IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-6, Issue-7 E-ISSN: 2347-2693

Investigation of Security Issues on Data in Triplet Levels of Cloud Environment

R. Denis[1*], P. Madhubala[2]

[1]Department of Computer Science, Periyar University, Salem, India
[1]PG Department of Computer Science, Sacred Heart College (Autonomous), Thiruvalluvar University, India
[2]PG & Research Department of Computer Science, Don Bosco College, Dharmapuri, India

[*]*Corresponding Author: denisatshc@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 24/Jul/2018, Published: 31/July/2018

***Abstract*—** Data protection is a crucial security issue for most organizations. Before moving into the cloud, cloud users need to clearly identify data objects to be protected and classify data based on their implication on security, and then define the security policy for data protection as well as the policy enforcement mechanisms. For most applications, data objects would include not only bulky data at rest in cloud servers (e.g., user database and/or file system), but also data in transit between the cloud and the user(s) which could be transmitted over the Internet or via mobile media (In many circumstances, it would be more cost-effective and convenient to move large volumes of data to the cloud by mobile media like archive tapes than transmitting over the Internet.). Data objects may also include user identity information created by the user management model, service audit data produced by the auditing model, service problem information used to describe the service instance(s), temporary runtime data generated by the instance(s), and many other application data. Different types of data would be of different value and hence have different security implication to cloud users. For example, user database at rest in cloud servers may be of the core value for cloud users and thus require strong protection to guarantee data confidentiality, integrity and availability. Sensitive business data is more vulnerable today than ever before, putting reputations and the bottom line at risk. Corporate trade secrets, national security information, personal medical records, Social Security and credit card numbers are all stored, used, and transmitted online and through connected devices.

***Keywords*—**Cloud Service Provider(CSP), Cloud Service Consumer(CSC), Data at Rest, Data in transit, Data in use

I. INTRODUCTION

Confidentiality, Integrity and Availability (CIA triad) are the three important properties of a data. Authentication, authorization and non repudiation are another three important properties associated with people who use the data [1]. Confidentiality is related to data privacy, where the data is not disclosed to unauthorized parties on any occasion [2]. 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. Non-repudiation is the assurance that an authenticated user cannot deny after performing a job. This survey is organized as follows, Section I contains the introduction of data security and its importance, Section II explores the different data stages, Section III dedicated for the study of various security issues and Section IV concludes the paper with future directions.

II. DATA STAGES

The flow of data through a cloud or by another means goes through various distinct stages, with each stage requiring one or more of the previous properties to be maintained. These stages are as follows:

A. Data-at-Rest

In this stage, data is stored at CSP's infrastructure and data security and privacy becomes CSP's responsibility [3]. CSP need to insure CIA of the data. This is when data has been stored in the cloud infrastructure. The main issue with this stage for the CSC is their loss of control over the data. The onus of defending against attacks at this stage hence falls on the CSP. Typically data is at rest when it is stored on a hard drive (or SSD) somewhere. In this relatively secure state, information is primarily protected by conventional perimeter-based defenses such as firewalls, passwords and anti-virus programs. However, these barriers are not impenetrable.

Organizations need additional layers of defense to protect sensitive data from intruders in the event that the network is compromised.

Data at rest generally refers data stored in persistent storage such as database, file system, tape, disk etc. If we want data to be secure in transit or motion it has to be firstly secure in rest. There are many techniques by which we can secure our data at rest such as Encryption, Anonymization, data masking, and data erasure and so on. Data security at rest is important as enterprises start to use the data repositories for big data analytics and at same time realizes the value of such data. So data security at rest is a key concern for all the security administrators. Encryption is the leading edge for securing data at rest.

B. 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 [3]. Encryption is one of the methods used to protect the data while in transit. This is when data is in the process of being transmitted either to the cloud infrastructure or to the computing device used by the CSC. Here, data is most at risk of being intercepted, hence violating confidentiality.

Data is at its most vulnerable when it is in motion, and protecting information in this state requires specialized capabilities. Our expectation of immediacy dictates that a growing volume of sensitive data be transmitted digitally—forcing many organizations to replace couriers, faxes, and conventional mail service with faster options such as email. Today, more than 100 million business emails are sent every day, with over 95% of the data payload in file attachments.

The moment that data is set in motion, we are unable to fully control it, making it more susceptible to eavesdropping. From an organizational perspective, this requires the need for data encryption, thus rendering information unreadable to unauthorized personnel. Therefore, even if eavesdropping had occurred or a mobile device is stolen, the data remains confidential and secure, and renders any invalid authentication useless [4].

The term "Data Security in Motion" describes the security of data while data is transmitting from one place or node to another. Sometimes it is also called data in use. Although movement of data from disk to processor and RAM or Cache is also considered as moving data, particularly in big data scenario where the storage and processing of data and other resources are highly distributed. Protecting big data while it is in motion is important in big data implementations. Industries like retail, healthcare, supply chain, network intelligence and energy production brings exclusive and unique requirements and standards for securing data in motion.

C. 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 that is the data is being processed to information [3]. Here, the issues might lie with the corruption of data while it is being processed.

Data in use is more vulnerable than data at rest because, by definition, it must be accessible to those who need it. Of course, the more people and devices that have access to the data, the greater the risk that it will end up in the wrong hands at some point. The keys to securing data in use are to control access as tightly as possible and to incorporate some type of authentication to ensure that users aren't hiding behind stolen identities.

In addition to these three stages, the data left out in case of data transfer or data removal also needs to be considered, since it can cause severe security issues in the case of public cloud offerings since a CSC may end up gaining access to sections of data not properly deleted from a prior CSC.

D. Data-after-Delete

Another important and neglected issue with data is, data-after-delete (data remanence) [5]. Data remanence is the residual physical representation of data that has been erased [6]. After storage media is cleaned, there may be some physical characteristics that allow data to be reconstructed [6, 7]. 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.

III. SECURITY ISSUES IN DATA STAGES

Cloud systems have a layered architecture of different services and control levels for users. SaaS, PaaS and IaaS layers are considered for associated security risks and problems. The first part of this section briefs about the security issues related to SaaS, PaaS, Iaas and the later parts details about the security issues at different levels while transmitting data.

A. Security concerns for Software as a Service (SaaS)

SaaS is exposed by attacks on API's, publishers, web portals and interfaces. The attacks on the SaaS are categorized into two broad groups: attacks on development tools and attacks on management tools. Most popular services on SaaS are web services, web portals and APIs. Intruders' attempt unauthorized access and gain of services by attacking web portals and APIs. These attacks affect data privacy. Intruders try to extract the sensitive information of API Keys, private keys, and credentials of publishers via different kinds of attacks and automated tools. Another possibility of attack on

this layer is exposure of secure shell for extracting key credentials.

Data protection - in cloud computing applications are deployed in shared resource environments; therefore, data privacy is an important aspect. Data privacy has three major challenges: integrity, authorized access and availability (backup/ replication). Data integrity ensures that the data are not corrupted or tampered during communication. Authorized access prevents data from intrusion attacks while backups and replicas allow data access efficiently even in case of a technical fault or disaster at some cloud location. Data are shared and communicated at the common network backbone. Hence malicious attackers or intruders can deploy hidden proxy applications between the cloud provider and consumer to scavenge information of login credentials and session details [8]. An intruder can also perform packet sniffing or IP-spoofing as a middle-party and can access and/or alter the restricted or sensitive information. One possible solution for the data privacy in cloud computing is Cisco Secure Data Center Framework that provides multilayer security mechanism [8].

Attacks on interfaces of the cloud interfaces can result in a root level access of a machine without initiating a direct attack on the cloud infrastructure. Two different kinds of attacks are launched on authentication mechanism of clouds. The control interfaces are vulnerable to signature wrapping and advanced cross site scripting (XSS) techniques. First kind of attack is referred to as signature wrapping attack or XML Signature Wrapping attacks. Single signed SOAP message or X.509 certificate can be used to compromise security of customers' accounts through operations on virtual machines or resetting of passwords. Second type of attacks exploits the vulnerability in XSS. The particular vulnerability attack steals username and password pair information.

Attacks on SSH (Secure Shell) is the basic mechanism used to establish trust and connection with cloud services, are the most alarming threat that compromises control trust. According to Ponemon 2014 SSH security Vulnerability Report [9], 74 percent organizations have no control to provision, rotate, track and remove SSH keys. Cybercriminals take full advantage of these vulnerabilities and use cloud computing to launch different attacks. An organizations' cloud workload can be used host botnets if SSH access has been compromised. Attackers have hosted the Zeus botnet and control infrastructure on Amazon EC2 instances [8]. The different types of attack on SSH include attacks on API keys, attacks on user credentials, and attacks on publisher credentials.

B. Security concerns for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

IaaS and PaaS layers are overlapped in the model due to their interdependency on each other. The attacks on these layers are grouped into three types: attacks on cloud services, attacks on virtualization, and attacks on utility computing. The security concerns for IaaS and PaaS are discussed below.

Hardware Virtualization - interconnectivity is the biggest security concern in the designing of cloud computing platform. VMs are linked using bridge and route virtual network configuration modes. The bridge mode works as a virtual hub shared among all the VMs, which may result in sniffing the virtual network by a compromised VM. In the route mode, where route works as a virtual switch, each VM is connected using a dedicated virtual interface. Any network intruder in a LAN segment of a network can access virtual environments by address resolution protocol (ARP) spoofing and MAC spoofing. ARP spoofing alters the ARP tables and management interfaces and systems. On the other hand, an intruder can mimic another host through MAC spoofing and also change address of host or guest Virtual Machine (VM) to gain access of restricted resources [10]. The attacks and exploitation of virtual environments are much diversified and they will increase in future since platforms are growing in number and complexity. Therefore, a mechanism for detecting attacks along with preventions is necessary.

Software Virtualization - attack may examine the VM images to launch an attack or steal of information, especially targeting development images, which are accidentally released [10]. It is also possible to provide a VM image having malware to cloud computing system resulting in theft and corruption of data. For example, cloud consumers are enticed to run tainted VM images contributed to image repository manipulating the registration process for first page listing.

Cloud Software's - Multi-tenancy in cloud computing requires multiplexing the execution of VMs from different consumer on the same physical server [8]. Softwares deployed on guest VM remain susceptible to attack and compromise. A malicious code in VM may interfere with the hypervisor or other VMs. Shortcomings in programming interfaces and processing of instructions are the main targets to uncover vulnerabilities [8]. This security concern also includes indirect attacks such as man-in-the middle during a live VM migration; insertion VM based rootkit during memory modification; a zero-day exploit in HyperVM; side-channel attack to gain information.

Utility computing - is the concept that emerged from grid computing, and it combines computation, storage and bandwidth to provide services on the demand through payment by the customer. It also provides two basic advantages of cost reduction and scalability. Security risk associated with utility computing is access by attackers who

want to utilize resources without paying [8]. Majority of hackers and crackers use the computing power or storage for the illegal use. The common use of public cloud includes e-commerce, web-application and Web site hosting making these services vulnerable to variety of attacks on possession, authenticity, integrity and utility. A compromised client may perform a Fraudulent Resource Consumption (FRC) attack by using the metered bandwidth of web-based service that results in a financial burden on the cloud consumer [11].

Service Level Agreement (SLA) - is an optimal way for ensuring security and trust. The implementation of SLA results in a well-designed contract of responsibilities between parties that can enhance security level. In cloud environment, SLA can be combined with the web service level agreement (WSLA) for mitigating security risks [8]. SLA defines the different levels of security and their complexity based on the services for the better understanding of the security policies to a cloud consumer. The existing cloud storage systems do not provide security guarantees in their SLAs effecting the adaptation of cloud services. A cloud storage service may leak private data, return inconsistent data or modify the data due to bugs, hacking, crashes, or misconfigurations. This security concerns require proper SLA guarantee models such as CloudProof [12].

C. 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 [13]. 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.

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 [14]. 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. .

Cross-Site Scripting (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 [14]. There are two types of XSS attack namely, stored attack and reflected attack.

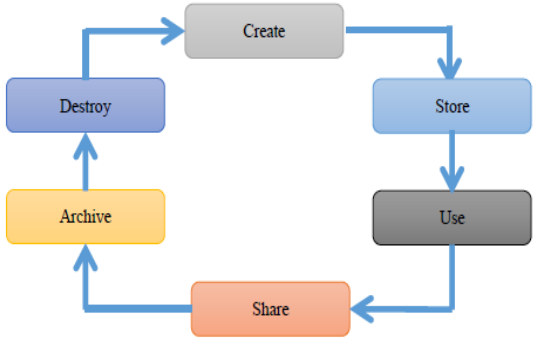
Cross-site request forgery (XSRF) attack - takes advantage of the trust established between an authorized user of a website and the website itself.

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 [14]. If a vulnerable component is exploited, this can lead to serious data loss or server takes over. Applications and APIs using components with known vulnerabilities may pull down the application's defence mechanism and enable to various attacks and impacts.

Under protected 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.

Cookie poisonings - 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.

Hidden field manipulation -is a part of the data manipulation attack [15]. 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].



Backdoor and Debug Option - is a hidden entrance to a computer system that can be used to bypass security policies [16]. 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 to get into the application for gaining access to sensitive information.

D. Security threats in the data level

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. 1. 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.

E. 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 [1]. When data is modified in an unpredicted way, this situation is called as loss of integrity [1]. When data is lost or become inaccessible, this situation is called "loss of availability" [1]. 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 [17]. 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.

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.

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 [18]. 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].

Broken authentication and session management - is 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 [14].

Broken Access Control - 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., [14].

Sensitive data exposure

This flaw occurs when web applications and APIs do not properly protect sensitive data [14] 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.

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].

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 [20].

F. Security threats in the middleware level

According to Techopedia [19], 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 and in IaaS, it is handled by CSC. 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 [19]:

- 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 [21]. 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 [22]. 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 [22].

G. Security issues in the operating system level

Operating System (OS) services are provided by CSP in PaaS and SaaS and it is provided by CSC in IaaS. 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 [23]:

- 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 [24]. Operating systems are susceptible to a number of internal and external attacks due to un-patched vulnerabilities, disgruntled employees or misconfigured server settings [24].

H. Security vulnerabilities in the virtualization level

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 [24].

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 behavior and in turn can get some sensitive information about the victim or the CSP itself [8, 24]. Timing side-channel attack [24] 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, 24].

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, 24].

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, 24].

VM Migration – Due to fault tolerance, load balancing and maintenance, a VM can migrate from one physical machine to another [7, 8, and 24]. 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 [24]. 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].

I. Security issues related to server level

Security in the sever level 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 [24]. Security misconfiguration and insufficient attack protection are some security issues that can be related to the server stack [14]. The following are the characteristics/functionalities of a cloud server [24].

- 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.

J. Security issues related to storage level

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.

Cloud Data Storage Threats threats are identified from the client's perspective, mainly due to the loss of physical control and the abstract nature of the cloud [24], as follows:

Data exposure – stored on remote cloud servers, out of the control of their owners, data are more likely exposed to potential adversaries. That is, the anytime/anywhere access increases the number of attackers, such as unauthorized insiders, revoked group members or even malicious cloud administrator. Additionally, due to law enforcement, when cloud servers are located in other countries, client's data may be accessed by enforcement agencies without permission or knowledge of their owners. Providing data confidentiality, in multi-tenant environments, becomes challenging and conflicting. This is considerably due to the fact that users outsource their data on remote servers, under the control and management of possible untrusted Cloud Service Providers (CSPs). It is commonly agreed that data encryption at the client side is a great alternative to relieve such data confidentiality concerns [18,19], as the cloud client preserves the deciphering keys out of reach of the provider. Nonetheless, this approach gives rise to various security and privacy issues. On one side, it increases key management concerns, such as, storing and maintaining keys' availability at the client side. The confidentiality preservation is even more complicated when flexible data sharing among a group of users is needed [20]. First, it requires efficient sharing of deciphering keys between authorized users. The challenge is to define a smooth group revocation which does not require updating the secret keys of the remaining users, so that the complexity of key management is minimized. Second, access control policies have to be versatile, flexible and distinguishable among users with different access rights. That is, data sharing may be realized among different users or groups, and users may belong to several groups. On the other side, the protection of the user's privacy requires more than just encryption of transmitted and stored data. For instance, the fact that a user invokes a specific content, or communicates with a specific client may already provide enough information to an adversary [24]. In addition, user identity information can contain Personally Identifiable Information (PII) which is of high critical to the user privacy.

Unauthorized Access – in cloud environments, access control is a highly non trivial matter of granting and revoking rights to specific users or dynamic groups. That is, access control policies needs flexibility and distinguishability among users having different access rights. In fact, data can be shared by different users that may belong to several groups. In addition, these groups may be highly dynamic. Thus, the challenge is to define an efficient revocation mechanism, at an arbitrarily fine granularity.

Data loss and manipulation – cloud providers generally claim storing data files with redundancy to protect against data loss. Additionally, they often disperse these data across multiple storage placements. Such distribution provides resilience against hardware failures. However, for storage capacities saving and operating costs reduction, dishonest providers might intentionally neglect these replication procedures, thus resulting in unrecoverable data errors or even data losses. This dishonest trend might be amplified as a large amount of "cold" data are accessed on rare occasions. Therefore, the data integrity checking is considered as a

relevant concern, especially as it is tightly linked to data availability. Data integrity verification might be operated in three ways:

Between a client and a cloud provider – a cloud customer should efficiently perform periodical remote integrity verifications, by not keeping the data locally. It means that solutions should take into consideration the constrained storage and computation capabilities of the customer and the large size of outsourced data.

Within a cloud infrastructure – it is important for a cloud provider to mitigate byzantine failures and drive-crashes by checking the integrity of data blocks stored across multiple storage nodes.

Between two cloud providers – in the case of the cloud of clouds scenarios [22, 24], data fragments are dispersed on multiple cloud platforms. Thus, a CSP, through its cloud gate, should periodically check the authenticity of the data blocks hosted in another cloud infrastructure.

SLA violation – the Service Level Agreement (SLA) relies on a contract signed between the client and the service provider including functional and non-functional requirements of the service [23, 25]. SLA considers obligations, service pricing, and penalties in case of agreement violations. However, due to the abstract nature of clouds, SLA violation with regards to data is multifold [44, 16]. First, for securely managing outsourced data, the cloud provider has to disperse clients' data across multiple storage capacities. Such distribution provides resilience against hardware. Nevertheless, to save storage capacities and reduce operating costs, dishonest providers might intentionally disregard these replication procedures, thus leading to unrecoverable data errors or data losses. Even if a fault tolerant policy is supported by the cloud providers, clients have no technical means for verifying that their data are safe, for instance, with regard to possible drive-crashes [24].
Second, SLA violation concerns also privacy preservation. That is, the U.S. Patriot Act [24] gives the government unprecedented access to outsourced data which are either physically hosted in the U.S. or generated by an American entity (i.e. an American enterprise or an enterprise having economic stakes in the U.S.).

Cheap and lazy provider – this threat model is widely considered in data auditing schemes [24], such that the cloud provider wants to save resources by storing fewer redundant data than necessary. In addition, this lazy provider pretends to perform some computations to provide the challenger with the expected answer.

Malicious users – malicious users are entities that attempt to deviate from the protocol or to provide invalid information, in order to disclose data outsourced by other legitimate clients or to learn extra information about another entity's inputs [24]. For example, in a sharing scenario, an attacker can be either a revoked user with valid data decryption keys, an unauthorized group member or a group member with limited access rights. As such, the attacker targets to get access to the outsourced shared data. The objective of this malicious user is to convince the cloud server that he is a legitimate group member.

K. Security issues related to network level

The Network is one of the important levels in cloud computing because the users are connected to the cloud through the network stack and the data are also transferred using this level. One of the important success of cloud computing depends on how secured it's underlying network infrastructure. According to Arup Chakravarty [25], 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 [24]. 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 standardized third party security framework for cloud computing which benefits both CSP and CSC [8].

Browser Attacks – is the top most network attacks and it 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 [26]. These attacks can be thwarted by regular updates to browser and related applications [26].

Brute Force Attacks – is the next top most network attack which is used by hackers to get the password or pin number by trial and error [26].

Denial-of-Service (DoS) attacks – is the third top most network attack 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 [26].

Secure Sockets Layer (SSL) attacks – 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. In this, the attacker intercepts an encrypted data before it can be encrypted and giving access to the sensitive data to the attackers [26].

Scans– 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– 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. [27].

Backdoor attacks– happen 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 [26].

Jamming adversaries - attacks on wireless devices in cloud and IOT target deterioration of the networks by emitting radio frequency signals without following a specific protocol [24]. The radio interference severely impacts the network operations and can affect the sending and receiving of data by legitimate nodes, resulting in malfunctioning or unpredictable behavior of the system.

Insecure initialization- A secure mechanism of initializing and configuring IoT cloud at the physical layer ensures a proper functionality of the entire system without violating privacy and disruption of network services [24]. The physical layer communication also needs to be secured in order to make it inaccessible to unauthorized receivers.

Low-level Sybil and spoofing attacks- The Sybil attacks in a wireless network are caused by malicious Sybil nodes which use fake identities to degrade the cloud functionality. On the physical layer, a Sybil node may use random forged MAC values for masquerading as a different device while aiming at depletion of network resources [24]. Consequently, the legitimate nodes maybe denied access to resources.

Insecure physical interface - Several physical factors compound serious threats to proper functioning of devices in IoT. The poor physical security, software access through physical interfaces, and tools for testing/debugging may be exploited to compromise nodes in the network [23].

Sleep deprivation attack - The energy constrained devices in cloud and IoT are vulnerable to ‘‘sleep deprivation’’ attacks by causing the sensor nodes to stay awake [24].

Replay or duplication attacks due to fragmentation - The fragmentation of IPv6 packets is required for devices conforming to the IEEE 802.15.4 standard which is characterized with small frame sizes. A reconstruction of the packet fragment fields may result in depletion of resources, buffer overflows and rebooting of the devices [24]. The duplicate fragments sent by malicious nodes affect the packet re-assembly, thereby hindering the processing of other legitimate packets [24].

Insecure neighbor discovery - The cloud and IoT deployment architecture requires every device to be identified uniquely on the network. The message communication taking place for identification must be secure to ensure that the data being transmitted to a device in the end-to-end communication reaches the specified destination. The neighbor discovery phase prior to transmission of data performs different steps including the router discovery and address resolution[24]. The usage of neighbor discovery packets without proper verification may have severe implications along with denial-of service.

Buffer reservation attack - As a receiving node requires to reserve buffer space for re-assembly of incoming packets, an attacker may exploit it by sending incomplete packets [24]. This attack results in denial-of-service as other fragment packets are discarded due to the space occupied by incomplete packets sent by the attacker.

RPL routing attack -The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is vulnerable to several attacks triggered through compromised nodes existing in the network [28]. The attack may result in depletion of resources and eavesdropping.

Sinkhole and wormhole attacks - With the sinkhole attacks, the attacker node responds to the routing requests, thereby making the packets route through the attacker node which can then be used to perform malicious activity on the network [28]. The attacks on network may further deteriorate the operations due to wormhole attacks in which a tunnel is created between two nodes so that packets arriving at a node reach other node immediately [29]. These attacks have severe implications including eavesdropping, privacy violation and denial-of-service.

Sybil attacks on intermediate layers - Similar to the Sybil attacks on low-level layers, the Sybil nodes can be deployed to degrade the network performance and even violate data privacy. The communication by Sybil nodes using fake identities in a network may result in spamming, disseminating malware or launching phishing attacks.

*Authentication **and secure** communication* - The devices and users in Cloud need to be authenticated through key

management systems. Any loophole in security at network layer or large overhead of securing communication may expose the network to a large number of vulnerabilities. For instance, due to constrained resources, the overhead of Datagram Transport Level Security (DTLS) requires to be minimized, and the cryptographic mechanisms ensuring secure communication of data in cloud must take into account the efficiency as well as the scarcity of other resources [30].

Transport level end-to-end security - The transport level end to end security aims at providing secure mechanism so that the data from the sender node is received by the desired destination node in a reliable manner [30]. It requires comprehensive authentication mechanisms which ensure secure message communication in encrypted form without violating privacy while working with minimum overhead [30].

Session establishment and resumption - session hijacking on transport layer with forged messages can result in denial-of service [30]. An attacking node can impersonate the victim node to continue the session between two nodes. The communicating nodes may even require re-transmission of messages by altering the sequence numbers.

Privacy violation on cloud-based IoT- Different attacks which may violate identity and location privacy may be launched on cloud or delay tolerant network based IoT [30]. Similarly, a malicious cloud service provider on which IoT deployment is based, can access confidential information being transmitted to a desired destination.

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

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

Risk profiling – due to the heavy workload cloud are less involved with ownership and maintenance of hardware and software. The cloud gives contract to organization to maintenance of software and hardware. This concept is good, but cloud does not know the organization internal security procedure, patching [30], auditing, security policies, hardening, and logging process. This unawareness comes greater risk and threats. For removal of threats cloud have an awareness of partial infrastructure details, logs and data, and cloud should have a monitoring and altering system.

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

IV. CONCLUSION AND FUTURE SCOPE

The cloud problems are mainly with the security and privacy of the data stored in the cloud. The cloud environments like heterogeneity, resource sharing, multi-tenancy, virtualization, mobile cloud computing and Service Level Agreement (SLA) that makes the cloud security more vulnerable. This paper provides the data stages and security issues at various levels. In future there is a plan to review about the solutions for maintaining the above discussed problem. Mean while, there are also new developments in cloud computing like Container-as-a-Service (CaaS),Software-defined networking, Software-defined-storage (abstracts the logical storage services and capabilities away from the underlying hardware) and Cloud-of-Things (CoT). All these new developments bring new challenges in cloud computing and they need to be addressed. When there is a change in technology, always review the security policies and procedures and update accordingly to protect the data and its privacy.

REFERENCES

[1] Pesante, L. "*Introduction to Information Security*", carnegie Mellon University, 2008. https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf

[2] Worlany, E. "*A Survey of Cloud Computing Security: ISuues, Challenges and Solutions*", November 2015.

[3] P.Ravikumar, P. Herbert Raj, "*Exploring security issues and solutions in cloud computing services"*, Cybernatics and information technologies, Vol.17, Issue.4, 2017.

[4] F e r r i l l. T. The Best Identity Management Solutions of 2017. 3 July 2017.

[5] Hari Krishna, B., S. Kiran, "*Security issues in cloud computing and associated mitigation techniques*", Procedia Computer Science, Vol.87, pp.246-251, 2016.

[6] Sabahi, F., "*Secure Virtualization for Cloud Environment using Hypervisor-Based Technology*", International Journal of Machine Learing and Computing, Vol.2, Issue.1, pp.39-45, 2012.

[7] Gallagher, P.R. " *A* Guide to Understanding Data Remanence in Automated Information Systems", The Rainbow Books, Chapter 3 and 4.1991.

[8] Syed Asad Hussain, Mehwish Fatima, "*Multilevel Classification of security concerns in cloud computing"* Applied Computing and Informatics, Vol. 13, pp.57-65, 2017.

[9] L. Ponemon, Ponemon 2014 SSH security Vulnerability Report.

[10] G. Pek, L. Buttayan," *A survey of security issues in hardware virtualization"*, ACM Comput. Surveys 45(3) pp.1-34, 2013.

[11] J. Idziorek, Exploiting Cloud Utility Models for Profit and Ruin Graduate Theses and Dissertations, Lowa State University, 2012.

[12] R. Bhadauria, S. Sanyal, "*Survey on Security issues in cloud computing ans associated mitigation techniques*", International Journal of Computer Applications, Vol.47, Issue.18, pp.47-66, 2012.

[13] Reed, A., C.Rezek, P.Simmonds, "*Security Guidance for critical Area of focus in cloud computing*", V3.1. Cloud Security Alliance(CSA).2011, pp.1-176.

[14] OWASP Top 10 Application Security Risks – 2017. Open Web Application Security Project (OWASP).

[15] Rathie, I. An Approach to Application Security. SANS Security Essentials White Paper, SANS Institute.

[16] OWASP Top 10 Backdoors, Open Web Application Security Project (OWASP).

[17] Rouse, M. Data Integrity, September 2005.

[18] Rouse, M. Authentication, February 2015.
Cloud Middleware informatiion avialable URL "https://www.techopedia.com/definition/30630/cloud-middleware-software".
Data Backup: Cloud Computing VS On-Site Options informatiion avialable URL "https://www.staples.com/content-hub/data-backup-cloud-computing-vs-on-site-options/"

[19] Farahzadi, A., P. Shams, "*Middleware Technologies for Cloud of Things – A Survey",* Digital Communications and Networks, Elsevier, 18 April 2017.

[20] Nolle, T. "*How to Address Security Risks Posed by Middleware Tools*", December 2014.

[21] Role of Cloud Computing Operating Systems. 8 March 2013.

[22] P. Herbert Raj, P. Jelciana "*Exploring security issues and solutions in cloud computing services"*, Cybernatics and information technologies, Vol.17, Issue.4, 2017.

[23] Chakravarty, A. Importance of the Network in Cloud Computing. 25 January 2012.

[24] Top 7 Network Attack Types in 2016. Calyptix Blog. 13 June 2016.

[25] Rouse, M. DNS Attack. July 2015.

[26] Jakimoski, K. "*Security Techniques for Data Protection in Cloud Computing*", International Journal of Grid and Distributed Computing, Vol. 9, 2016, No 1, pp. 49-56.

[27] J. Rezazadeh, R. Farahbakhsh. Middleware Technologies for Cloud of Things – A Survey. – Digital Communications and Networks, Elsevier, 2017.

[28] Minhaj Ahmad Khan, Khaled Salah, "*IoT Security: Review, blockchain solutions, and open challenges"*, Future Generation Systems, Elsevier, Vol. 82, pp.395-411, 2018.

Authors Profile

Dr. P. Madhubala pursued Ph.D. in Computer Science from Mother Teresa Women's University, kodaikanal in the year 2017. She is currently working as Head & Assistant Professor in PG & Research Department of Computer Science, Don Bosco College, Periyar University, Salem since 2007. She has published more than 13 research papers in reputed international journals and participated in conferences including IEEE and it's also available online. Her main research work focuses on Cloud Security and Privacy, Cryptography Algorithms, Network Security, and Big Data Analytics. She has 17 years of teaching experience and 5 years of Research Experience.

R. Denis pursued Bachelor of Science from Loyola College, Madras University and Master of Computer Applications from Thiruvalluvar University in the year 2009. He is currently pursuing Ph.D. and working as Assistant Professor in PG Department of Computer Science, Sacred Heart College since 2015. He has published more than 4 research papers in reputed international journals and presented papers in National and International conferences. His main research work focuses on Cloud Security and Privacy, Cryptography Algorithms, Big Data Analytics and Data Mining. He has 8 years of teaching experience.

