources and software licensing, etc. Security, capacity optimization and service delivery and high availability are the main challenges of multi-tenancy [16].

3.2. Cloud computing service delivery models

Table 1 [17] list all the services provided by the CSP to CSC. There are nine services a CSP can provide to CSC. They are: Applications, Data, Runtime, Middleware, Operating System, Virtualization, Servers, Storage and Networking which are also the basic components in traditional computing [18, 19, 8]. Later in this paper, the different security issues arising at each service level are described in detail. The SaaS model provides all the nine services to CSC. So the SaaS model can be called as a complete cloud. They are described briefly in Table 1.

Table 1. Services provided by CSP

Services	IaaS	PaaS	SaaS
Application	CSC	CSC	CSP
Data	CSC	CSC	CSP
Runtime	CSC	CSP	CSP
Middleware	CSC	CSP	CSP
Operating System	CSC	CSP	CSP
Virtualization	CSP	CSP	CSP
Server	CSP	CSP	CSP
Storage	CSP	CSP	CSP
Networking	CSP	CSP	CSP

Cloud security issues vary from one service model to another and also from one deployment model to another. So, it is important to understand the different services provided by these three models before we go into the security issues.

3.2.1. Infrastructure-as-a-Service (IaaS)

Fig. 3 depicts the services (shown with the red soft box and arrow) provided by IaaS to CSC [1]. In IaaS, CSP provides the computing resources like processor, storage, network to CSC. Other services become CSC's responsibility. These computing resources could be physical or virtual. CSP allows CSC to install and use any operating system and applications and they bill only the resources used by the CSC. Here, security should be a shared effort by CSP and CSC like the shared responsibility models adapted by AWS and Microsoft Azure. Storage, Compute, Backup and Recovery, Services Management are a couple of examples of IaaS applications. Amazon's Elastic Compute Cloud (EC2), Amazon's Simple Storage Solution (S3), Rackspace cloud and GoGrid are few examples of IaaS.

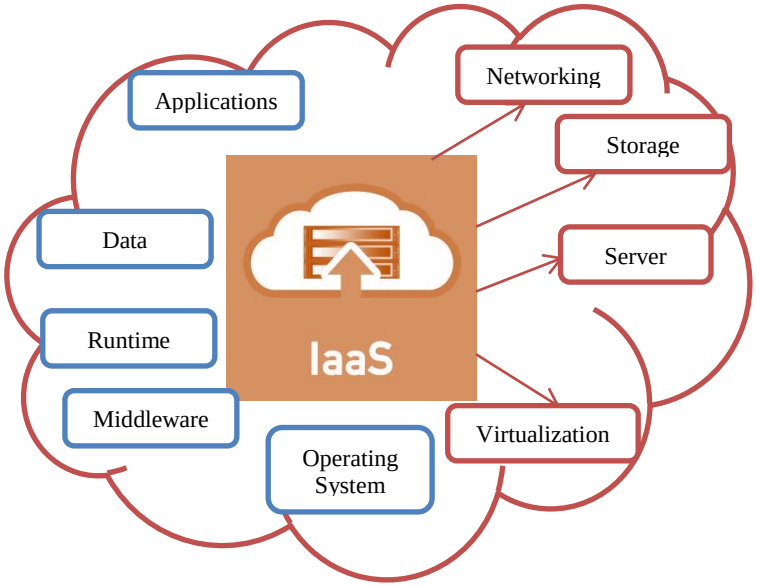

Fig. 3. IaaS model with services provided

3.2.2. Platform-as-a-Service (PaaS)

PaaS is the middle layer in the cloud computing model where PaaS can be built on top of IaaS. In PaaS, CSP provides customers with all the IaaS services plus the operating system, middleware and runtime services. Fig. 4 shows the different services (shown with the green soft box and arrow) provided by PaaS. Other services like data and applications become CSC's responsibility.

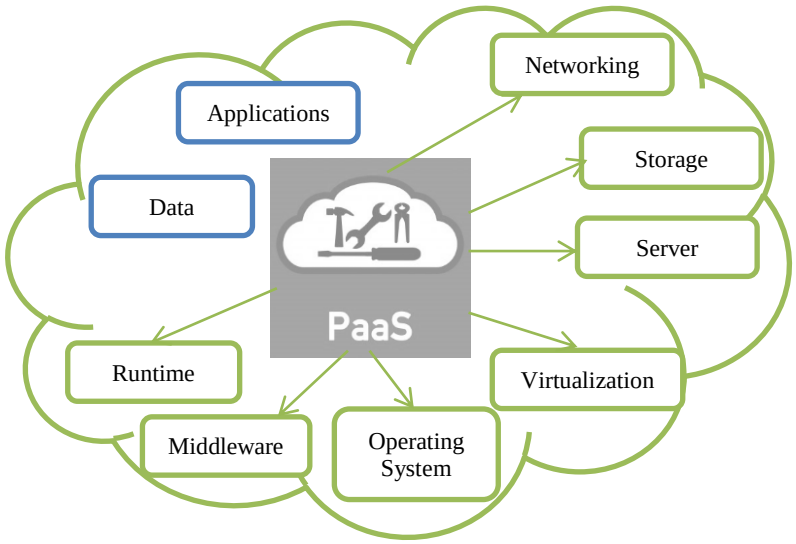

Fig. 4. PaaS model with services provided

CSP can bill the CSC based on the number of customers, type of resources used and the duration of the platform used. Business intelligence, Integration and Development and testing are a couple of PaaS applications. Like IaaS, the security is a shared responsibility by both CSP and CSP. Google App Engine, Microsoft Azure platform, Salesforce's Force.com and Amazon Web Services (AWS) are examples of PaaS.

3.2.3. Software-as-a-Service (SaaS)

In this model, a CSC can access the software through internet uploaded by the CSP. SaaS is the final layer in the cloud computing model and it can be built on top of IaaS and PaaS. CSC can make use of the CSP's infrastructure, platforms and all other functionalities on a pay-per-use approach as shown in Table 1. Here, CSPs are responsible for everything, including the security. Fig. 5 depicts the different services (shown with the orange soft box and arrow) provided by SaaS to the CSC. SaaS provides all the services to the CSC. ERP, CRM, Email are a couple of SaaS applications. These applications are deployed as hosted services by CSP and can be accessed by CSC through internet. The CSC can be an organization or a government where their staff are provided with software applications like email, etc., or individual users who want to use those applications. Examples are Google Apps and Microsoft Office 365 [20]. Here, the major security responsibility lies with the CSP because most of the services are provided by them and the CSC has very little control over the security.

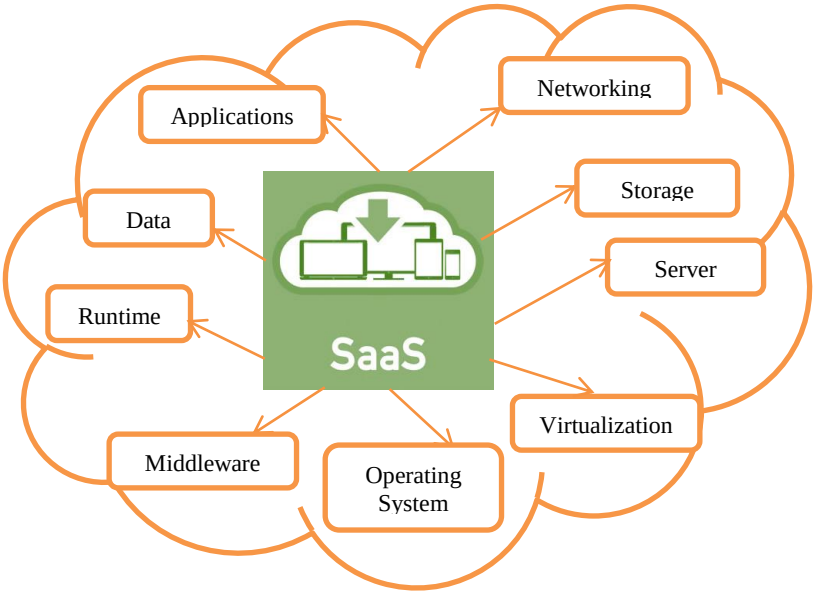

Fig. 5. SaaS model with services provided

3.3. Cloud computing deployment models

There are four basic deployment models in cloud computing. They are described briefly below:

- Public cloud – In this model, CSC share the CSP's infrastructures through the internet along with other customers. This model is open to all and therefore has more risks than the other models.
- Private cloud – In this model, CSC uses infrastructures exclusively located with an organization or premises and they also manage the resources. This model is not open to all and therefore has less risk compared to other models.
- Community cloud – In this model, a private cloud is shared by many customers with common policies and procedures. This cloud gets benefits from both private and public clouds. It gets the security benefits from private cloud and economic benefits of public cloud.
- Hybrid cloud – This model is a combination of public, private and community clouds. This gets the benefit from all the three cloud models.

4. Cloud computing security

Even though cloud computing has a bunch of benefits; customers are still sceptical about migrating to cloud computing, mainly due to data security and privacy [20]. In cloud computing, technology, physical and logical control, services and infrastructure, standards, policies and procedures should work together to protect data. Here, security is governed by both CSP and CSC. In general, CSP is responsible for the cloud infrastructure and CSC is responsible for anything they put in to the cloud, like data. AWS called it as a Shared Security Responsible Model [21]. The following sub-section provides the basics of data security.

4.1. Data security fundamentals

Confidentiality, Integrity and Availability (CIA triad) are the three important properties of a data. Authentication, authorization and nonrepudiation are another three important properties associated with people who use the data [22]. *Confidentiality* is related to data privacy, where the data is not disclosed to unauthorized parties on any occasion [20]. *Integrity* of data refers to the confidence that the data stored in the cloud are not tampered by unauthorized parties. It is also applicable when the data are transit. *Availability* of data refers to assuring that whenever the CSC needs data, the data should be available to them immediately and can't be denied. These three basic data security properties are tested, highly in the pubic cloud deployment model. Authentication is the proof for a person to access his or her own data. Authorization is the process of finding out whether a person has the right to perform an activity on data. Nonrepudiation is the assurance that an authenticated user cannot deny after performing a job.

4.2. Data stages

The data from CSC to CSP and vice versa flow through various stages. The important stages are four [6]:

4.2.1. Data-in-transit

In this stage, the data is in the process of transmitting from CSC (computing devices) to CSP (cloud infrastructure) or vice versa. Here, data can be intercepted and in turn can affect confidentiality. Encryption is one of the methods used to protect the data while in transit.

4.2.2. Data-at-rest

In this stage, data is stored at CSP's infrastructure and data security and privacy becomes CSP's responsibility. CSP need to insure CIA of the data.

4.2.3. Data-in-use

At this stage, data is accessed, processed and converted into information. The main problem at this stage is data can be corrupted while processing [20]. Later in this paper, we discuss methods to protect data while it is being used.

4.2.4. Data-after-delete

Another important and neglected issue with data is, data-after-delete (data remanence) [6]. Data remanence is the residual physical representation of data that has been erased [23]. After storage media is cleaned, there may be some physical characteristics that allow data to be reconstructed [23, 24]. It is the responsibility of the CSP that the data is safely deleted at the end of the data life cycle. Apart from the above four stages of data, tracing the data path (data lineage) is important for auditing in cloud computing especially in the public cloud [6].

4.3. Security issues in the nine stacks of services of cloud computing

Some of the security threats and vulnerabilities could be overlapping between more than two stacks. For example, Denial-of-Service (DoS) attack can overlap between application and network stacks. This section describes security issues in all the nine stacks of services provided by cloud computing and it provides solutions to avoid or mitigate security issues.

4.3.1. Application and runtime security issues

There are a number of applications and runtime level security issues in cloud computing. Cloud computing applications are normally delivered through internet using web browsers. Cloud computing can host and run any type of applications from simple word processing software to any complex customized software with the appropriate cloud computing middleware. Any flaws in the web applications may reflect as vulnerabilities in the cloud computing service model especially in the SaaS model. Application security ensures that an application software is developed under secure Software Development Life Cycle (SDLC), deployed, managed and until

decommissioned to protect it from threats and vulnerabilities in the cloud environment especially in the public cloud [15]. Application security is a challenge across all the three service models (IaaS, PaaS and SaaS) from attackers even if there is no vulnerability existing in the application. Application security in the IaaS and PaaS models are more challenging than the SaaS model because the application's security responsibility comes under the jurisdiction of CSC. The following are some of the important application and runtime stack security threats.

4.3.1.1. Command injection attacks

According to Open Web Application Security Project (OWASP), injection attacks are the top most application security threat in the web application and also in cloud computing [25]. There are a number of command injection attacks that can happen at the application stack. They are SQL injection, Lightweight Directory Access Protocol (LDAP) injection and eXtensible Markup Language (XML) injection attacks. Refer [26] for a detail study on command injection attacks.

Solution to avoid injection attacks [25]:

- Use safe Application Programming Interface (API) which avoids the use of the interpreter or provides a parameterized interface.
- If parameterized API is not available, then escape special characters using specific escape syntax for that interpreter.
- Apply strict input validation where ever is possible.

4.3.1.2. Cross-Site Scripting (XSS) attack

This XSS attack happens whenever an application takes an untrusted data and sends it to a web browser without a proper validation. This allows the attacker to execute scripts in the victim's browser which can hijack user sessions, deface websites or redirect the user to malicious sites [25]. There are two types of XSS attack namely, *stored attack* and *reflected attack*. More information on XSS attacks can be found on [26].

4.3.1.3. Cross-site request forgery (XSRF) attack

In this XSRF, an attacker takes advantage of the trust established between an authorized user of a website and the website itself. More information on XSRF attacks can be found on [26].

Solution to avoid XSS and XSRF attacks [26]:

- Ensure that Hyper Text Markup Language (HTML) don't format in form fields.
- Apply input validation on all fields, strings, variables and cookies.
- Don't store unnecessary data in cookies and if it is stored, limit the expiry time for cookies.
- Encrypt all data communications between clients and servers.
- Don't check the **Remember Me** option when authenticating on websites.

4.3.1.4. Using components with known vulnerabilities

Components such as libraries, frameworks and other software modules, run with the same privileges as application are generally classified as components with known vulnerabilities [25]. If a vulnerable component is exploited, this can lead to serious data loss or server take over. Applications and APIs using components with known vulnerabilities may pull down the application's defence mechanism and enable to various attacks and impacts.

Solutions to avoid components with known vulnerabilities [25]:

- Continuously update the versions of both server-side and client-side components and their dependencies using tools.
- Continuously monitor the sources of vulnerabilities in the components and use software composition analysis tools to automate the process.

4.3.1.5. Under protected APIs

APIs are essentially software interfaces, generally standards based, that cloud providers make it available to their customers for the purpose of managing cloud services. Insecure or under protected APIs can pose a variety of risks related to confidentiality, integrity, availability and accountability. Whatever vulnerabilities exist for applications also applies to APIs.

Solutions to avoid under protected APIs [25]:

- Establish a secure communication between client and the APIs.
- Establish a strong authentication scheme with APIs and secure all credentials, keys and tokens.
- Harden the parser configuration of the data formats against attacks.
- Implement an access control scheme that protects APIs from being improperly invoked, including unauthorized functions and data references.
- Protect against all injection attacks.

4.3.1.6. Cookie poisoning

Cookies are small files which contain information on a user's identity related credentials and are stored on the user's computer. There are many types of cookies created for various purposes. Cookies can be accessed by either from the server or from the client's computer. Here, attackers can access the cookies illegally and can change or modify the cookies to impersonate like an authorized user [6]. Once the attacker gets the user's credentials, then he can access the entire user's data and can do anything with the data.

Solution to avoid cookie poisoning [6]:

- Perform regular cookie clean-up.
- Implement encryption scheme for the cookie data.

4.3.1.7. Hidden field manipulation

It is a part of the data manipulation attack [27]. There are certain fields hidden in web sites and they contain page related information and are generally used by the developers. These hidden fields are highly prone to attack by hackers and these fields

can be easily modified and posted back on the web. This leads to severe security violations [6].

Solution to avoid hidden field manipulation [27]:

- Validate and verify the value of the hidden fields whenever there is a change in those fields before the page is submitted.

4.3.1.8. Backdoor and debug option

The Backdoor is a hidden entrance to a computer system that can be used to bypass security policies [28]. Application developers generally enable the debug option while publishing a website so that they can make developmental changes in the code and get them implemented in the website [6]. Sometimes these debugging options are left enabled and no one notices. Attackers can make use of this backdoor entry and enter into the website or application and can make any changes.

Solution to avoid backdoor and debug option:

- Enable debug option with strong authentication.
- Once the website or application is running, disable the debug option.

4.3.2. Security threats in the data stack

In the traditional enterprise computing, the data is stored within the enterprise computing and it is subject to its physical, logical and personnel security and proper access control polices [4]. But in the cloud computing, the data is stored outside the customer's place, i.e., in the CSP side. Consequently, the cloud computing must employ additional security measures apart from the traditional security checks to ensure that data is safe and there are no data breaches due to security vulnerabilities in the cloud computing. There are a number of data related security issues in cloud computing, especially in SaaS model because the CSC has no control over the data and it is stored at the CSP's server. There are six stages in the data life cycle [15] as shown in Fig. 6. Once data is created, the data security is very important until the data is destroyed. The following data security issues are more prevalent in cloud.

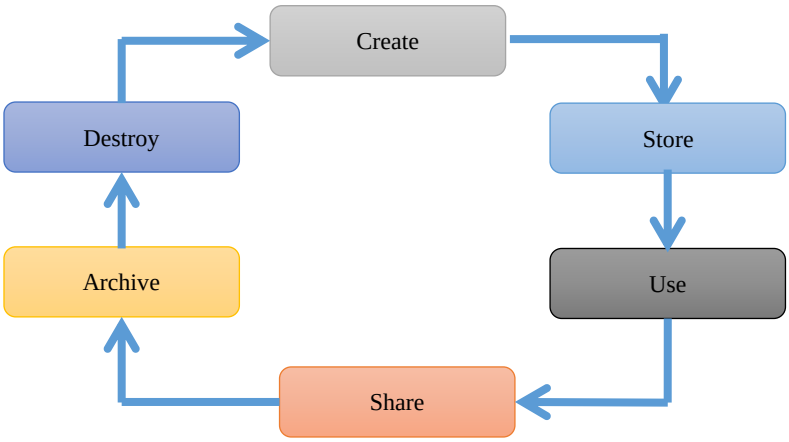

Fig. 6. Data life cycle

4.3.2.1. Security issues related to CIA triad

In this section, all security issues related to the CIA are discussed. When data is read or copied by someone who is not authorized to do so, this situation is called as loss of confidentiality [22]. When data is modified in an unpredicted way, this situation is called as loss of integrity [22]. When data is lost or become inaccessible, this situation is called "loss of availability" [22]. All these three losses can make a big impact in cloud computing because data is the core component for any business process. Data integrity is the assurance that digital information is not corrupted and only be accessed by the authorized users. So, integrity involves maintaining the accuracy, consistency and trustworthiness of data over its entire life cycle [29]. CIA triad can be easily maintained in a standalone computing system and it can be maintained with proper security measures in enterprise computing but in cloud computing, it requires additional efforts to protect data due to the distributed nature of the infrastructure and multi-tenant architecture of the cloud computing. The following procedures can be followed in the CIA triad at each stage of its life cycle to secure the data:

- After the data are created, classify the data and identify the sensitive data.
- Create policies on what activities are allowed for different types of data.
- Store the data with proper physical and logical security protection with proper backup and recovery plan.
- Create proper access methods for different types of data.
- Identify which type of data can be shared, whom it can be shared with and define data sharing policies. In cloud computing, many such policies are collectively called as Service Level Agreements (SLA).
- Also make a corrective action plan in case something happens to the data, like data corruption or hacking due to flaws in the network or communication devices while in transit.
- Create polices for data archive and destroy data.

Integrity should be checked at data as well as computation level [8]. To maintain the integrity in computation, only the authorized applications are allowed to access the data and use it for computation. Do not allow users to deviate from normal computing. An effective Identity and Access Management (IAM) can avoid loss of confidentiality and integrity. Loss of data and data inaccessibility can attribute to loss of availability. Cloud computing employs techniques like scalability and high availability at the architecture level to address the data loss. The following are some methods and procedures to improve data security related to the CIA triad at different stages of data life cycle.

Solutions to improve data security related to CIA triad:

- Always use data encryption when the data is stored (data-at-rest) and also when the data is shared (data-in-transit). Use strong encryption algorithms like Advanced Encryption Standard (AES) and Rivest, Shamir Adleman (RSA) algorithms. In [8, 30], different types of encryption methods are described. Amazon S3 uses one of the strongest encryption algorithms, 256-bit AES [21].
- Encryption methods cannot protect data against configuration errors and software bugs even though they can provide confidentiality against attacks from a

cloud provider [8]. Hash methods can be used to find out accidental and intentional data changes. But they consume more bandwidth and time consuming.

- Researchers [8, 31, 32] insist to include Third Party Auditing (TPA) for data integrity because they are specialized in that.
- Ateniese et al. proposed Provable Data Possession (PDP) scheme to investigate statistically the correctness of the data without retrieving the data from the cloud storage [33]. Ateniese et al. [34, 35], Wang et al. [36] and Sookhak et al. [37] overcome the limitations of PDP.
- Always store the encryption keys and the encrypted data separately [38].
- Implement proper Identity and Access Management (IAM) techniques for users to access data [17].
- Data availability issues can be addressed by using data duplication, redundancy, backups and resilient systems [38].
- Always include an alternative strategy, in case the service fails with the CSP [17].
- Data dispersion (segmentation) technique can be used to address the availability issue, if other methods are not effective. Here the data is stored as fragments in many clouds and the data can be reconstructed when it is required to use fragmentation techniques [15].

4.3.2.2. Security issues related to authentication, authorization and accounting

Authentication, Authorization and Accounting (AAA) is the process of identifying a user, enforcing policies, confirmation on user's identity to connect, to access or use the cloud resources and monitor them. A simple authentication scheme is, user enters a login name and password and they are verified against the credentials stored in the computer. If the credentials are matched, the user is allowed to enter into the system. In certain scenario, it is called as Authentication and Access Control (AAC). Authentication identifies a user and access control authorizes what are the resources the user can access in the cloud. If it is a standalone computer, the credentials are stored locally in the computer itself. In enterprise computing, the credentials are stored in the server in the form of Active Directory (AD) or LDAP. In a private cloud, the authentication is done same as the enterprise computing via a virtual private network. In public cloud, internet is used by customers to connect to CSP, applications from different users can co-exist with the same CSP (resource pooling) and CSC can access the applications from anywhere through any devices. So, the authentication in public cloud is more subject to vulnerability than private cloud [15]. Password based authentication does not provide effective security measures in public cloud. Passwords can be easily cracked using many methods, like a brute force attack, dictionary attack, phishing or social engineering attack. So, CSP should include highly secured authentication methods in public cloud. In cloud computing, customers connect to cloud services through APIs and these API's are designed to accept tokens rather than passwords [15].

In cloud computing, along with users, machines also need to be authenticated because certain machines are used in automated actions like online backup, patching and updating systems and remote monitoring systems [39]. Since the cloud

applications are accessed through various devices, there should be a strong authentication methods like RSA token, OTP over the phone, smartcard/PKI, biometrics, etc., for the original identity confirmation and determine the type of credentials [15]. This will enable identifiers and attributes with a strong level of authentication to be passed on to the cloud application and the risk decisions can be made for access management. According to Cloud Security Alliance (CSA) [15], there are different types of authorization models, namely Role-based, Rule-based, Attribute-based, Claims-based and Authorization-based access control. If attackers can hack user credentials, then confidentiality, integrity and availability of data will be affected. Most of the CSP includes some form AAC or Identity, Entitlement and Access management (IdEA) [15]. In some cases, authentication and authorization are delegated to CSC's user management system through federation standard (authenticate users using corporate credentials in public cloud) [15]. There are a number of methods and standards available to avoid security issues related to AAA. The following are some of the important methods and standards:

Solutions to avoid security issues related to AAA:

- Employ single-sign-on policy where ever possible [17].
- Implement multi-factor authentication, which enables both identity and access management which is used in Amazon Web Services (AWS) [40].
- Biometric authentication has the potential to be the most secure form of single-sign-on authentication [40].
- Implement RSA cryptosystem which can accept different authentication models like two-factor authentication, knowledge based authentication and adaptive authentication, which are very effective for data protection in cloud computing [41].
- Employ Intrusion Detection System (IDS), firewalls as well as segregation of obligations on the different network and cloud layers to enable proper access control in cloud computing for better data protection [41].
- Employ any third party identity management solutions such as Microsoft Azure Active Directory, Okta identity management, McAfee cloud identity manager, etc., [17]. Recently, in a corporate environment, Identity-Management-as-a-Service (IMaaS) solutions are getting more popular [42].
- Cloud applications should perform risk-based authentication on the transactions apart from performing authentication during the initial connection. This role-based authentication is based on device identifier, geo-location, ISP, heuristics information, etc., [15]
- It is recommended that cloud applications should use open standards wherever applicable, such as Security Assertion Markup Language (SAML), an XML-based OASIS (Organization for the Advancement of Structured Information Standards) open standard for exchanging authentication and authorization data between security domains and Open Authorization (OAuth), an open standard for authorization, allowing users to share their private resources using tokens rather than credentials [15].

4.3.2.3. Broken authentication and session management

This security threat is part of the AAA. This type of threats occurs due to incorrect implementation of authentication and session management in the application domain. Weak account management functions, user credentials are not properly protected, session IDs are exposed in the URL, etc., are examples of this type of threats. Attackers generally target the privileged accounts, take advantage of the situation and can compromise passwords, keys, session tokens or to exploit other implementation flaws to assume the privileged account identities [25].

Solutions to avoid broken authentication and session management:

- Implement a single set of strong authentication and session management controls.
- Avoid XSS flaws which can be used to steal session IDs.

4.3.2.4. Broken access control

This threat occurs when there is a lack of enforcement on restriction of what authenticated users are allowed to do. Using this loophole, attackers can access another user's accounts, view sensitive files, modify another user's data, change access rights, etc., [25].

Solutions to avoid broken access control:

The following three methods [25] can be used to prevent access control flaws which require selecting an approach for protecting each function and each type of data.

- Check Access – Every use of a direct reference from an untrusted source must be checked for access control to guarantee that the user is authorized for the requested resource.
- Use per user or session indirect object references – This method uses a coding pattern which prevents the attackers from directly targeting unauthorized resources.
- Automated verification – Implement automation to verify proper authentication deployment.

4.3.2.5. Sensitive data exposure

This flaw occurs when web applications and APIs do not properly protect sensitive data [25] such as financial, healthcare and Personally Identifiable Information (PII). Here, attackers can steal or modify such weakly protected data and can indulge in credit card fraud, identity theft or other crimes. The data include data at rest, in transit and in use.

Solution to avoid sensitive data exposure [25]:

- Encrypt all sensitive data at rest, data in transit using strong encryption algorithms.
- Don't store sensitive data unnecessarily.
- Use strong standard encryption algorithms and strong keys. Also, practice good key management system.
- Store passwords with algorithms specifically designed for password protection.

- Disable autocomplete on forms requesting sensitive data and disable caching for pages that contain sensitive data.

4.3.2.6. Other data related security issues

There are other minor data related security issues which can occur through data location, multi-tenancy and backup in cloud computing. In cloud computing, data is stored in diverse geographic location and they are bound to different legal jurisdictions [15]. If the data location is not safe physically and logically then there is always a threat to the CSC's data. In this type of situation, data is vulnerable to external hackers as well as malicious insiders. In cloud computing with multi-tenant architecture, a user can intrude into another user's data location because multiple users can store their data in the same location using physical or virtual storage concept [4]. A detail on this multi-tenant security issues are covered later in the virtualization.

All data, especially the sensitive data should be regularly backed up and tested in cloud computing for proper data recovery in case of disasters. It is recommended to use strong encryption techniques to protect backup data if the data is sensitive [4]. In cloud computing, depending on the cost, business and data, two types of back up can be done, namely, on-site backup and cloud-based backup. On-site backup is cheaper, easier to set up and runs faster. Here, the backup and the production environments are the same and if any natural disasters happen then all the data including the backup are lost. In cloud-based backup, CSC's data is stored off-site and if any natural disasters happen on the CSC's site then the data is still available with the cloud. Cloud-based backup is expensive, slower for large backups [43].

Solutions to avoid other data related security issues:

- It is important that the CSC should know the logical and the physical location of the data, if not at least which state and country the data belongs to. This is due to all the potential regulatory, contractual and other jurisdictional issues [15].
- There should be separate location and jurisdictional polices to govern the data location [15].
- Implement intelligent data segregation techniques to segregate the data from different users.
- Data leakage can be avoided by employing strong encryption techniques for the backup data.

4.3.3. Security threats in the middleware stack

According to Techopedia [44], a middleware is a software platform that sits between an application/device and another application/device. It makes the connection between any two clients, servers, databases and applications. In cloud computing, middleware lies between operating system and application stacks and provides a number of functionalities to the user. Middleware services are handled by CSP in PaaS and SaaS (refer Fig. 7 and Fig. 8) and in IaaS, it is handled by CSC (refer Fig. 6). CSP is responsible for any security issues related to middleware in PaaS and SaaS and CSC is responsible in IaaS. The following are some of the important functions of middleware in cloud computing [44]:

- Helps the user to create business application.
- It facilitates concurrency.
- It helps to perform transactions.
- It facilitates threading and messaging.
- It provides a service component architecture framework for creating Service-Oriented Architecture (SOA) applications.

Web servers, application servers and databases are examples of cloud middleware. Middleware programs generally provide communication services and serve the purpose of a messenger so that different applications can send and receive messages within cloud computing. In cloud computing, different applications situated at different physical locations and cloud middleware are used to interface all these applications to perform their job.

Since middleware interacts between any applications/devices, they are bound to security issues which can occur due to applications, devices and also at the interface stage. Since most of the data transmission and operation occurs through middleware, the security is a vital issue in middleware [45]. If middleware is running sensitive applications or the middleware is on a platform where sensitive information is processed or stored then the middleware is under high risk. In this scenario, middleware can create a secondary path through which applications and data can be compromised [46]. To address the security issues in middleware, firstly the developers should establish an Application Lifecycle Management (ALM) practices to impose middleware security; secondly the developers should optimize network security and lastly add incremental security to middleware tools and interfaces [46].

Solutions to avoid security issues related to middleware [46]:

- To reduce the security risks in the middleware, separate sensitive applications from open applications running on the same platform.
- Enforce strict authentication process for middleware components and application components of the ALM process before they are being integrated into the middleware platform or application. This is the first step to address security in the middleware stack.
- The next step to address security in the middleware is network security. Use application-specific overlay networks which are usually built in encrypted tunnels, can provide both access protection and interception security and even reduce the risk that information would be compromised ‘in flight’ between component to assure nonrepudiation.
- The third step to address the middleware security is middleware itself. In that, efforts should be taken care to prevent unauthorized introduction or interception of messages in the workflow / message bus management which is the most vulnerable part of middleware. Include Web Services (WS) framework, especially WS-Security between components and in particular to secure connections to service/message buses. Middleware architectures (Microsoft’s .NET, IBM’s Websphere and Oracle Fusion) are available commercially and they can be used because they provide security tools which are integrated and available via standard development tools and practices.

4.3.4. Security issues in the operating system stack

Operating System (OS) services are provided by CSP in PaaS and SaaS (refer Fig. 7 and 8) and it is provided by CSC in IaaS (refer Fig. 6). So, CSP is responsible for providing defence against any OS's related security issues in PaaS and SaaS. CSC is responsible for IaaS security. OS is one of the important services to support the underlying complexity of well managed cloud computing resources [47]. Apart from providing basic OS services, cloud OS should provide the essential cloud characteristics like scalability, interoperability and portability. In addition, cloud OS provides a desired level of security and ensures Quality-of-Service (QoS). The following four elements are important for creating an operationally sophisticated cloud computing environment [47]:

- Abstract and well defined interfaces that conceal implementation details.
- Support for security at the core.
- Capability to manage virtualized workloads and.
- Workload optimization to offer superior performance and QoS.

Every OS comes with some form of security vulnerabilities and cloud computing has multiple operating systems of heterogeneous type and the vulnerability complexity also increases in the cloud environment. When security is implemented as a framework within the OS, it improves the overall security of both virtualized and non-virtualized environments and the same OS services can be applied to on premise, private cloud or public cloud environments [48]. Operating systems are susceptible to a number of internal and external attacks due to un-patched vulnerabilities, disgruntled employees or misconfigured server settings [49].

Solutions to avoid vulnerabilities in the OS stack [49]:

The main purpose of doing hardening in the operating system is to protect organizations against security breaches and malicious attacks. It also improves the overall efficiency of the OS environment by verifying user permissions, patching vulnerabilities, installation of necessary software updates and deactivating unnecessary programs. The following are some basic hardening techniques that can be used for the OS stack:

- Non-essential services – Stop all non-essential services and configure only the services which are required for the essential operation of the OS.
- Fixes and Patches – OS should be updated with the latest security updates and it should be an on-going process.
- Password Management – OS should support a good password management policy like strong password, regular change of passwords, number of failed login attempts, etc.
- User accounts – When the employees leave an organization their accounts should be deleted or disabled. Also, unused user accounts should be disabled or deleted.
- Directory and File Protection – Enforce policies for accessing directories and files through file permissions and access control lists.
- File System Encryption – Some of the OS file systems support encryption of files and folders. If the data is sensitive then encrypt the folder as well as the files.

- Enable Logging – OS should be configured to ensure logging of all errors, activities and warnings.
- File Sharing – Unnecessary file sharing should be disabled.
- Application Hardening – All the applications installed in the OS should be hardened to protect against any vulnerabilities.
- Hardening the Network and their related operations – All network devices should be updated regularly with the latest fixes and patches. Access to all the network devices like wireless access point should be protected by strong passwords. All unnecessary network services and protocols in the host OS should be disabled. Block all the ports that are not needed using a firewall.

4.3.5. Security vulnerabilities in the virtualization stack

Virtualization is provided by the CSP in all the three delivery models, namely IaaS, PaaS and SaaS. So, CSP is responsible for providing defence against vulnerabilities related to virtualization. Virtualization is the process of creating a virtual version of something such as a server, storage device, network, application or even an OS where the framework divides the resource into one or more execution environments. In other words, virtualization is a technique, which allows sharing a single physical instance of a resource or an application among multiple customers or organizations. Virtualization is not a new concept. It was actually started with mainframe computing decades ago and continues in the personal computing (dividing the physical hard disk into logical partitions). As virtualization becomes more popular with the introduction of cloud computing. Network virtualization, Storage virtualization, Server virtualization, Data virtualization, Desktop virtualization and Application virtualization are the six areas in I.T. where virtualization can be applied [50].

There are a number of research papers on virtualization and their security issues in cloud computing [3, 4, 6, 7, 8, 23, 50]. The general benefits of virtualization are multi-tenancy, better server utilization and data centre consolidation. Virtualization benefits enterprises to reduce capital expenditure on server hardware and improves operational efficiency [15]. Even though virtualization brings many benefits to cloud computing, they also bring some security issues related to guest operating system, hypervisor (software, firmware or hardware that creates, runs and manage virtual machines, it is also called as a virtual machine monitor) and Virtual Machines (VM). The following are some security issues related to virtualization.

- VM Side-channel attacks – This attack occurs when the attacker is in another virtual machine of the same physical hardware with the victim and both sharing the same processor and cache. When the attacker alternates with the victim's VM execution, the attacker can get some information about the victim's behaviour and in turn can get some sensitive information about the victim or the CSP itself [8, 51]. Timing side-channel attack [52] is a type of side-channel attack where the attacker tries to get information through the time needed by various computations.
- VM Image sharing – In VM, there is a shared image repository which is used to share VM images of users. Through this shared image repository, a malicious user can inject code into VM to create problems [7, 8, 53].

- VM Shared resources – VMs on the same server can share CPU, memory, I/O and others. Because of these shared resources, a malicious VM can gather some information from other VMs through shared memory and other shared resources [7].
- VM Rollback – VMs are able to roll back to their previous states if an error happens. This can re-expose VMs to security vulnerabilities that were patched or re-enable previously disabled accounts [8, 54].
- VM Escape – In VM, a malicious user or a VM can escape from the VMM monitoring and can interfere with hypervisor or other guests without being noticed [8, 53, and 55].
- VM Migration – Due to fault tolerance, load balancing and maintenance, a VM can migrate from one physical machine to another [7, 8, and 56]. The data and the code of the VM are exposed when transferring through a network between two physical hardware locations and are vulnerable to attackers [57]. Also, it is possible for an attacker to transfer a VM to a vulnerable server and then can compromise it [8].
- Hypervisor Issues – The Hypervisor or VMM is responsible for managing and isolating VMs from each other. It is responsible for proving, managing and assigning resources because it is the interface between physical hardware and the VMs. A malicious attacker can compromise a hypervisor in order to get full control of it [8].

Solutions to avoid security issues related to virtualization:

- VM Guest hardening – Employ hypervisor-based APIs to harden and protect VM instance, including firewalls, Host Intrusion Prevention System (HIPS), web application protection, antivirus, file integrity monitoring and log monitoring [15].
- Hypervisor Security – The hypervisor should be hardened and locked down using best practices. The server hosting the hypervisor should be highly secured in all aspects (authentication, authorization, encryption, secured network, Host Intrusion Detection System (HIDS), physical security etc.) because hypervisor is the controller for everything in the virtualization host [15, 23].
- Improving VM security – Install a full set of security tools in each individual VM to add an extra layer of security [15]. Employ policy-based management and virtualization management framework [15]. Use network-based security and virtual patching that can inspect the traffic for known attacks before it can get to a newly started VM. Also enforce Network Access Control (NAC) features to isolate a stale VM's until their rules and pattern files are updated and scan has been done [15]. Encrypt VM images at all times to save VM images at running and dormant [15]. When a VM is moved from one physical server to another, delete all the data in the old server.

4.3.6. Security issues related to server stack

Security in the sever stack is CSP's responsibility because the server stack is provided by CSP. A cloud server is a logical or physical server that is built, hosted and delivered through a cloud computing platform over the internet. A cloud server is considered as logical when it is delivered through server virtualization, i.e. the physical server is logically distributed into two or more logical servers; each one can

have a separate OS, user interface and applications by sharing the underlying physical hardware from the server. A physical server is generally a dedicated cloud server and is also accessed through the internet [58]. Security misconfiguration and insufficient attack protection are some security issues that can be related to the server stack [25]. The following are the characteristics/functionalities of a cloud server [59].

- Computing infrastructure can be physical, virtual or a mix of the two and can be scaled up or down accordingly (scalability and flexibility).
- Cloud server has the capabilities of an on-premises server.
- It enables high intensive workloads for users and store huge data.
- All the services are automated and can be accessed on demand through APIs.
- More reliable than traditional servers.
- Supports pay-as-per use approach.

Solutions to avoid security issues related to server:

When all the eight stacks in the cloud service are secured, the cloud server is also secured. All those solutions provided for the security issues in the Application, Data, Runtime, Middleware, Operating System, Virtualization, Storage and Network stack applies to cloud server also because server is the one which manages them. The following are some of the solutions that can be used by a cloud server to mitigate security vulnerabilities.

- Remote Access – Encourage cloud server administrators to login locally. If remote login is required, then make sure a secured remote connection is established by tunnelling and encryption protocols. Enforce security tokens and single sign-on for remote login. Remote access should be restricted to a specific number of IPs and to specific accounts only [60].
- Physical Security – Physical access to the server and the data centre should be restricted and only authorized people should be allowed inside. All physical access to data centre should be logged and audited regularly [21]. Data centre should be fitted with video surveillance, IDS and other electronics systems. They should be installed with fire protection and continuous power systems. Establish a proper climate and temperature monitoring systems to avoid overheating and reduces the possibility of service outages [21].
- Standard Security Procedures - Include the standard security procedures like firewalls, anti-virus software, monitoring and HIPS [59].
- Service Auditing – Include service auditing, which is a process of finding out what services are running on the servers, which ports are used for communication and what protocols are used. This information helps to configure the firewalls settings [61].

4.3.7. Security issues related to storage stack

Security in the storage stack is CSP's responsibility because the storage stack is provided by them. Amazon, Microsoft and Google are the three major cloud providers in the storage-as-a-service solutions. Most of the security issues discussed in Sections 4.4.1 and 4.4.2 (Application and Data) are applicable to storage stacking also.

Solutions to avoid security issues related to storage:

- Enforce all the security measures related to data (especially data-at-rest) like AAC, encryption, etc.
- Establish physical security for the storage devices or the data centres. Employ policies for data duplication, data-after-delete, etc.

4.3.8. Security issues related to network stack

The Network is one of the important stacks in cloud computing because the users are connected to the cloud through the network stack and the data are also transferred using this stack. One of the important success of cloud computing depends on how secured it's underlying network infrastructure. According to Arup Chakravarty [62], networks are no longer the traditional packet switching platforms, it is the heart and soul of the intelligence which integrates with other smart applications to differentiate the multitude of services (voice, video and data) that can be enabled over a medium. CSP provides this network stack as part of the infrastructure and they are also responsible for any network related security issues. Cloud networking adds new security challenges to the cloud computing security issues due to additional networking capabilities [63]. Network security issues are one of the biggest challenges in cloud computing [64]. Public cloud suffers more vulnerabilities than private cloud due to the nature of the public cloud (Internet, changing topology, etc.) [6]. Network security is one of the services provided by Security-as-a-Service (SecaaS), a standardised third party security framework for cloud computing which benefits both CSP and CSC [15]. Fig. 7 shows the top network attacks in 2016 [65].

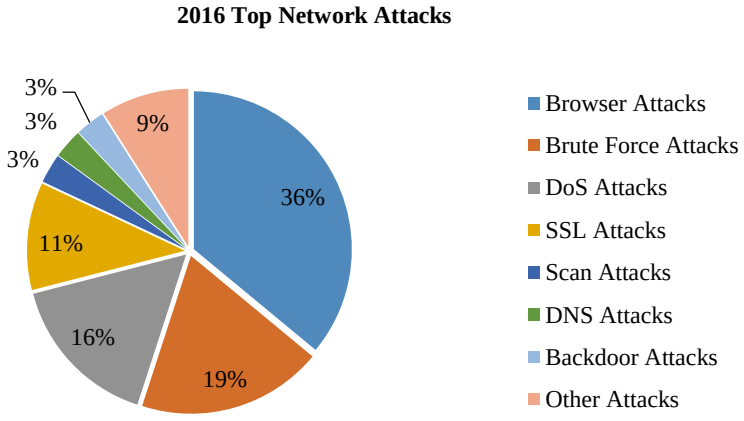

Fig. 7. Top seven network attack types in 2016

Browser Attacks – is the top most network attacks in 2016 (36%). This attack happens through the Internet by tricking the users to download malware that is disguised as a software or application. Hackers can exploit the vulnerabilities in the

OSs or applications and launch the attack [66]. The recent ransomware, 'Wanna Cry' is a Worm or a Trojan which exploited the vulnerabilities in the Microsoft OS and did major havoc in May 2017 [67]. These attacks can be thwarted by regular updates to browser and related applications [66].

Brute Force attacks – is the next top most network attack (19%) which is used by hackers to get the password or pin number by trial and error [66].

Denial-of-Service (DoS) attacks – is the third top most network attack (16%) where the attacker prevents legitimate users from accessing services or information. This attack succeeds when the attacker overloads a server with many superfluous requests than the server can process [66]. Different types of DoS and Distributed Denial-of-Service (DDoS) attacks are given in lesson 2 [26] and also in [68, 69].

Secure Sockets Layer (SSL) attacks – SSL establishes an encrypted link between a browser or an email server and a client. When a website is secured with SSL, the URL begins with https. This attack stands fourth in the network attack (11%) in 2016. In this, the attacker intercepts an encrypted data before it can be encrypted and giving access to the sensitive data to the attackers [66].

Scans (3%) – port scans are pre stage before an attack. It helps the attackers to find out which ports are open in a computer and identify the OS vulnerabilities to launch for future attacks.

Domain Name Server (DNS) attacks (3%) – in this attack, the attacker takes advantage of the vulnerabilities in the DNS. DNS is used to translate the domain name into an IP address. There are a number of DNS attacks like DNS hijacking, DNS spoofing (DNS cache poisoning), DNS hijacking, DNS amplification attack, DNS flood, etc. [70].

Backdoor attacks (3%) – happens when cloud applications allow computers to connect remotely. Some of these attacks are designed to bypass IDS. Port binding, connect-back and connect availability use strategies can be used through backdoor [66].

Other Network attacks (9%) – Other network based attacks like eavesdropping, Man-in-the-Middle attack, spoofing, sniffer attacks, compromised-key attacks, etc. [71].

Solutions to avoid network related security issues:

- Update patches regularly for OS, Browsers, Applications and Software to thwart browser/cyber-attacks.
- Use proper password management policy to mitigate brute force attacks [66].
- Install anti-virus software, firewalls, email filters and NIDS/HIDS [6, 66, 72] to protect from DoS/DDoS attacks. A defence federation is used in [73] to guard against DoS/DDoS attacks.
- To mitigate SSL attacks, use Transport Layer Security (TLS) protocol for communication over a network [74].
- Install IDS and advanced firewalls to detect port scan [26].
- Employ Domain Name System Security Extension (DNSSE) to reduce the effect of DNS threats [6] and install IPS.
- Install firewalls, network patterns and anti-malware to mitigate backdoor attacks.

To have a more secured network in cloud computing, the following services are recommended by CSA [15].

- Support CSC with Authentication and Access Control (AAC).
- Provide CSC with security gateways (Firewalls, Web Application Firewalls (WAF), SOA/API).
- Provide CSC with security products (IDS/IPS and Server Tier Firewall).
- Provide CSC with security monitoring and incident response.
- Provide CSC with DoS protection/mitigation.
- Provide CSC with secure 'base services' like Domain Name System Security Extension (DNSSEC), Network Time Protocol (NTP), OAuth, Simple Network Management Protocol (SNMP), management network segmentation and security.
- Provide CSC with traffic/net flow monitoring.
- Provide CSC integration with Hypervisor layer.

5. Conclusion

Cloud computing is a combination of many existing and emerging technologies like the internet, networking, operating systems, hardware, software, middleware, virtualization, multi-tenancy, etc. When cloud computing integrates all the above technologies, the existing challenges and issues become more challenging and demanding. If the data stored in cloud computing is more sensitive, then the security becomes utmost important. A recent statistics from **statista.com** shows that there is a steady increase in the revenue of public cloud market worldwide. This indicates that people are confident in adapting to cloud computing, especially to the public cloud. Security issues are addressed better with the introduction of SecaaS. According to **rightscale.com** survey, security is no more the top challenges in cloud computing. Lack of resources and expertise become the top challenge in 2016.

There are also new developments in cloud computing like unikernels (minimal, specialized OSs that offers improved security, a smaller footprint and fine-grained optimization for micro services), container orchestration (container is an OS-level virtualization method for deploying and running distributed applications without launching an entire VM for each application), Container-as-a-Service (CaaS), Software-defined networking (a concept to design and manage networks that abstracts applications away from the underlying networks), Software-defined-storage (abstracts the logical storage services and capabilities away from the underlying hardware) and Cloud-of-Things (CoT), (a concept combining cloud computing and Internet-of-Things (IoT) for smart city applications). These latest developments also bring new challenges in the security domain which needs to be addressed. When there is a change in technology, always review the security policies and procedures and update accordingly in order to survive from hackers and attackers.

References

1. Hogan, M., A. Sokol. NIST Cloud Computing Standards Roadmap. Version 2. NIST Cloud Computing Standards Roadmap Working Group. NIST Special Publications 500-291, NIST, Gaithersburg, MD, 2013, pp. 1-113.
2. Columbus, L. Roundup of Cloud Computing Forecasts and Market Estimates 2016. 13 March 2016.
   https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#1c7e6a002187
3. Khalil, I. M., A. Khreishah, M. Azeem. Cloud Computing Security: A Survey. – Computers, Vol. **3**, 2014, pp. 1-35.
4. Subashini, A., V. Kavitha. A Survey on Security Issues in Service Delivery Models of Cloud Computing. – Journal of Network and Computer Applications, Elsevier, Vol. **34**, 2011, Issue 1, pp. 1-11.
5. Hari Krishna, B., S. Kiran, G. Murali, Pradeep Kumar, R. Reddy. Security Issues in Service Model of Cloud Computing Environment. – Procedia Computer Science, Vol. **87**, 2016, pp. 246-251.
6. Bhadauria, R., S. Sanyal. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. – International Journal of Computer Applications, Vol. **47**, 2012, No 18, pp. 47-66.
7. Hashizume, K., D. G. Rosado, E. Fernández-Medina, E. B. Fernandez. An Analysis of Security Issues for Cloud Computing. – Journal of Internet Services and Applications, Vol. **4**, 2013, No 5.
8. Aldossary, S., W. Allen. Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. – International Journal of Advanced Computer Science and Applications, Vol. **7**, 2016, No 4.
9. Catteddu, D., G. Hogben. Cloud Computing: Benefits, Risks and Recommendations for Information Security. European Union Agency for Network and Information Security (ENISA), 2009, pp. 1-125.
10. Sumitra, B., C. R. Pethuru, M. Misbahuddin. A Survey of Cloud Authentication Attacks and Solution Approaches. – International Journal of Innovative Research in Computer and Communication Engineering, Vol. **2**, 2014, Issue 10, pp. 6245-6253.
11. Sushmitha, Y., V. Krishna Reddy, Pavan Deja, D. Reddy. A Survey on Cloud Computing Security Issues. – International Journal of Computer Science and Innovation, Vol. **2015**, 2015, No 2, pp. 88-96.
12. Herbert Raj, P., P. Ravi Kumar, P. Jelciana. Mobile Cloud Computing: A Survey on Challenges and Issues. – International Journal of Computer Science and Information Security, Vol. **14**, 2016, No 12, pp. 165-170.
13. Brunette, G., R. Moghul. Security Guidance for Critical Area of Focus in Cloud Computing. V2.1. Cloud Security Alliance (CSA). 2009, pp. 1-76.
14. Xiao, Z., Y. Xiao. Security and Privacy in Cloud Computing. – IEEE Communications Surveys & Tutorial, Vol. **15**, 2012, No 2, pp. 843-859.
15. Reed, A., C. Rezek, P. Simmonds. Security Guidance for Critical Area of Focus in Cloud Computing. V3.0. Cloud Security Alliance (CSA). 2011, pp. 1-177.
16. Price, D. The Challenges of Multi-Tenancy. 26 March 2014.
    https://cloudtweaks.com/2014/03/challenges-multi-tenancy/
17. Ravi Kumar, P., P. Herbert Raj, P. Jelciana. Exploring Data Security Issues and Solutions in Cloud Computing. – In: Proc. of 6th International Conference on Smart Computing and Communication (ICSCC'17)), National Institute of Technology, Kurukshetra, India, 7-8 December 2017.
18. Ludwig, S. Cloud 101: What the Heck Do IaaS, PaaS and SaaS Companies Do? VentureBeat, 14 November 2011.
    https://venturebeat.com/2011/11/14/cloud-iaas-paas-saas/

19. S o o k h a k, M., H. T a l e b i a n, E. A h m e d, A. G a n i, M. K. K h a n. A Review on Remote Data Auditing in Single Cloud Server: Taxonomy and Open Issues. – Journal of Network and Computer Applications, Vol. **43**, 2014, pp. 121-141.
20. W o r l a n y o, E. A Survey of Cloud Computing Security: Issues, Challenges and Solutions. 30 November 2015.
http://www.cse.wustl.edu/~jain//cse570-15/ftp/cld_sec/index.html
21. Amazon Web Services: Overview of Security Processes. August 2016.
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
22. P e s a n t e, L. Introduction to Information Security. Carnegie Mellon University, 2008.
https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf
23. S a b a h i, F. Secure Virtualization for Cloud Environment Using Hypervisor-Based Technology. – International Journal of Machine Learning and Computing, Vol. **2**, 2012, No 1, pp. 39-45.
24. G a l l a g h e r, P. R. A Guide to Understanding Data Remanence in Automated Information Systems. The Rainbow Books. Chapter 3 and 4. 1991.
25. OWASP Top 10 Application Security Risks – 2017. Open Web Application Security Project (OWASP).
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
26. T a y l o r, P. J., J. N u f r y k. CompTIA Security+ Exam Study Material, 2014.
27. R a t h i e, I. An Approach to Application Security. SANS Security Essentials White Paper, SANS Institute.
https://www.sans.org/reading-room/whitepapers/application/approach-application-security-16
28. OWASP Top 10 Backdoors, Open Web Application Security Project (OWASP). **https://www.owasp.org/images/a/ae/OWASP_10_Most_Common_Backdoors.pdf**
29. R o u s e, M. Data Integrity. September 2005.
http://searchdatacenter.techtarget.com/definition/integrity
30. S u n, Y., J. Z h a n g, Y. X i o n g, G. Z h u. Data Security and Privacy in Cloud Computing. – International Journal of Distributed Sensor Networks, Vol. **10**, 2014, Issue 7, pp. 1-9.
31. W a n g, C., S. C h o w, Q. W a n g, K. R e n, W. L o u. Privacy-Preserving Public Auditing for Secure Cloud Storage. – IEEE Transactions on Computers, Vol. **62**, 2013, Issue 2, pp. 362-375.
32. B a l u s a m y, B., P. V e n k a t a k r i s h n a, A. V a i d h y a n a t h a n, M. R a v i k u m a r, N. D e v i M u n i s a m y. Enhanced Security Framework for Data Integrity Using Third-Party Auditing in the Cloud System. – In: Proc. of Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Advances in Intelligent Systems and Computing, Springer, Vol. **325**, 2015, pp. 25-31.
33. A t i e n i e s e, G., R. B u r n s, R. C u r t m o l a, J. H e r r i n g, L. K i s s n e r, Z. P e t e r s o n, D. S o n g. Provable Data Possession at Untrusted Stores. – In: Proc. of 14th ACM Conference on Computer and Communication Security, 2007, pp. 598-609.
34. A t i e n i e s e, G., R. D i P u e t r o, L. V. M a n c i n i, G. T s u d i k. Scalable and Efficient Provable Data Possession. – In: Proc. of 4th International Conference on Security and Privacy in Communication Networks, Art. 9, 2008.
35. A t i e n i e s e, G., R. B u r n s, R. C u r t m o l a, J. H e r r i n g, O. K h a n, L. K i s s n e r, Z. P e t e r s o n, D. S o n g. Remote Data Checking using Provable Data Possession. – ACM Transaction of Information and System Security, Vol. **14**, 2011, No 1, pp. 12-34.
36. W a n g, Q., C. W a n g, K. R e n, W. L o u, J. L i. Enable Public Auditability and Data Dynamics for Storage Security in Cloud Computing. – IEEE Transactions of Parallel and Distributed Systems, Vol. **22**, 2011, No 5, pp. 847-859.
37. S o o k h a k, M., A. G a n i, M. K. K h a n, R. B u y y a. Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing. – Information Sciences: An International Journal, Vol. **380**, 2017, Issue C, pp. 101-116.
38. CSCC Security for Cloud Computing Ten Steps to Ensure Success. – Cloud Standards Customer Council, 2015, pp. 1-35.
39. R o u s e, M. Authentication. February 2015.
http://searchsecurity.techtarget.com/definition/authentication

40. S h i n d e r, D. L. Authentication in the Cloud. InfoSec Institute.13 August 2014. **http://resources.infosecinstitute.com/authentication-cloud/#gref**
41. J a k i m o s k i, K. Security Techniques for Data Protection in Cloud Computing. – International Journal of Grid and Distributed Computing, Vol. **9**, 2016, No 1, pp. 49-56.
42. F e r r i l l. T. The Best Identity Management Solutions of 2017. 3 July 2017. **https://www.pcmag.com/article2/0,2817,2491437,00.asp**
43. Data Backup: Cloud Computing VS On-Site Options. **https://www.staples.com/content-hub/data-backup-cloud-computing-vs-on-site-options/**
44. Cloud Middleware. **https://www.techopedia.com/definition/30630/cloud-middleware-software**
45. F a r a h z a d i, A., P. S h a m s, J. R e z a z a d e h, R. F a r a h b a k h s h. Middleware Technologies for Cloud of Things – A Survey. – Digital Communications and Networks, Elsevier, 18 April 2017. **https://doi.org/10.1016/j.dcan.2017.04.005**
46. N o l l e, T. How to Address Security Risks Posed by Middleware Tools. December 2014. **http://searchmicroservices.techtarget.com/tip/How-to-address-security-risks-posed-by-middleware-tools**
47. Role of Cloud Computing Operating Systems. 8 March 2013. **http://www.getcloudservices.com/blog/role-of-cloud-computing-os/**
48. H u r w i t z, J., M. K a u f m a n. The Role of the Operating System in the Cloud Environment. Hurwitz White Paper, 2011. **https://www.redhat.com/f/pdf/The_Role_of_the_OS_in_the_Cloud.pdf**
49. The Operating System Hardening Issues and Practices Information Technology Essay. 23 March 2015. **https://www.ukessays.com/essays/information-technology/the-operating-system-hardening-issues-and-practices-information-technology-essay.php**
50. L i u, Y., Y. S u n, J. R y o o, S. R i z v i. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. – Journal of Computing Science and Engineering, Vol. **9**, 2015, No 3, pp. 119-133.
51. R i s t e n p a r t, T., E. T r o m e r, H. S h a c h a m, S. S a v a g e. Hey, You Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. – In: Proc. of 16th ACM Conference on Computer and Communications Security, ACM, 2009, pp. 199-212.
52. A v i r a m, A., S. H u, B. F o r d, R. G u m m a d i. Determinating Timing Channels in Compute Clouds. – In: Proc. of ACM Workshop on Cloud Computing Security Workshop, ACM, 2010, pp. 103-108.
53. J a n s e n, W. A. Cloud Hooks: Security and Privacy Issues in Cloud Computing. – In: Proc. of IEEE 44th Hawaii International Conference on System Sciences (HICSS'11), IEEE, 2011, pp. 1-10.
54. W u, H., Y. D i n g, C. W i n e r, L. Y a o. Network Security for Virtual Machine in Cloud Computing. – In: Proc. of IEEE 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT'10), IEEE, 2010, pp. 18-21.
55. S o n g, M. H. Analysis of Risks for Virtualization Technology. – Applied Mechanics and Materials, Vol. **539**, 2014, pp. 374-377.
56. C o r r a d i, A., M. F a n e l l i, L. F o s c h i n i. VM Consolidation: A Real Case Based on OpenStack Cloud. – Future Generation Computer Systems, Vol. **32**, 2014, pp. 118-127.
57. Z h a n g, F., H. C h e n. Security-Preserving Live Migration of Virtual Machines in the Cloud. – Journal of Network and Systems Management, Vol. **21**, 2013, No 4, pp. 562-587.
58. Cloud Server. **https://www.techopedia.com/definition/29019/cloud-server**
59. What is a Cloud Server? IBM Cloud. **https://www.ibm.com/cloud-computing/learn-more/what-is-a-cloud-server/**
60. Web Server Security and Database Server Security. **https://www.acunetix.com/websitesecurity/webserver-security/**
61. E l l i n g w o o d, J. 7 Security Measures to Protect Your Servers. 5 March 2015. **https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers**

62. C h a k r a v a r t y, A. Importance of the Network in Cloud Computing. 25 January 2012. **https://blogs.cisco.com/datacenter/importance-of-the-network-in-cloud-computing**
63. S c h o o, P., V. F u s e n i g, V. S o u z a, M. M e l o, P. M u r r a y, H. D e b a r, H. M e d h i o u b, D. Z e g h l a c h e. Challenges for Cloud Networking Security. – In: Proc. of International Conference on Mobile Networks and Management, 2010, pp. 298-313.
64. W a n g, J. J., S. M u. Security Issues and Countermeasures in Cloud Computing. – In: Proc. of IEEE International Conference on Grey Systems and Intelligent Services (GSIS), 2011, pp. 843-846.
65. McAfee Labs Threats Report. March 2016. **https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf**
66. Top 7 Network Attack Types in 2016. Calyptix Blog. 13 June 2016. **https://www.calyptix.com/top-threats/top-7-network-attack-types-2016/**
67. Ransom.WannaCry. Symantec Security Response. 24 May 2017. **https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99&tabid=2**
68. D a l z i e l, H. Summary of 5 Major DoS Attack Types. 1 November 2013. **https://www.concise-courses.com/5-major-types-of-dos-attack/**
69. DDOS Attacks. **https://www.incapsula.com/ddos/ddos-attacks/**
70. R o u s e, M. DNS Attack. July 2015. **http://searchsecurity.techtarget.com/definition/DNS-attack**
71. Common Types of Network Attacks**.** **https://technet.microsoft.com/en-us/library/cc959354.aspx**
72. V i e i r a, K., A. S c h u l t e r, C. B. W e s t p h a l l, C. M. W e s t p h a l l. Intrusion Detection for Grid and Cloud Computing. – IT Professional, IEEE Computer Society, Vol. **12**, 2010, Issue 4, pp. 38-43.
73. L o, C. C., C. C. H u a n g, J. K u. A Cooperative Intrusion Detection System Framework for Cloud Computing Networks. – In: Proc. of 39th International Conference on Parallel Processing Workshops (ICPPW), IEEE, 2010, pp. 280-284.
74. R o u s e, M. Secure Sockets Layer (SSL). November 2016. **http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL**