Global Scientific JOURNALS

GSJ: Volume 8, Issue 9, September 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

# Cyber Security Threats & Vulnerabilities in Cloud Computing and Security Measurements

Ken Lim Kim Son[1][2018-2020]

[1] AeU, Malaysia, MMU, Malaysia

kennpc@outlook.com

Faculty of School Of Information & Communication, AeU Malaysia (2018)
Prof. Dr. Titik Khawa Binti Abdul Rahman, titik.khawa@aeu.edu.my
Faculty Information Science and Technology, MMU Malaysia (2020)
Assoc. Prof. Ts. Dr. Md Shohel Sayeed, shohel.sayeed@mmu.edu.my
Dr. Nazrul, nazrul.muhaimin@mmu.edu.my

## Abstract

Cloud Computing is a way of computing, where the data is stored and retrieved online. The usage of cloud computing is increasing tremendously. Cloud Computing provides flexibility and proven delivery of IT services that benefits business and users. Today world with IoT spread widely, Cloud Computing is becoming a better way to run businesses. It has formed on conceptual and infrastructural basis for tomorrow's computing. It has changed the way of computing and the concept of computing resources. These new innovative, technical and pricing opportunities bring changes in the way the people live and the business operated. Cloud Computing systems give organizations company-wide access to computer applications through the cloud platform without getting hardware and software or software licenses. It makes cost-effective when company budgeting their IT Capex and Opex. This report provides a review of the cloud computing concept and its solution to address relevant security vulnerabilities and threats issues in cloud computer service and model.

**Keywords:** Cloud Computing, Threats, Vulnerabilities, Virtual Machine, Virtual Network, Security Measures, Governance, Compliance.

2

# 1 Introduction

Cloud computing has been defined as a technology model for enabling convenient, on-demand network access to a shared pool of configurable computing resources including servers, applications, network, storages and other computing services that can be rapidly provisioned and released with minimal management. The cloud computing is also a latest technology trend of information technology with computing services that provided to computers and other devices on-demand. According to a Gartner report (2011), cloud computing is the first top 10 technologies and trends that will be strategic for most organizations. The objective of cloud computing is to offer faster, flexibility in data storage, and network services with computing resources visualized as services and delivered over the Internet (Zhao G, et al., 2009, p.347-358). As per figure 1,the cloud is a distributed architecture with a centralized server and network resources offers potential of data management, ubiquitous access, self-service provisioning and virtualization. It aims for cost reduction, optimization, flexibility, acceleration of work development, agility, scalability, availability and ability to adapt to change and other computing service as per demand. To give a more efficient computing service to the people. According to a Gartner report (2011), cloud computing is the first top 10 technologies and trends that will be strategic for most organizations.

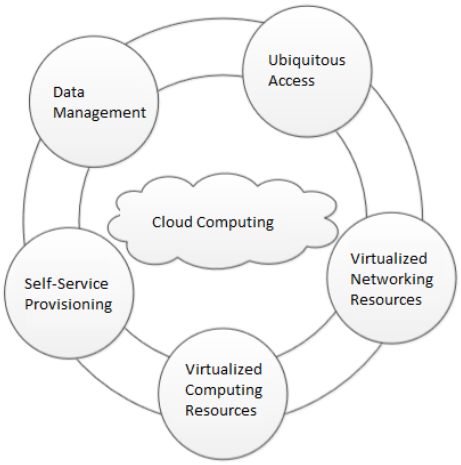


Figure 1: The discipline of cloud computing's elements. *(Source: Jose Moura & David Hutchison, 2016)*

Cloud computing are formed by leveraging many technologies including Web 2.0 Service, Service Oriented Architecture, virtualization to optimize the resources utilization and other technologies that provide a common platform for user's computing needs. The hardware systems and software systems and applications delivered as services over the Internet are formed up as a cloud computing. Cloud computing services are distributed from data canters sited all over the world and makes possible for its users to use the virtual resources via internet as per requirement.

Adopting cloud computing comes with benefits and barriers to adoption. The most significant barriers are security, privacy, legal and compliance issues. These barriers are due to the uncertainties on the security on cloud computing services including network on the cloud, infrastructure on the cloud, application on the cloud, data and information in the cloud, etc. Such uncertainty becomes a main concern of the information executives and companies that planning to embark to cloud platforms. The information executives and companies concerned about how to smoothly move their infrastructure, applications and data including sensitive data to the cloud. Security is their primary concern when transmitting data over the Internet and from the cloud systems to user's computers. Not only that, the security holds the data in the cloud and concerns relate to risk areas including data storage, internet that depends externals internet service providers, are the public dependency link, control access, multi-tenancy, security integration become a big question mark for them.

The different between on-premise infrastructure and network, cloud platform has its large-scale resource distribution, almost a complete virtualize platform and heterogeneous in the configuration by the cloud providers. The common security measurement place within on-premise infrastructure and network such as basic authentication, identity management and some form of authorization is no longer sufficiently or flexible for such security and interoperability in cloud computing platform. Hence, cloud computing is inheriting risks to organizations as compared to the existing on-premise infrastructure and network systems.

The security issues of cloud computing can be categories within three service models, security issues for Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS).

As far as SaaS is growing, the security for this model is a big question, e.g. if a virtual server that hold ten virtual machines has been hacked, the all ten machines are at risk. The identity management for this model is not mature because SaaS itself from the cloud providers are usually not able to integrate the SaaS platform. Due to software service sharing pool, the control level is limited (refer to figure 2) and the data secrecy may be weak too. Access from anywhere and anytime comes with risks, usually SaaS that enables it mobility, e.g., smartphone is not equipped with security features.

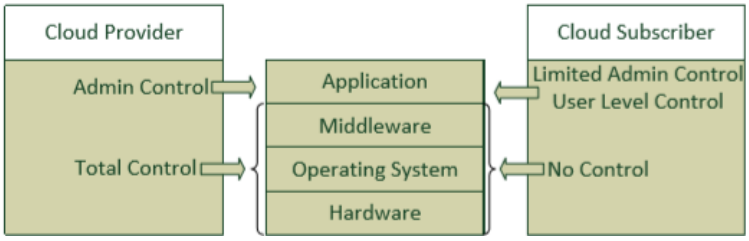


Figure 2: The control responsibilities for cloud provider and users in SaaS model. *(Source: Jose Moura & David Hutchison, 2016)*

4

Most organizations are concerned about the security implications associated with PaaS model and its data privileged access, distributed architectures and data location. According to Char Sample (2018), the challenge in encrypting the data is the main obstacle for PaaS model. Similarly, the control is limited in this cloud service especially at application and operating system layers.

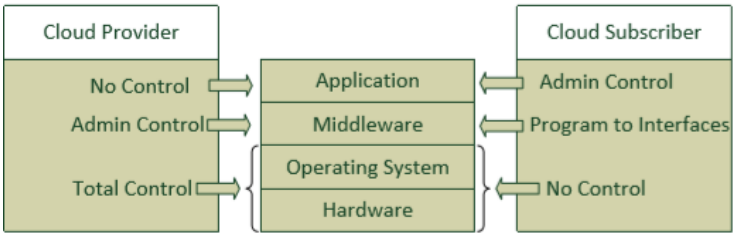


Figure 3: The control responsibilities for cloud provider and users in both PaaS and IaaS models. *(Source: Jose Moura & David Hutchison, 2016)*

Similarly, IaaS model exposes security issues. The concern over the control access, permission, database access rights that applied to application layers. Requirements like Data Lost Prevention (DLP), location tags, data access rules, robust delegation of administration might not be able to enable by the IaaS model. Multi-tenants sharing the same storage is the key concern in IaaS platform as well, the data may be commingled with data from other tenants.

Cloud computing services are categories as a public cloud and a private cloud. Cloud solutions like Microsoft Azure is an example of public cloud, anyone can access when service applications and storage that are being provided over the Internet (IJER, 2014, p.221). A private cloud is usually for internal usage and manage by in-house IT team or outsourced to a 3rd party that comprise resources sharing of computing services within organizations. A community cloud is another type of private cloud where a few organizations have similar requirements and sharing infrastructure so to realize some of the benefits of cloud computing.

Threats and vulnerabilities are common risks that lead to a misconduct in using/managing of information and data when some vulnerable flaws are exist in the systems that makes attacks to be successful. The finding of vulnerabilities and threat among three cloud models is discussed in this report including what cloud service models are affected by such threats and vulnerabilities. The report will address how these threats and vulnerabilities can be exploited to perform attacks, the relationship between threats and vulnerabilities and relevant countermeasures to address these issues within the cloud computing platforms.

5

## 2 Security Problems in Cloud Computing

Cloud computing is the provision of dynamically scalable and often virtualized resources as a service over the internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet. Cloud computing services often provide common business application online that are accessed from a web browser, while the software and data are stored on the servers over the Internet. In such services, the standardization work in the cloud computing has its interoperability issues, more critically the security issues including both vulnerability and threat that arise in the cloud services regardless in any SPI model. The purpose of this topic as a basis of the literature review is to analyse security issues in cloud computing with a brief description on the identification of vulnerabilities and threats. A number of security issues have been identified which are broadly categorized according to the area of interest in this study. The general. A relevant mitigations and security measurements are discussed in the report to provide homogeneity security issues that may lead to the attack and giving analysis of data collected from the literature review and security with its correctness actions that can be applied as practical actions to fix those gaps and issues that have been identified. The nature of cloud is combined with different services utilized of APIs and interfaces, model of consumption and resource allocation with provisioning, management, self-services, orchestrations for dynamic allocation of resources based on the giving systems and application input. These leads to probability and interoperability with limitations in regardless of any model in SPI within public cloud or private cloud. Both have significant results in limited control, configuration, security protections and availability variances (Jaydip Sen, 2014).

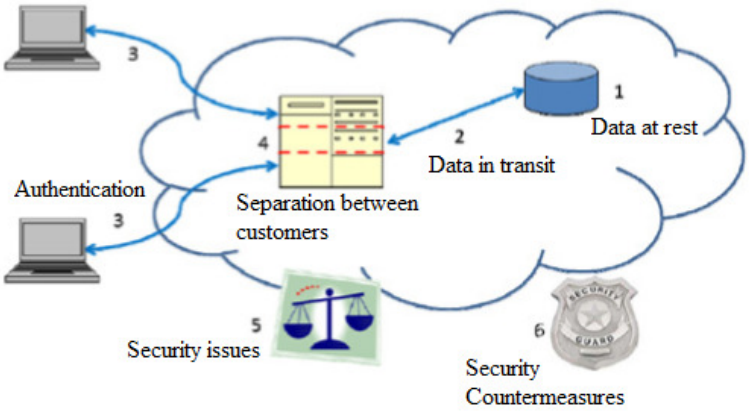


Figure 4: Areas of security concerns in cloud computing. *(Source: Jaydip Sen, 2014)*

There is substantial security attention of security vulnerabilities and threats that required security countermeasures to fix. The landscape of vulnerability and threat to security in cloud computing change as organizations move to the cloud. Cloud service

6

systems and applications including its data and content can be exploited and manifest in new and different ways other than through the old vectors that exist in the cloud computing. It is critical that to acknowledge that the cloud structure and its architectures in the SPI model can mitigate current security vulnerabilities and threats in order to make sure that cloud computing satisfies organizational security requirement. In this report, the examination is carried out for the vulnerabilities and threats against data and information asset residing in the different cloud service models, the security issues with the cloud and relevant considerations of attacks and availability issues and security countermeasures, as well as some sample of cloud security vulnerabilities and threats incident (Jaydip Sen, 2014, p.9).

7

## 3 Objective of Security Measures

The objective is to organize an investigation in an attempt to gain solution to the security issues in the cloud computing services. The key objective is also to find out the proper security measurements for cloud computing including architecture of the most flexible and secure cloud environment. Removes many of security headaches that come with infrastructure with relevant security measures with security solutions. Increasing security posture in the cloud including visibility into usage and resources which answering and validating the hypothesis of security vulnerabilities and threats that relate to the cloud services. A conceptual framework to address the objectives as part of the development of security issues identification that results in relevant security measurements.

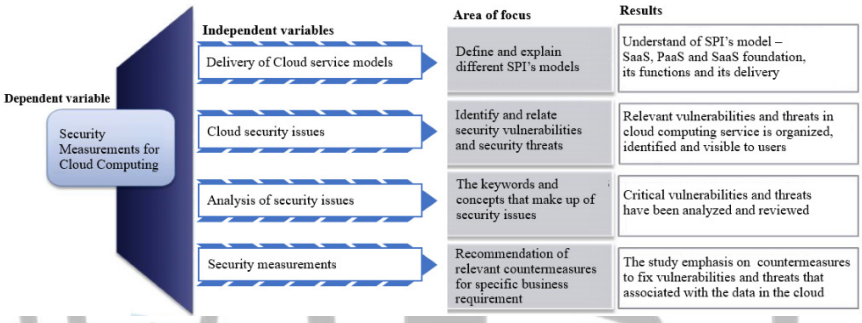


Figure 5: a conceptual framework of independent and dependent variables of security measurements for cloud computing (source: Larry Dragich, 2012).

8

# 4 Cloud Review

## 4.1 Cloud Service Models

The service model is also known as SPI model – Software, Platform and infrastructure models provides the following services

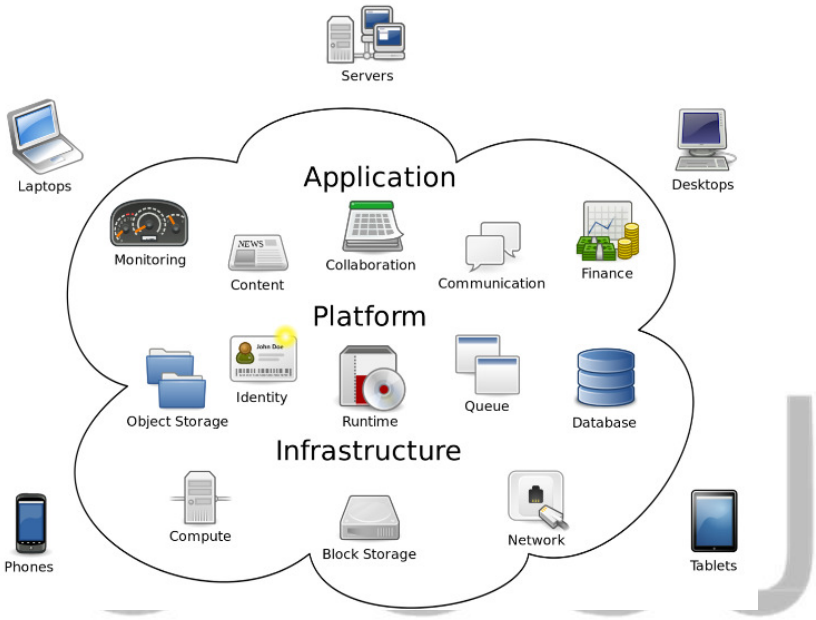


Figure 6: Cloud SPI models – SaaS for application layer, PaaS for platform layer and IaaS for infrastructure layer. (Source: 360logica.com, 2018)

a. SaaS allows customer's application as a service that running on a cloud infrastructure. Users can access the application over the Internet from their computers or devices, e.g. mobile device. In most cases, no upfront cost is needed for SaaS because the model offered as on-demand services. The cost to host applications is rathe low, customers only need to pay, managed and maintain the hosted applications, no underlying infrastructure cost is involved in this model including cost for servers, operating systems, network and storages. Some SaaS example is Salesforce, Microsoft Azure, Zoho Expenses, etc.

b. PaaS provides a platform for customers to build higher level service in the cloud without a local platform for servers and operating system. Customers would have the capability to deploy applications including systems and operating system support, software applications, and development to offer as a service. Customers can control or manage their application layers without managing the underlying cloud infrastructure including servers, network, storage, etc. in most cases, mixture of servers and operating systems are offered by PaaS providers, such as Linux server, MySQL, etc.

9

c. IaaS offers computing services and resources over the internet. The infrastructure is hosted in the cloud offer customer creation of virtual machines, install operating systems, deploy databases such as SQL and provision of storage for centralize repository server, backup and its retention. IaaS allows customers to access and manage their infrastructure to monitor performance, troubleshoot application issue, manage servers and applications load balance, manage firewalls, manage costs and manage data protection including disaster recovery and etc. Microsoft Azure services and Amazon AWS are the providers offer IaaS services.

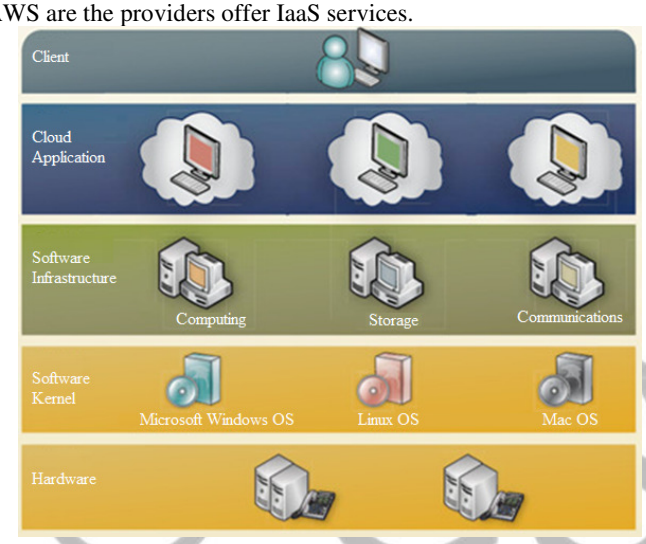


Figure 7: Cloud computing's architectural model. *(Source: Jaydip Sen, 2014)*

Understand of relationship and security challenges of these three cloud service models is critical. As shown in the figure 7, IaaS is the foundation of all cloud services with PaaS building upon IaaS and SaaS is built upon PaaS. In some cases, it is trusting that the built are on the other way around.

These three models are always relating to each other, a PaaS platform can be used to deploy IaaS and SaaS, an IaaS can be built as a PaaS and offered SaaS. Each model has its own inherent security flaws, when these models are dependant to each, numerous of security challenges can come simultaneously. These security issues lead to a number of security concern, including legal and compliance, risk management, access control for infrastructure, applications and network layers, and cloud provider dependant risks. For example, SaaS are depending on the cloud providers with minimal controls, IaaS with a common problem because cloud providers own the underlying infrastructure, the customers do not have insight/visibility of their infrastructure and they will not have transparency of the configuration since cloud providers keeping all the details and configurations.

10

The security result may be inconsistent for these models with a mixture of security protection related to the authenticity and credibility of the cloud services and cloud providers. Hence, trust is a big issue which raises security concerns to use cloud services. (Ryan & Falvy, 2012). Confusions may be created if an attack is happening especially cloud computing service is shared amongst customers.

### 4.2 SaaS Security Issues

The model is typically on-demand services, such as CRM and ERP applications (Ju J, et al., 2010, p.384-387), email and instant messaging, conferencing, etc. customers would have less visibility of the security of the services which also the least control among the three-delivery model in the cloud. Due to less visibility and control, it exposes security risks and concerns over the adoption of SaaS applications and services.

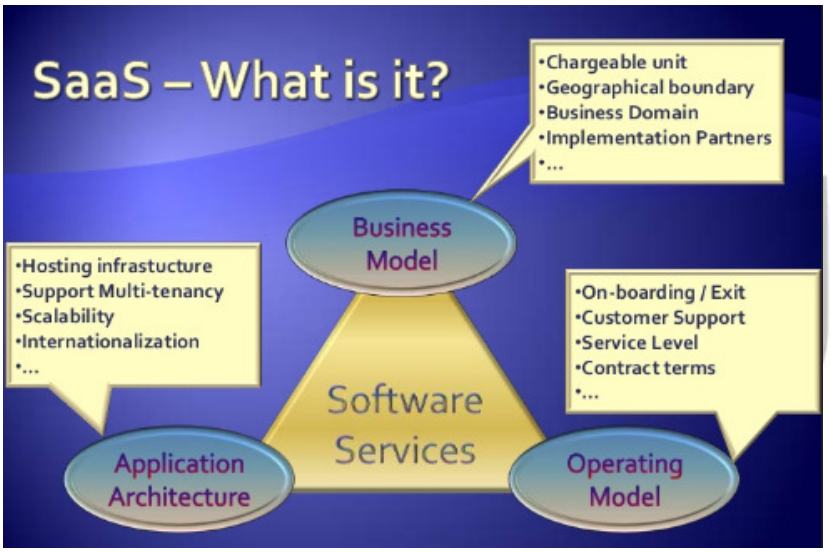


Figure 8: Business model in SaaS delivery services. *(Source: Kannan Subbiah, 2012)*

The business model for software service includes hosting infrastructure, support multi-tenancy, scalability and internationalization. These services are discussed in the following sub-chapters which cover the application security, multi-tenancy, data security and accessibility to the mentioned software services.

a. Application Security

Applications can quickly change the world, empower business and connect users around the globe. However, without proper security built-in during development these applications can be compromised by attackers to put user data at risk, cripple user trust with the application, and result in financial losses or regulatory fines.

Likewise, applications from the cloud computing services create certain vulnerabilities because these applications usually are delivered through the Internet (Ritinghouse, Jw, Ransome JF, Jensen M, et al., 2009, p.109-116). Users used it via web browsers, as such some flaws in the web applications are expected. Web browsers are always the most favourite tool that used by attackers to initiate an attack to compromise users' computers. Attackers used the web to perform attach, such as stealing or grapping of sensitive data (Owen D, 2010). In the past, application in the local network are not effectively protected from attacks, but applications in the cloud computing, such as SaaS platform are required new security approaches (Subashini S, Kavitha V, 2010) to protect it. E.g. developer assume some parts of applications can't be seen or tampered with or invoked by the users, the impact led to access control failure. Access control including authorized data access and access to privileged functionality.

Application hosting in the cloud is permitted to access by authorized users including HTTP and HTTP traffic to permit services. But a typical firewall does not protect an application, it protects traffic and access may be logged but the details of application and it traffics are rarely investigated because many malicious activities do not how 'abnormal' traffic or behaviour. Similarly, antivirus software installed on the client machine detects system level issues, not the security issues detected from the browser. Up to a certain extent, a compromise application may operate normally. There are more security issues for applications, e.g. 3rd party application linked to business site. One of the best practices to begin the application protection is follow the identified top ten security threats that define in the OWASP.

b. Multi-tenancy

In SaaS model, multi-tenants are sharing the same underlying infrastructure and same resources including software services. In this case, the administration of service and support is also be shared. This is because of cost deduction, cost sharing and resource sharing among tenants. Sharing of same application stack which multi-tenant's data are stored in the same database and the database can be moved on an unencrypted network device and managed by common application process (OWASP, 2018), as such, it is a challenge for logical security in the application to split one tenant's users from others (OWASP, 2018). The sharing of underlying infrastructure and software services come to certain security risk including shared services could become a single point of failure, change control may not be able to co-ordinated, weaker logical security control between tenants, which malicious or ignorant tenants may decrease the security posture of other tenants. Sometimes, a single instance application or database serves multi-tenants (Chong F, et al., 2011), as such the risk of data leakage between tenants is high. As suggested by Bezemer C-P (2010), security policies are required to make sure that different customer's data are kept separate.

If attacker or hackers can compromise the application and database, chances of getting or stealing of data of hundreds of different customers who stored their application and database in the cloud is high. Majority multi-tenant cloud computing services are created by web 2.0 which may pose in new user interfaces and lack of security features. E.g. attacker initiated an attack by using WebGoat v5.4. SQL injection attacks that

represent a serious threat to any database-driven application that shared among tenant. Such attack methods are easy to learn and successfully compromise the system. The damaged causes can range from considerable to complete system compromise for multiple users. Despite these risks, an incredible number of systems on the internet sharing among users are susceptible to this form of attack.

c. Data Security

A key concern for technology is the data security. It is one of the major challenges for SaaS model which customers/users are relying on the cloud provider to have a proper security and security baselines when embarking to the cloud services. Data is always in plaintext format when it is stored. When data is stored in plaintext formation, hackers can obtain access to information, collecting information about your systems, access personal data for ID theft, to commit user transaction fraud more easily. Hence, it is critical that SaaS provider to provide the security measurement for the data that is being stored and processed in the cloud (Ju J, et al., 2010, p. 384-387). Backing up and recovering of data in the cloud expose to security challenges (Subashini S, Kavitha, 2010) when facilitate the backup for recovery in an event of disaster recovery is needed. Some cloud service providers sub-contract the data protection strategy to the 3rd party service providers in order to have backup and recovery process in place to meet the audit and business continuity purposes, such sub-method raise security concerns as well because the cloud provider may have lost visibility to the data that is being backed up by the 3rd party service providers.

The process of compliances is complex in the SaaS model, the data is stored in the cloud provider's data centres, some cloud service providers do not envision the compliance standard with its regulations in the cloud computing (Rittinghous, JW, 2009) which led to security and privacy issues that should be enforced by the cloud provider. It is always good practice to sanitize all input data, especially data that will used in OS command, application parameters and scripts, and database queries, as such, not only it is easily instigated, it is also a threat that, with a little common-sense and forethought, can easily be prevented even if the threat like SQL injection, cross-scripting attacks have been prevented in some other manner.

d. Data Accessibility

Cloud computing offers accessibility in convenience and makes access from anywhere and anytime from any Internet connected devices including mobile connected in the public WIFI hotspot and home connected computers. As such it exposes certain security risks and challenges. According to the Cloud Security Alliance (2012), today's mobile computing and the top ten threats and vulnerabilities including insecure Wi-Fi network especially open hotspots, information stealing malware are found in the operating system in any IoT device, proximity-based hacking, official applications and non-secure marketplaces. A report by Media Access Australia (2014), acknowledged that cloud-based services have challenges in accessibility because both application and web services offer different cloud accessibility features, such feature is for easy to use way and simplicity when it comes to access, hence, it exposes to weak security protection.

13

### 4.3 PaaS Security Issues

This model of cloud computing offered applications over the Internet without on-premise hardware, storages and software. PaaS application security consist of security for the platform and security of the applications that deployed on the platform. PaaS providers are responsible for securing the platform software stack. The security includes databases engine runs the applications. The security issues are the main roadblock for delaying of IT modernization. Refer to figure 8d c, to the finding by Cioinsight (2018), the biggest barrier of PaaS adaption is the security issues and operational risks (43%) for PaaS platform as compared to the failure to demonstrate needed ROI (39%), lack of budget (49%) and inability to recognise the value of PaaS and related services (32%).

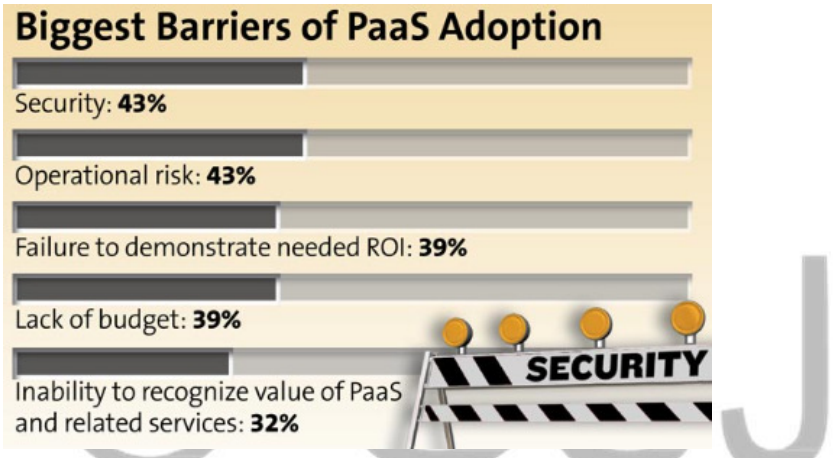


Figure 9: IT modernization is delayed by security issues. *(Source: Cioinsight, 2018) Cioinght, 2018. IT modernization delayed by security issues. Available at*

The common PaaS security issues and challenges are described as follow:

a. 3rd Party Relationship

PaaS offers 3rd party web services. The services component including mashup that mix single element of sources that inherits security issues such as network security, data security, etc. Users on a PaaS platform are relying on security in web services, 3rd party services and development tools, thus users are not getting grips with 3rd party data and network security underlying in the PaaS platform.

b. Development Life Cycle

Setting up application security is a big challenge for developers in the development of applications. The speed at which application will change in the cloud will affect both security development in application and system development life cycle (Ritighouse, JW, 2009).

14

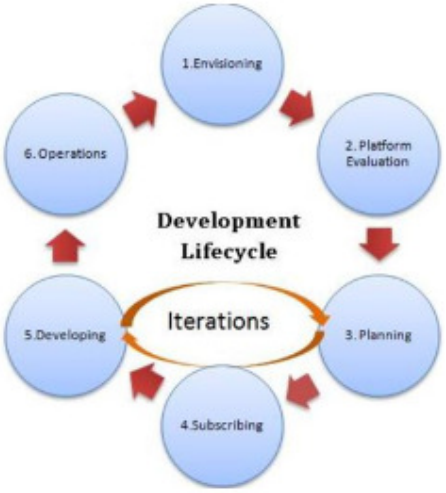


Figure 10: Cloud service model's Development Lifecycle. *(Source: Cloudyinnashvile.com, 2018)*

The iteration has never stopped for platform development lifecycle (DLC). Such DLC is applicable to all cloud service models. Frequently upgrade of PaaS by developers become an essential for application development processes and make it flexible to keep up with technology changes (Ertaul L, Singhal S, 2010). Certainly, such changes increase security issues and can compromise the security of the applications. Other than development, data stores on different location with different legal regimes can compromise its security and data privacy, moreover if the data is stored in inappropriate locations, legal issues may arise.

c. Underlying Infrastructure Security

In PaaS model, it offers development tools to create SaaS applications as both use multitenant architecture for multiple and concurrent users sharing the same platform and application software. In this model, developers are responsible for safeguarding the underlying infrastructure and the application services (Chandramouli R, Mell P, 2010). In most cases, developers would have full control on the application security, but they cannot assure that the development tools are secured. However, there is very little literature about security issues for this model.

### 4.4 IaaS Security Issues

IaaS is having standard services for computing capabilities, including servers, basic storage, network components, data centre facilities and virtualizations. IaaS provides access various infrastructure over the Internet. Customers can have full visibility, better control and management of the resources they have in the IaaS platform. They can configure security policies and control software running in the virtual instances, but the

underlying infrastructure, network, rack capacity and storages to setup as a service before setting up own infrastructure is always controlled by the cloud providers.

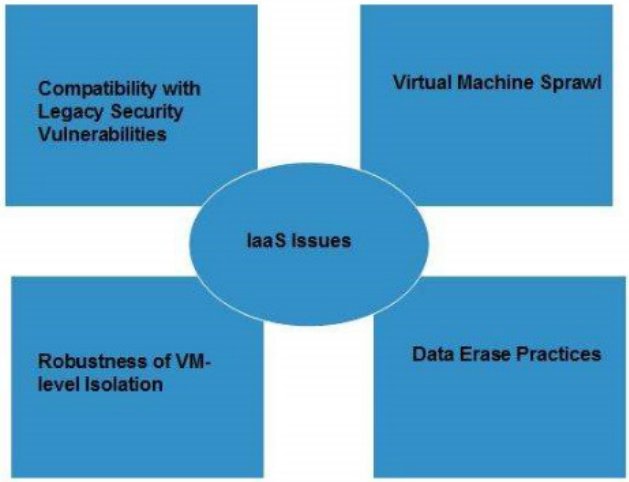


Figure 11: Some common IaaS security issues. *(Source: tutoriaspoint.com, 2018)*

The most common in this service model is the vulnerability and threat found in the underlying infrastructure - virtualization technology.

a. **Virtualization**

Virtualization is a critical component for cloud service models. It exposes the systems to the current attack vectors and new vectors or new source of attack. There are many security issues that associated with the three models of cloud computing, especially IaaS platform that is having a greater challenge. Virtual machine's vulnerabilities include no restriction in the provisioning of virtual resources, no control for virtual machine creation, and IP addresses that are visible in the cloud making attacker simply map the targeted virtual machine that is stored within the cloud. According to Jennie Susan Reuben (2007) on his survey on virtual machine security, the most challenge issues are virtualization in the IaaS platform that actually adds more points of entry and more interconnection complexity. For example, the virtual machine's images, there isn't control of virtual machine's images in the cloud repository because these image data are dormant artefacts data, it cannot be patched or secured. There are two boundaries in the virtualization, including the physical system as a host machine of virtual machines and virtual instances of various systems. The focus of this study detailing the challenges in virtualization that exist in the cloud computing is discussed in the next topic.

**b. Virtual Machine Monitor**

The virtual machine monitor (VMM) is a kernel-mode driver running in the virtual host systems. It acts a firewall in between virtual machines and virtual host systems with its limited functionality. The VMM itself entail security flaws since it functions is to control and monitor its virtual machines (Jenni Susan Reuben JS, 2007). VMM has access to the physical computer processor and manages resources between the two

environments, including migrating virtual machines between physical servers, preventing malicious or poorly designed applications running in a guest operating system from requesting excessive hardware resources from the host operating system (Microsoft TechNet, 2018) and for maintenance purposes including fault tolerance and load balancing (Cloud Security Alliance, 2010). Such tool for monitoring tend to expose to certain security issues, including attacker can compromise the migration tool (Wesam Dawoud W, el, 2010) in the VMM and copy a virtual machine to the malicious server. As such exposes the content of the specific virtual machine which can compromise the VM's data integrity and confidentiality.

**c. Shared Resource**

A virtual host system runs multiple virtual machines, it allocates to each virtual machine a share of the physical resources. With the default resource allocation settings, all virtual machines associated with the same host receive an equal share of CPU, memory, I/O and others, as such the security of each virtual machine may decrease due to the resources sharing between virtual machines. Prior to such sharing, scavenging of data is sometime is not completely performed. As such, it leads to potential of data steal and data recover by attackers to initiate attack activities. Other virtual machines information and shared resources can be inferred by a malicious virtual machine without the required of compromising the hypervisor (Keiko Hashizume, et al., 2013). There are potential risks that compromise a virtual machine hypervisor which make the virtual machine become a primary target. The security module and its define rules of virtual machine monitoring can be bypassed when two virtual machines communicated via covert channels (Ranjith Poliyedath, et al., 2012). Attackers can infer information of other virtual machines through a malicious virtual machine that can observe its shared resourced without notification by its virtual machine monitor.

**d. Virtual Machine Image/Template Data Store**

In IaaS model, virtual machines can be built as a template that containing its configuration, including its baseline security configuration to create virtual machine instances. The templates can be used as a fundamental to the security of the cloud (Jinpeng Wei, et al., 2009). A virtual machine can be built from the scratch or can be created using the template or image created and stored in the virtual host system's data store. For example. Microsoft Azure, offer a public template/image in the Azure repository where authenticate customers can retrieve the template/image, attackers who have a valid account can store images/templates that containing malicious script/code such as Backdoors code and Trojan Horse script into the repository compromise the cloud system (Bernd Grobauer, et al., 2011; Mohamed A. Morsy, et al., 2010; Wayne A Jansen, 2011). Other users/customers who are in the same cloud platform, their virtual machines will be infected with the hidden malicious script/code. The virtual machine application itself is known as weak in security, hence the data leakage problem sometime happens. (Grobauer B, et al., 2011). When creating a virtual machine template or image, confidential information such as user credential and password or cryptographic key such as both encrypt and decrypt keys are included while the template or image is being created. When the virtual host system holding the virtual machine templates/images is offline, it is hard to patch with security vulnerability because the virtual machine

templates/images are dormant artefact that difficult to patch when they are offline (Ken Owens, 2013).

### e. Rollback of Virtual Machine

The virtual host systems to function for proactive maintenance, allowing users to take snapshot of the virtual machine's current state before any configure is tried on the virtual system. With virtual snapshot function, it enables rollback function which reverts changes made by a user to roll back to the previous state when its snapshot was captured (Viveknayyar, 2013). Rollback function will work when the user is logged off from the virtual machine. However, the rollback function exposes to security vulnerabilities that were patched or the accounts or password that has been enabled in the previous point of virtual machines. Such rollback can result in the propagation of virtual machine's settings and configurations errors and vulnerabilities. (Tal Carfinkel & Mendel Roseblum, 2005).

### f. Virtual Machine Life Cycle

A critical consideration on the virtual machine life cycle. The life cycle helps in overseeing the virtual system implementation, delivery, operation and maintenance of virtual machine instances over the course of VM's existence. Virtual machines were designed for conveniences, it can be moved and migrated through online or even in suspended mode that make the system hard to detect hidden vulnerability. Virtual machines can be vulnerable (Mohamed A. Morsy, et al., 2010) even the machine is in offline mode which a virtual machine can be instantiated with a template or an image that contain script or malicious code to inject of the code to another virtual machine in the process of setup

### g. Virtual Network

Virtual network computing enables IT provision to have a section to launch computing resources in a virtual network that you define. Users have complete control over the virtual networking environment, including configure network settings, routing settings, IP addresses, sub-net mask configuration, etc. However, cloud computing is resource pooling for different tenants, hence network components are shared between them. As such, there are security risks of virtual network vulnerabilities is existed. A potential cross-tenant attacks by attacker for such resource sharing (Gronauer B, et al., 2011, p50-57). The interconnectivity between virtual networks increases the security challenge in the cloud computing (Hanqian Wu, et al., 2010). Assigning a dedicated physical network to the virtual machine to have interlinked between the virtual machine and virtual host is more secure. However, most hypervisor uses virtual networks to link virtual machines to have direct connection and more efficient in term of managing the virtual machines. But for such interlink and direct virtual network connectivity, it creates potential security attacks where an attacker can use the spoofing and the sniffing techniques to initiate an attack to the virtual machines in such virtual network (Jenni Susan Reuben, 2007; Gao Xiaopeng, et al., 2010).

18

# 5 ANALYSIS & DISCUSSION

The cloud computing is categorized in the different models are generally for applications and infrastructure that are extended to be accessible through the internet which has received increasing interest from enterprise since its inception (Rania El-Gazzar, 2014). But there are strong technical security arguments in favour of cloud computing regardless of any of the service model. The literature review explained some of the security issues related to the cloud computing services including cloud users face serious security issues before they can decide to adopt the cloud computing and when they are already stepping into the cloud computing. However, the review indicates that the security issue that exists in the cloud computing seem is unavoidable, the challenges are getting plenty of attention. The adoption of cloud computing is moving fast and is hot in the market, but security offering in the cloud computing services is somewhat foggy, especially when the different cloud service provider offers different security or little to no security making the selection of cloud service become tricky.

The results of finding relevant vulnerabilities and threats that associated with data and underlying infrastructure in the cloud and all cloud service models is listed in the table 2 and the table 3 with its description. The effort emphasis on these are given a brief description or security measurements and a practical action to mitigate these security issues in the cloud computing.

## 5.1 Security Issues Analysis

This report highlights of analysis for an existing threat and vulnerability in the cloud, each of the security issue is explained with description. Such analysis gives an overview about the vulnerabilities that was found in the cloud service models and which models are being affected by these vulnerabilities. APIs and interfaces (V1) that are commonly used in cloud services for variety computing requirement, including to integrating cloud instances using third-party tools and interconnect for cloud instance and on-premise system. However, a report by Cloud Security Alliance (CSA) reported that insecure APIs and interfaces are the top threats to cloud computing (Dave Shackleford, 2016).

Table 2: Security vulnerabilities in cloud computing services. (Source: Keiko Hashizume, et al., 2013).

| ID | Vulnerabilities | Description |
|---|---|---|
| V1 | Insecure APIs | Such APIs including HTTP, REST and XML in the cloud computing are being generated for integration with different systems and application. These APIs is being used in all cloud service models. Although cloud services can be accessed, but these APIs are tending to have security issues, including weak credential, no authorization verification and no validation of data input. Such APIs always being updated due to the bugs found in the application (Nilanjan Dey, 2009). |

19

| | | |
|---|---|---|
| V2 | Unlimited resources allocation | This either the service was over provisioned or under provisioned (Daniele Chatteddu and Giles Hogben, 2009) over the SPI model. Once onboard to the cloud network without a proper data and resource sizing, such issue is always happening. As such, resource usage is increasing and lead to inaccuracy of resource allocation, lost control due to data undersize or oversize and costs to pay for the additional resources. |
| V3 | Data vulnerabilities | The most critical security issue that applies in all cloud service models. This includes, no separation of data (Veiga J, 2009); Data are collocated with different owner including competitors or even the intruders; Data are stored in different jurisdictions that have different laws (Ertaul, et al., 2010); Data stored in the cloud cannot be deleted or removed or rather cannot be deleted or removed thoroughly (Ertaul et al, 2010); Data protection including backup and restore are done by the third-party providers (Townsend, 2009); The location to store the data is not known or not available to users (Wayne A Jansen, 2011) and data is stored, transferred and processed in clear plain text (Jisa, 2018). |
| V4 | VM's vulnerabilities | This commonly happen in IaaS model and sometime PaaS platform that rely on virtual systems. The reason includes; No restriction in provisioning and decommissioning of resource with virtual machines (Vic Winkler, 2011); Possible covert channels in colocation of virtual machines (Ranjith Poliyedath, 2012); No control for virtual machine migration – vMotion that allows migrations from a host server to another. This is due of load balancing, fault tolerance, snapshots and maintenance requirements (Wesam Dawoud, et al., 2010).<br>The flexibility of using the snapshot function in virtualization can lead to data leakage. No control in rollback also leads to reset vulnerabilities as virtual machines can be backed to the previous state, it causes patches applied after previous state missing.<br>Virtual machines' IP addresses are visible in the cloud, attackers can map the targeted VM that is stored within the cloud (Thomas Ristenpart, et al., 2009). |
| V5 | VM templates' vulnerabilities | No control of virtual machine's templates in the cloud repository (Mohamd A. Morsy, 2010). Templates are dormant artefacts, hence, it cannot be patched (Tal Garfinkel and Mendel Rosenblum, 2005). |
| V6 | Hypervisor's vulnerabilities | Hypervisors code is complex and flexible configuration of hypervisors can be exploited. |

20

| | | |
|---|---|---|
| V7 | Virtual network's vulnerabilities | A several VMs are sharing the same virtual networks/bridges (Hanqian Wu, et al., 2010). |
| V8 | Virtual machine hoping and escape | Hypervisor can be exploited and have write access to the virtual machine so to take control of the underlying systems and network systems especially when sharing mechanism is one of the feature in virtualization. A virtual machine can escape from the virtualize sandbox and gain access to the hypervisor (Dejan Lukan, 2014). |

The table 2 shows that the virtualization is the most critical technology that may get attacked. Unlimited resource allocation (V2) refers to the virtual machine allocation that spinning off or provision of a virtual machine on a physical host in which the virtual machine comes with predefined CPU (vCPU), memory (vMEM), storage (Data Store), VLAN and IP addresses (Han Ping Fung, 2017). Provisioning of resources can go beyond IaaS hardware resources, which including PaaS and SaaS, etc. such allocation could lead into human error if resources sizing is not properly calculated or properly assign to its limit and control.

Analysis that conducted by Dejan Lukan (2014) show that 90% of the company's operational model is based on cloud services which they have worry free about the security. However, data vulnerabilities (V3) are the most critical security issues applies in all cloud services. In this case, some cloud providers don't have a good security model in place specifically for data protection. As such, regardless whether the data is visible or non-visible, such weaknesses in protecting data can be exploited by the attacker.

Vulnerability in virtual machines (V4) is a common issue found within the infrastructure system because some systems that running in virtually functions are run as a non-privileged user with certain admin access rights. As such virtual machine contains such vulnerabilities could allow remote attacker to execute code on the vulnerable system (Microsoft, 2002) to perform stealing of privilege account and malformed of data to cause application fail to run. A feasible feature to migrate the virtual machine can lead to potential data leakage. Such flexibility including snapshot, migration function, rollback, etc. can be the targeted of exploiting by intended attackers.

VM's template/image (V5) are dormant artefacts, since no patching is available for such templates and images, this vulnerability could be exploited or copied or transferred by unknown users from the data repository.

According to Neil MacDonald (2011), hypervisors are vulnerable (V6). Hypervisor is a software, it was written by someone including Microsoft, VMWare, etc. As such, hypervisor tend can be complex and flexible in configuration, and all these hypervisors would have vulnerabilities. Such vulnerability in hypervisor would cause breaches in virtualization platform and represent a worst-case scenario, e.g. IT operation failure.

Network for virtualization system is sharing the same network and configuration, vulnerability in virtual network (V7) including access or interfere with traffic that belongs to others network. As such, network violation happens (Leonardo Richter Bays, 2015), and can be targeted by denial of service attack. These vulnerabilities impact the virtual network's integrity and confidentiality (Leonardo Richter Bays, et al., 2015).

As per a study by Neil MacDonald (2011), 35% of the virtualization vulnerabilities resulted in an escape to the hypervisor. As mentioned in virtual machine hoping and escape (V8), the hypervisor can be exploited to write access due to the virtual system sharing mechanism. On top of hypervisor, a physical virtual host can host multiple virtual machines, the hypervisor can be exploited remotely by an attacker. A virtual machine can escape from the virtualised sandbox from a virtual host or machine itself. The objective is to gain access to the hypervisor and consequently all the VMs. However, such escape does not affect the virtual host's operating system.

The above vulnerabilities in the virtualization are the security issues that impact the security of the cloud computing and its underlying platform. Some of these vulnerabilities due to;

- Inadequate hiring screening and practices (Cloud Security Alliance, 2010) which some cloud providers never perform background checks of their staffs. The staff that as cloud administrator would have full access to the cloud data.
- Inadequate customers background checks because cloud providers usually never do that since customers is their source of business and as such, anyone can subscribe to cloud easily. Attackers can conduct malicious activity to the apocryphal accounts without being checked.
- Inadequate in security knowledge because not everyone is good at security or having awareness about the importance of security. As such, it has a major impact on the cloud computing since many people interacting with each other in the cloud including vendors, customers, suppliers, end users or any third-party organizations.

Cloud computing itself is flexible for demand usage, most of the cloud providers has integrate or build up certain security for protection, however, the philosophy is while improving cloud services, it also introduced threats (Galen Gruman, 2008).

The following table 3 gives an overview of threats that exist in the cloud computing.

Table 3: Security threats in cloud computing services. (Source: Keiko Hashizume, et al., 2013)

| ID | Threats | Description |
|---|---|---|
| T1 | Credential hijacks | A common threat that always discovered by forensic investigation. This applies to all SPI model. Account or service account can be hijacked by an attacker for them to |

22

| | | |
|---|---|---|
| | | perform malicious activities so to get access to the resources they want. These accounts are usually stored in the systems insecurely and commonly stored in plain text format. These accounts can also be used in social engineering or redirect of transactions including credit card transaction. |
| T2 | Scavenging of data | Data is not able to delete or remove, attackers can steal those data or recover it (Tim Mather, et al., 2009) for them to initiate attack activities. |
| T3 | Data leakage | Data is transferred and processed especially when data are stored, transferred and processed in a clear plaint text format. As such, it leads to a high potential of information leakage. |
| T4 | Data manipulation | Attackers use the techniques like command and control, SQL injection, cross-scripting and object redirections to manipulate the data that sent from the application component to the central server that store the core application systems. |
| T5 | Denial of Services (DoS) | Attackers can flood the system using attack like ping of death, SYN flood, etc. to any system or application that resided in any cloud model to make the system and application data become unavailable since system cannot satisfy requester especially legitimate users since data is unavailable. |
| T6 | No security protection while migrating virtual machine | Platform service and infrastructure service are favourable for testing of virtual machine migration and actual virtual machine migration. Online migration (vMotion) of VMs exposes the VM's content and state file to the network. |
| T7 | Malicious virtual machine creation | When virtual machine is sitting in the infrastructure service platform, attackers can inject malicious codes like backdoor script and trojans in the public repository by using a valid account (Bernd Grobauer, et al., 2011). |
| T8 | Virtual network spoofing and sniffing | Similarly, in IaaS platform, malicious virtual machines can exploit the virtual network using ARP spoofing and flooding sync command and control. As such, to redirect traffic and packet from one virtual machine to another (Jennie Susan Reuben, 2007). |

Credentials hijacking (T1) which accounts, and services have been hijacked and exposed to the following threats highlighted in figure 13.

23

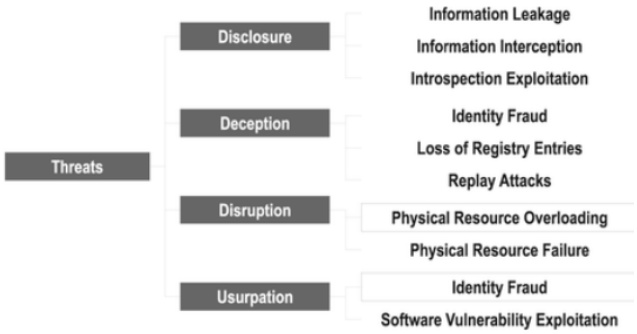


Figure 13: Relevant threats that lead into different security issues that violate constraints on systems and application in the cloud. (Source: Leonardo Richter Bays, 2015)

Cloud computing is web-based technology. Hence, there are many computational activities are conducted in the cloud including transfer and store of data. The analysis shows that data scavenging threats (T2) associated with data being stored and processed remotely, so when the data cannot be deleted or removed, the data can be recovered by unintended users/attackers.

Data scavenging is the technique of piecing information that was found from in bits of data. Attackers can retrieve/recover the data is data is not completed removed or deleted to perform laboratory attacks and keyboard attacks (Shilpi Chandna, et al., 2014, p.107).

Data leakage (T3) is possible from the cloud computing itself since the underlying infrastructure is virtualization system, which data can be leaked from a virtual machine to another when data is being transferred without protection like encryption. Attackers may grasp these data including sensitive data for financial gain. According to the analysis conducted by Prof. Sushimumar (2015) reported that more than 51% of data leakages were resulted from global attacks and 43% of leakages were due to accidental events. Such percentage of global attack is increasing year after year.

Manipulation of data (T4) which attackers used injection technique, command and control, etc. for changing of data. Such manipulation including manipulating of financial figure fraudulent, trends in sales data theft, etc.

Denial-of-service (T5) is blocking a specific service from its intended usage. Attackers flood the system and network, making the system and network is inaccessible. There are many ways of DoS attack can be launched by attackers, including application layer floods by a buffer overflow in a specific application, malformed its data, exploited race condition in multi-threaded systems (AppliCure), injection attacks, excessive file send to a system, and etc.

24

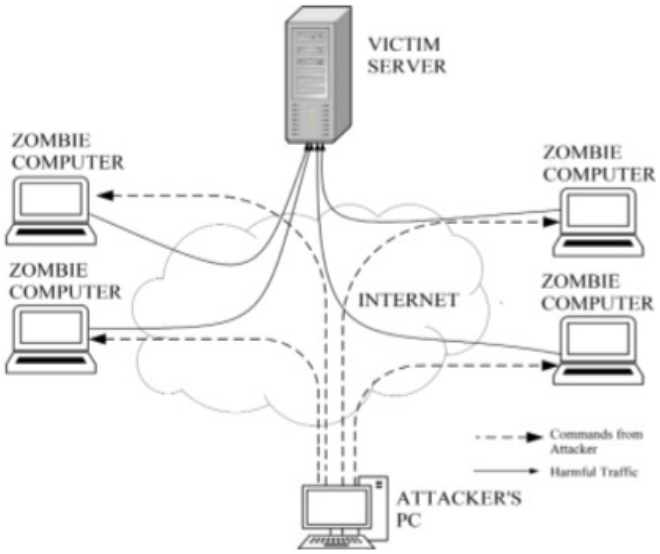


Figure 14: An overview of DoS/DDoS attack over the cloud computing. (Source: Iqra Sattar, et al., 2015).

Such attack is becoming a fast-growing concern (Elmustafa and Rasha, 2015). The severity of such attack is high with a magnitude of loss. Such attack also extended to Distributed Denial-of-Service, which does more damages in service availability (Elmustafa and Rasha, 2015).

Insecure in protecting of VM migration (T6) which migration can be performed with a virtual host to another or over the Internet insecurely. In this process, a specific VM is the only application handle by the hypervisor, which hypervisor cannot ensure the security during the migration process (Santosh Kumar Majhi, 2016). Such migration exposes system's content and state file to the network and to the intended users/hackers.

Malicious VM creation (T7) is one of the threat that allow attackers can initiate the data access freely (Wesam Dawoud, et al., 2010) when migrating of a VM, transfer or snapshot the VM to the untrusted host (Tal Garfinkel, 2005) and perform the flooding sync attack to disrupt the VM when creating and migrating several VMs concurrently. An analysis conducted by a security consulting firm revealed that malicious in a VMware virtual disk configuration file would allow attackers to access the file system using the fuzzing technique on the virtual host machine to gain access to critical files (Joseph Granneman, 2012).

25

### 5.2 Analyze of Open Standards in Cloud Computing

Cloud computing is deployed in open standards, including open source software. This is critical to the foundation of cloud computing growth. Security issues remained as the main concern for organizations to onboard to the cloud. These contentious issues further delay the cloud adoption. Cloud computing is also referring to green in computing, which no on-premise infrastructure is required other than power and capacity saving. However, the study of such green computing it lacks substantial evidence to support the statement because going green doesn't anything for security and protection initiative for data stored in the cloud. Cloud consumer needs not to purchase anything including security protection and monitoring other than paying a predictable subscription for the system and application services running in the cloud. Cloud consumers pay for what they access and use. The analysis shows that many information technology divisions spent a signification of time and effort for infrastructure and application upgrade which some projects didn't really add value to the business process, nor add security posture and meet its purpose on return on investment. Onboard to the cloud computing helps IT get rid of time and effort for the upgrade. However, although onboard to the cloud allowing IT to focus on strategic activities that has a greater impact on the business, but onboard to the cloud is always coming with security and risk concerns. The consideration for any cloud service model needs reliability, which improve improves through the use of multiple redundant sites, it makes cloud computing suitable for business continuity and disaster recovery. Nonetheless, many major cloud computing services have suffered outages, and IT and business managers can at times do little when they are affected. Security could improve due to centralization of data, increased security-focused resources, etc., but the concerns can persist about loss of control over certain sensitive data, and the lack of security for system kernels. Maintenance cloud computing applications are easier to maintain, since they don't have to be installed on each user's computer. They are easier to support and to improve since the changes reach the clients instantly.

### 5.3 Security Countermeasures

The cloud computing service means data and applications can be resided everywhere. As a result, organizations are working with a security multitude of systems and applications in the cloud including underlying infrastructure, software and application and devices used by cloud consumers/users to access data. The figure 15 illustrates relevant security countermeasures that can be considered to fix security issues found in the cloud systems and applications.

26

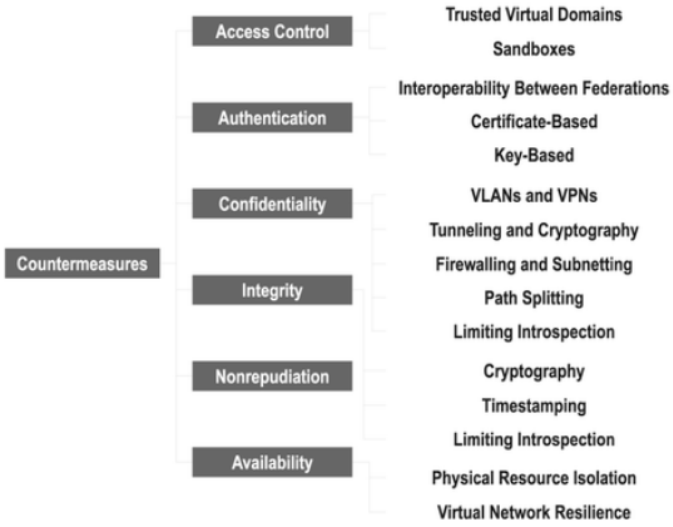


Figure 15: Relevant security countermeasures to fix different security issues. (Source: Leonardo Richter Bays, 2015)

And on top of above, relevant security measures that can be conceptually and practically apply to fix those threats and vulnerabilities that have been identified in the cloud computing services is highlighted in the following;

**a. Security countermeasures for insecure APIs and interfaces**

As mentioned earlier in the security analysis, APIs and interfaces are commonly used for cloud instance, cloud application, tools and on-premises system integration and interconnect. Most of the cloud service providers managing the cloud service require having security mechanisms like transport security which through a secured global API gateway infrastructure that allow API-serving systems and applications are accessible over transport security channels, e.g. SSL/TLs channels. Such APIs are required to have a time-limited authentication and authorization. Such authentication can be generated using a temporary login with two form factor authentication or key-based secrets to authenticate. For example, Google cloud platform is required users to be authenticated using two-form factor authentication when accessing Goole account or other Google services.

APIs for development practices like XML code and input from application perspective are required to be tested. Such testing can be exploited via cross-site request forgery attack methods and inject of standard flaw for XML code input and output to certify that the API is secure for integration (Google Cloud Platform, 2018). These APIs and interfaces must be designed to protect against any malicious attempt to circumvent policy (InstaSafe, 2018).

New forms of message protection involve its structure, integrity, coding and encoding, as well as hardware token and keys are the general best practices can be enforced

when considering of APIs and interfaces for cloud systems and applications (Google Cloud Platform, 2018).

**b. Security countermeasures for VM resource allocation**

Improper resource allocation causes server run inefficiently. The measure to maximize the virtual machine to virtual host ratio including building up virtual machine resource baseline (Rob McShinsky, 2009) to size the resources needed for certain applications and system workloads.

The resource allocation can be configured in such a way in the reservation pool to control the resource allocation. Resource allocation settings can be determined by the amount of usage in processor, memory and capacity to be assigned to a virtual machine including the sharing setting, its reservation and limit threshold. This can be controlled to set an upper bound on the resources in a virtual machine so not to over provisioned or under provisioned. As such, to guarantee that a particular VM is allocated a higher percentage of resources.

**c. Security countermeasures for data vulnerabilities**

Security measures are essential, critical and urgent in the face of stronger cybercriminals. The objective of such security countermeasures is to stop critical vulnerabilities and extend protection from global predators.

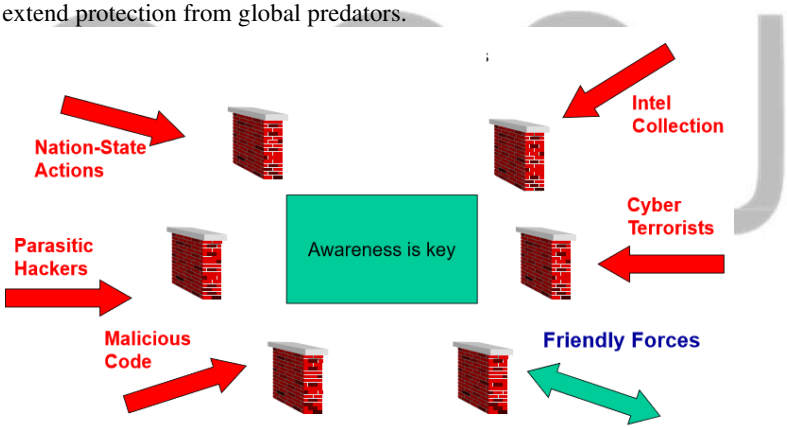


Figure 16: A common defense strategies. (Source: Philip Loranger & Rober Ingwalson)

Awareness is the key (figure 16) for data security protection and defense strategy. The data ownership and right must be defined to enable a basic for trust of data and the data ownership must not be subject to unilateral amendment by the cloud provider (Wayne Jansen & Timothy Grance, 2011, p.19).

Other countermeasures, including prevention can be taken place, including validating user input in a system or a web application against its expected output and encode user supplied output. This can prevent phishing attacks, deface a website and a system or a web application uses input from a malicious user to generate output without

validating or encoding the input. This process strongly validates user input using accepted 'known good' as a strategy or isolates incoming files and check them legitimately before executing them.

**d. Security countermeasures for vulnerabilities in virtual machines**

Protecting of virtual systems or virtual assets is as hard as protecting its physical hardware (Joseph Rannemma, 2012). There are many malicious activities targeted virtual systems, and it has made virtualization no longer safe from preventing hacker accessing of the confidential data that stored in the virtual machines. This happens when targeted a virtual machine is accessible from the internet. Trusted virtual domain can be implemented to split the communication between VMs, as such to make sure that different virtual machines is able to maintain its confidentiality, integrity and information flow within its isolated domain (Serdar Cabuk, et al., 2007). Virtual machine installed with virtualization application and relevant operating systems required to be patched and hardened. Hardening can be done by increasing the policy thresholds and putting in the virtual firewall after the firewall with access rules. The access rules is to apply the access and deny rules to the virtual machines in different trusted virtual domains as well as the access to virtual machine via virtual private network (VPN) with authentication requirements. Implement of endpoint security like antivirus, host intrusion prevention system and even vulnerability assessment to ensure free of system's loophole. Access control to the virtual machine must be enforced with restriction of access, and grant permission for each of the entities with authentication in the system. Availability is also another key factor for security countermeasure which the resources for virtual machine must be granted only to the authorized entity with its performance specification including virtual machines in disaster recovery site and system load balancing.

**e. Security countermeasures for vulnerabilities in VM's templates or images**

It is known issue for virtual machine images do not have any patch when it comes to vulnerable. However, virtual system is opened protection for virtual machine snapshots via the virtual sphere data protection. Proper cleanup of templates/images that are not in-used and keep the frequent used templates/images in a repository store that with relevant security in place, e.g. data store system that with endpoint protection, or behind a firewall that having access policy lists

**f. Security countermeasures for vulnerabilities in hypervisors**

The hypervisor is a core feature of virtualization technology. The flexible in configuration exposes to risk of attack. The hypervisor level requires constant update to address the disclose vulnerability including hypervisor bug. Continue to work with virtualization principals to get the latest fix for the hypervisor because they designed such virtualization to optimize IT operation, and at the same time to ensure that users are running on virtual platform is supported by them.

**g. Security countermeasure for vulnerabilities in virtual network**

Virtual network components, including virtual switch, virtual firewall, etc. in virtual network environments, a proper security measurement must be implemented to protect of virtual machine, data and application against from an attack, or information leakage, interception and, deception, usurpation, disruption even exploitation. In order to prevent these vulnerabilities, networks can be segregated. Federation of virtual networks with authentication, which to ensure of entities of the network access. Segregation is also similar to the isolation; this is to distinct of network and services access.

In most cases even in the public broadcast, the incoming traffic is blocked from external network, so no packet is flowed into virtual systems. Unless explicit firewall rules are created for access for the connection from outside network. Firewall including the use of tunneling in the firewall to isolate the network traffic (Leonard Richter Bays, et al., 2015) and restrict access to the virtual machines. Such isolation and segregation can also be extended to the virtual switches and routers for different virtual local area network (VLAN) or demilitarized zone (DMZ) configuration and routing tables.

**h. Security countermeasures for VM hoping and escape**

- HyperSafe

This is a lightweight approach for flow integrity in hypervisor control. The hyperSafe has its unique self-protection capability (Zhi Wang and Xuxian Jiang, 2011) for lifetime control flow integrity. It consists of non-bypassable memory lockdown that enables the self-protection for the hypervisor and which prevent of memory exploitation and restricted a pointer indexing which convert the data control into a pointer indexer (Zhi Wang and Xuxian Jiang, 2011). Refer to figure 17, the hypersafe with self-prevention of malicious write into the memory page tables.

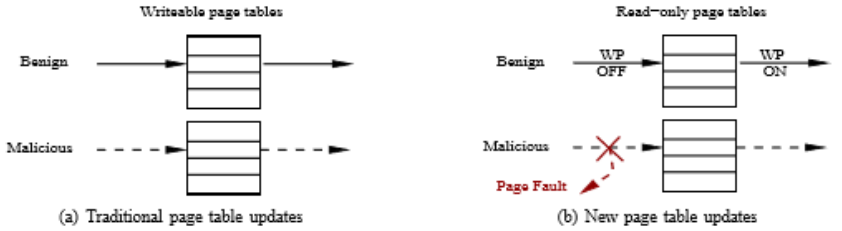


Figure 17: Self-protection in HyperSafe from compromised by memory exploitation. (Source: Zhi Wang and Xuxian Jiang, 2011)

- Trusted entities

The trusted entities with trusted cloud services and trusted data center enable cloud consumers to make sure that cloud environment is isolated with its security and integrity. The trusted cloud services platform managed the virtual systems with virtual machine monitor functions, as such, to monitor the process of virtual machine migration is running on the trusted platform which the trusted platform is provided by trusted data center. In such scenario, isolating and segregating of workloads of virtual machines can be expected, as such allow cloud consumers to control, isolating virtual system and

30

network in order to have security protection for all entities of cloud systems, applications, endpoint computing and users who accessing the services.

**i. Security countermeasures for malicious virtual machine creation**

Security framework is recommended for a better control of all the underlying infrastructure for cloud computing. This includes system and application filters, record tracking for resources and service utilization, traffic tracking and monitoring, data storage and repository maintenance, patching and hardening practices, etc. Although not all recommended measures help in fixing vulnerabilities especially when scanning of system and network sometime is not favoured by some people due to its privacy and confidential data, but at least minimize the potential of being attacked.

**j. Security countermeasures for credential hijacking**

The credential hijacking is also known as account service hijacking. It has turned up become a serious threat to accounts used for cloud computing purposes. Such security breach means attacker or hacker has gained access to the data, or copy, or manipulate, or falsify of data using legitimate login credential and password (Dan Virgilito, 2014).

- Identity Access Management (IAM)

The security measures that could take place with IAM solution to restrict the identity access with an algorithm, prohibit of account sharing, digital signatures for authentication and level of encryption to encrypt the data.

Cloud Security Alliance (CSA) promotes the use of best security practices for cloud computing. CSA has issued an Identity and Access Management (IAM) guidance for best practical action for identity and access management. The relevant identity and access management including user privilege and management, duties separation, roles-based access that commonly used in infrastructure for administration delegation, user access identity and etc.

- Dynamic credential

Dynamic credential whereby when users switch their access in different locations or when the user has exchanged of data packets, it presents different values of algorithms for the credential for access purposes.

The technique of fragmentation-redundancy-scattering provides intrusion tolerance and secure of storage, which it breaks the sensitive data into insignificant fragments in order to not have any significant information and subsequently scattered the fragments in a redundant pattern via vary way of distributed systems.

- Digital signatures

One of the common countermeasures is implement of digital signature, which using Rivest-Shamir-Adleman algorithm (RSA). RSA provides security with public and private key algorithm to digitally sign the data that sending over the internet. With security evolving in RSA algorithm up to key length of 2048-bit, making the RSA algorithm strong and not easy to break by the hacker. As such, is one of the efficient method to protect data over the cloud/Internet.

- Encryption

A method to secure data or 'lock' the data using encryption to translate the data to ciphertext. This is applied in a bidirectional way of data transfer from the cloud system or send to the cloud system especially the sensitive data. In regardless of encryption method, whether one way or bidirectional, the recipient has to decrypt the data using its private decryption keys. Data that being encrypted by the cloud providers exposes privacy issues, especially when cloud providers need to decipher/decrypt the data for certain system or the application process. When encrypting the data, ensure of strong algorithm is applied, e.g. encrypt using Advanced Encryption Standard (AES) and Secure Socket Layer (SSL). Such technique of encryption can prevent side channel attacks on the cloud data store and its de-duplication.

Homomorphic encryption can be used for performing of arbitrary computation on ciphertext without requiring of decipher/decryption. The method is only applicable to basic homomorphic encryptions due to its multiplication and addition requirement in operations which required extensive processing power that incur a massive response time and power utilization.

**k. Security countermeasures for data scavenging**

Data scavenging can be useful when data are completely removed or deleted. However, it is harmful if data scavenging is incomplete. In this case, the data scavenging process with the measure can be enabled by settings, including sets time value and change the stale of the scavenge to start data scavenging on the data that is no longer in used. A routine check to validate and ensure that deleted data is completely removed from the cloud's system, repository stored and the system bins. Data scavenging can be further performed with the option of enabling secure cache against pollution and checking the indication of the total data that were scavenged. Such, to increase the integrity and effectiveness of data scavenging.

**l. Security countermeasures for data leakage**

Data protection is one of the key measures to prevent business in a vulnerable position (Prof. Sushikumar, et al., 2015). Most cases of data leakage involve the confidential data that lead to unintended users or such data is compromised. There are several measures that can be applied to prevent data leakage. One of the most effective measure is having a firewall with intrusion detection and prevention capabilities to rules internal and external traffic including rules inside virtual nodes that being deployed in the cloud for internal and third-party access. The firewall will be the first layer of defense for the data in the cloud and actively monitor and block of relevant vulnerabilities and threats, including issue correlation, traffic pattern detection, monitor anomalies action and against known attacks (Cloud Security, 2012).

Data lost protection (DLP) can block and quarantine outbound and inbound data that contain suspicious malicious, code, abnormal pattern of traffic and application control to restrict and limit access to the data. The right management capability can be implemented to restrict and limit the data from print, copy, modify and delete. Refer to figure 18, the process of data flow only to intended users or authenticated users. DLP monitors

32

how emails are being sent including confidential email that sent by authorized users (B. Purohit and P. Prakash et al., 2013, p.1313) even they are granted with permission.

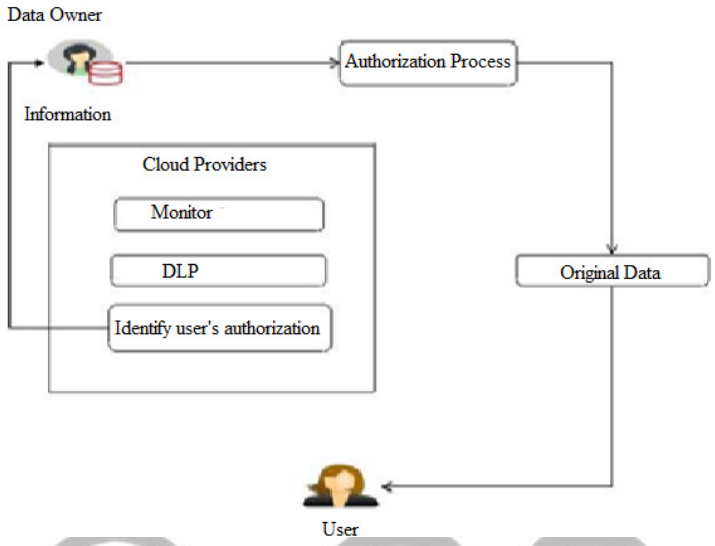


Figure 18: The flow of data sent to intended users with DLP and authentication process. (Source: S. Geetha, et al., 2016).

**m. Security countermeasures for data manipulation**

Data that exposes to the public is always being compromised and become targets of attack. A typical web application firewall (WAF) or cloud-based WAF can be adopted to place in front of web application systems to scan and analyse potential threats and violations. WAF can be used to inspect web traffic including secure web traffic to inspect specific threats and violations. For example, Singapore Power has control and practices in protecting of customer's information by using a WAF solution that is able to detect the data pattern, data trends, repetition, data clusters and data pathways which are the sequence of data in abnormal ways. These data manipulations will be detected and blocked by the specific violation rule to prohibit the access.

**n. Security countermeasures for Denial-of-service (DoS)**

In order to prevent DoS attacks that causing system failure, financial losses, extortion, brand damage, sabotage, etc., many ways of prevention can be applied practically to increase the security posture and minimize the potential of denial of service attack. One of the countermeasures is to use DoS attack detection and identification techniques to monitor the network and data traffic to distinguish between what is legitimate traffic and what is malicious traffic (Mike Chapple, 2016). Web application firewall like Incapsula service in the cloud come with dynamic profiling capability, its measure the traffic flow pattern, rates, behaviour, history based filtering, data flow frequent to detect a possible threat including DoS attack. As such, help organization to determine what kind of attack is underway that would affect their system functionality and business

operation. Incapsula service that comes with throttling and rate-limiting functions can help in responding to DoS attack in order to reduce the effect of the attack. Such response stop incoming traffic in the event of an attack is occurring while still allowing outgoing traffic to the external party until the incident is mitigated.

A cloud based DoS defender system like Akamai Distributed Denial of Service Defender can be adopted as a layer of security guard against DoS attack in order to minimize the risk of data theft and maximize the protection for any evolving threats with the help of security rules and updated threat library that done by the threat intelligence team (Akamai, 2018). Other than experiencing in DoS, relevant suggestion for such attack is applied to the Distributed Denial of service (DDoS). This DDoS causes severe damages than just DoS attack because it is a kind of volumetric attacks. Prevention and mitigation with security measures by aid of relevant detection and prevention for in-depth analysis and react potential incident by redirecting such traffic to mitigation devices for further action.

**o. Security countermeasures for threats in VM migration**

A secure migration framework can be implemented to preserve migration integrity and protect of privacy thorough the migration process. Security framework includes discovery of virtual machine that requires to migrate, stealth virtual machine migration which hiding the virtual machine on the network or behind the firewall and migrate the virtual machine in staging condition by using prototype systems as experimental evaluation, such as Xen systems, Open source Linux systems. These systems help in evaluation of migration time especially virtual machine's data with encryption that need time to decrypt before migration take place. A firewall is always the most effective security measure that revealed the result of migration results.

**p. Security countermeasures for virtual network spoofing and sniffing**

Virtual network security presents a virtual network framework that secures the communication among virtual machines. Virtual network includes virtual switch, virtual router and virtual firewall. Each of these virtual components can be the targeted of spoofing and sniffing. Security countermeasure such as access control that applies only for authorized access; trusted VLAN including interoperability between virtual networks for network segregation, information flow with integrity, confidentiality, isolated and interoperation between federated networks; path splitting for data propagation and data flow to hinder information interception attack (Leonardo Ritcher Bay, et al., 2015); subnetting for extra layer network to divide network in different purposes; virtual network resilience with fault tolerance; , encryption algorithm and etc. can be put in place to against virtual network spoofing and sniffing.

34

## 6 Results of Security Measurements

In order to facilitate the smooth sailing of various findings, thereby doing research as efficiently as possible by yielding maximal information and minimal of effort and time. The main purpose of such studies is that of formulating security issues for more precise investigation in the area of focus in the cloud so to develop the working hypotheses from an operational point of view. The major emphasis in such finding is on the discovery or ideas and insightful of data collected pertaining to the objectives of research and questions.

Analysis of the data collection is derived from the journals and articles that elaborate the ways that this information can be useful in the design of the cloud services and mitigation of security issues that exists in the cloud services. The analysis is also assessed based on an appropriate set of criteria to select secondary data to be used in the study since most of the journals are published by technology researchers and authors, the level of research validity and reliability is high and creditable. For furthering analysis of data collection, the inbuilt flexibility in research design is included because the research problem, broadly defined initially, is transformed into one with a more precise conceptual study. Secondary data were used to process to identify the security issues and countermeasures that helps in mitigating and resolving the security requirement in the cloud and research needs. The process including collection of data through information published by credible authors, processing to identify the security issues for finding and analysis, follow by provenance of security measures. Each of this process addressed different aspects of the potential research in the study. Generally, the methods in the context of conducting study, the purpose of study are clearly defined and detailed in the report. Thorough planned of finding with adequate analysis for confirming the security countermeasures to fix the security issues as well as justification of the findings and discussion to address the cloud problems.

The effectiveness of the finding provides clarity and information in the support of reaching decisions and results to the dilemma that is posed. The desired results of most researches are in the answers or decision options to make up the dependent variable in the research framework to ensure that all research questions have been asked in the design structure capable of producing valid results in meeting the objectives of the study. That is, including the outcome in fixing and solving the security risks that have been discussed in the statement of cloud problems. The research design addresses the research objectives in identifying of threats and vulnerabilities, analysing risks and issues and defining security measurements as a practical execution to improve the security posture for organizations who need security assurance to protect their data. The outcome of the research for security issues in cloud computing is also reviewed, analysed and discussed together with the cloud architecture and cloud computing classification and its different service models. The security vulnerabilities and threats have been analysed, the result with answers and decisions on the security measurement is reviewed and solved the problem that have been identified in the cloud services. Organizational aspects of the cloud service model and its security posture is discussed including the underlying technologies that were used in the cloud and the contact

between the cloud consumers and cloud service providers was also addressed with data security perspectives.

The key of cloud architecture impact security architecture is a common and concise other than the security issues and security countermeasures. It couples with a consistent taxonomy of offering which the cloud services and architecture can be deconstructed, mapped to a model compensating security and operational control, risk assessment, compliance standard and management framework (Beaker, 2009). Proper security measures are required to get the trust of users in this modern technology (Aizeh Amin Soofi, et al., 2014). Despite of advantages and security issues in the world of cloud, there are networking concerns that hamper its fast adoption. The outcome of the report also emphasizes network related issues that arise due to the public nature of cloud computing, network sharing, virtualization and the emerging challenges from security breaches with the demand in providing a resilient cloud computing infrastructure and services.

A guidance through mind-expanding on reducing effort in cloud security works, including an action for safeguarding of data, security measurements and enhancement with strategic and tactical options need to be further explored and research with the relevant contributions from the industry, academia and standardization arenas. The current information technology environment is constantly changing. Enterprises are generating more data than ever before and technologies such as cloud computing, Big Data, Artificial Intelligence and Internet of things (IoT) are shaping the contours of an evolving digital ecosystem. With the emergence of new cyber security legislation, the evolutionary forces require a new paradigm for defining the next generation security. Cybersecurity threats will continue to increase in volume and sophistication. Such a demanding cybersecurity regime entails a shift in focus from protection to early detection, response, and rectification. Businesses need to adopt new strategies and invest more in resources to detect and mitigate potential breaches before they occur.

The objectives to determine cloud computing and its service models possess security protection effects has been determined. The effect including implementing of security measures to fix the security vulnerabilities and threats that related to the cloud services has been explained; the analyst of vulnerabilities and threats that make up the security issues in the cloud computing has been addressed and define security measurement that can be used to mitigate and solve relevant security issues is highlighted and resolved.

36

## 7 Conclusion

Cloud computing is a modern technology. It provides flexible, efficient, cost effective and high-performance computing services to the businesses and all of us. By understanding the cloud service models in cloud computing platform, the architecture, technology use, process and human capital requirement and change is critical and important. There are many advantages of adopting different cloud service models to improve the IT operation and business performance, but there are also a series of security issues arise for this modern technology. This report described certain studies in literature about the security issues within the platform and relevant security countermeasure that could be adopted to address the issues.

The future of cloud computing can be transformed via artificial intelligence (AI). In future, AI will be adopted as a tool to transform information technology in the cloud to help businesses, education, government to automate information services delivery and boosting agility, decreasing risk and streamlining operation. AI helps to accelerate the business performance, solve business challenges in which organization lack of resources or staffs to success (Microsoft, 2018, Whit Andrews, 2017)). AI can be used for software development roadmap in all cloud service models because it makes the technology learning with combination of advanced machine learning, deep learning, natural language processing and business rules to disrupt the technology development life cycle (Deigo Lo Giudice, at al., 2016). AI technology integration with algorithms, composition and source large data sets to train and test applications to make application smarter. This integration with infrastructure services and tools backed by a best-of-breed infrastructure with enterprise grade security, availability, fault tolerance, access control, compliance and manageability (Microsoft, 2018) including disaster recovery, resilience and interoperability. The AI plays an important in the future advanced technology that can be used to integrate security mitigation. It fixes security issues quickly and confidently in pinpointing security bugs and remedies, threats and vulnerabilities redirection, security design for communication, etc. AI will be the valuable acumen on the latest cybersecurity outlook such as advanced malware detection, data theft prevention and secure cloud to learn innovative ways to strengthen the security posture and network performance.

The combination of cloud computing and AI presents a unique opportunity for cloud and AI professionals to explore the endless possibilities for the future, certainly including AI for cyber security in the cloud space. It will become the fastest path to technology as a Service with cloud services and automate the processes to speed technology innovation and business outcomes.

**References**

1. 360logical.com, 2018. Cloud computing – SPI models.
2. Aizeh Amin Soofi, M. Irfan Khan, Ramzan Talib and Umer Sarwar, 2014. Security issues in SaaS delivery model of cloud computing. By International Journal of Computer Science and Mobile Computing, Volume 3, Issue 3, March, p.15-21
3. Akamai, 2018. Denial of service attacks (DoS). Available at https://www.akamai.com/us/en/resources/denial-of-service-attacks-dos.jsp
4. Amphoen, Cloud Computing, available at https://www.scribd.com/document/96506209/Cloud-Computing
5. Anthony Bisong, Syed and M. Rahman, 2011. An overview of the Security concerns in Enterprise Cloud Computing. 28 January. IJNSA, Volume 3, Issue 1.
6. Anushree Malviya. Cloud computing. by Ewing Christian Institute of Management and Technology. Available at https://www.scribd.com/doc/23359066/Ppt-Cloud-Computing
7. AppliCure. Prevent denial of service (DoS) attacks. Available at http://www.applicure.com/solutions/prevent-denial-of-service-attacks, 4, April.
8. Arjun Komath, Cloud computing Seminar Topic Abstract. Available at https://www.scribd.com/document/162166169/Cloud-Computing-Seminar-Abstract
9. B. Purohit and P. Prakash et al., 2013. Data leakage analysis on cloud computing. Volume 3, Issue 3, May p.1313.
10. Beaker, 2009. Cloud Computing [Security] Architectural Framework, 19 July. Available at http://www.rationalsurvivability.com/blog/2009/07/cloud-computing-security-architectural-framework/
11. Bernd Grobauer, Tobias Walloschek and Elmar Stocker, 2011. Understanding Cloud Computing vulnerabilities. By IEEE Security Privacy, 1540-7993/1, p.51-57.
12. Boston College, 2016. Writing a literature review: Phase 1 scope of review. In reference to Boston College Libraries for research guides in writing a literature review. Available at https://libguides.bc.edu/c.php?g=44038&p=279691. 21 January, 2:49PM.
13. Cioinsight, 2018. IT modernization delayed by security issues.
14. Cloud Security, 2013. Preventing data leakage: Proactive security from the cloud, 14 November, 23:11pm.
15. Cloud Security Alliance, 2010. Top Threats to Cloud Computing V1.0. *2010.* Available at https://cloudsecurityalliance.org/research/top-threats, March.
16. Cloud Security Alliance (2012). Security guidance for critical areas of Mobile Computing, v1.0, by Cloud Security Alliance, retrieved from https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf,
17. Cloud Standard Customer Council, 2017. Security for cloud computing- Ten steps to ensure success, version 3.0, December.
18. Cor-Paul Bezemer and Andy Zaidman (2010). Multi-tenant SaaS applications: maintenance dream or nightmare? In the Proceedings of the 4th International Joint ERCIM/IWPSE Symposium on Software Evolution (IWPSE-EVOL), 2010, ACM.

38

19. CSA, 2011. Security guidance for critical areas of focus in cloud computing v3.0. Available at https://downloads.cloudsecurityalliance.org/assets/research/security guidance/csaguide.v3.0.pdf
20. Dan Marnescu, 2013. Cloud computing: Cloud vulnerabilities. By Tech Magazine 2013. July.
21. Dan Virgilito, 2014. How to reduce cloud security threats, 21 Feb.
22. Deigo Lo Giudice, Christoper Mines, Amanda LeClair, Romand Curran and Amy Homan, 2016. How AI will change software development and application, 13 October.
23. Dustin Amrhein, at el., 2009. Cloud computing use cases – A white paper produced by the cloud computing uses cases discussion group, version 1.0. Available at https://www.scribd.com/document/17929394/Cloud-Computing-Use-Cases-Whitepaper, 5 August.
24. Daniele Chatteddu and Giles Hogben, 2009. Cloud Computing: Benef*its,* risks and recommendations for information Security. 2009. 20 November.
25. Dave Shackleford, 2016. Cloud API security risks: How to assess cloud service provider APIs, 01 June.
26. Dejan Lukan, 2014. The top cloud computing threats and vulnerabilities in an enterprise environment, 24 November, 00:12am.
27. Dimitrios Zissis and Dimitrios Lekkas, 2010. Addressing cloud computing security issues. Journal of Science Direct for future generation computer systems, volume 28, Issue 3, March, p.583-592.
28. Dr. M. Bhandri, 2009. http://canjsurg.ca/wp-content/uploads/2013/12/53-4-278.pdf. 27 Jan, p.279.
29. Dustin Owens, 2010. Securing elasticity in the Cloud, Volume 8, Issue 5, 6 May, p.1-7.
30. Elhossiny Ibrahim, 2017. What is the difference between VM allocation and resource allocation in cloud computing?
31. Elmustafa and Rasha 2015. Network Denial of Service threat security on cloud computing. In International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). 5. 341-350, October.
32. Ertaul, Singhal and Gokay, 2010. Security challenges in Cloud Computing. In Proceedings of the 2010 International conference on Security and Management SAM'10. P.36–42.
33. F.A.Alvi, B.S Choudary, N. Jaferry and E.Pathan, 2014. A reviw on cloud computing security issues and challenges.
34. Galen Gruman, 2008. InfoWorld - Virtualization's secret security threats, 13 March, p.5.
35. Gansen Zhao, et al., 2009. Cloud Computing: A Statistics Aspect of Users. Volume 5931, ISBN
36. 978-642-10664-4
37. Gao Xiaopeng, Wang Sumei, and Chen Xianqin, 2010. VNSS: A Network Security sandbox
38. for virtual Computing environment. In IEEE youth in the conference on information Computing and telecommunications. DOI 10.1109/YCICT.2010.5713128, 28 November.

39. Google Cloud Platform, 2018. Google Cloud Platform Security – Deploy on an infrastructure
40. protected by top experts in information, application, and network security. Available at https://cloud.google.com/security/
41.
42. Han Ping Fung, 2017. What is the difference between vm allocation and resource allocation in
43. cloud computing?
44. Hanqian Wu H,Chuck Winer, Yi Ding and Li yao, 2010. Network Security for virtual machine
45. in Cloud Computing, November. Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference On. 10.1109/ICCIT.2010.5711022.
46. Ian Massingham, 2016. Security best practices. By Amazon web service – Webinar channel. Journal through the cloud. Available at https://www.youtube.com/watch?v=rXPyGDWKHIo, 8 September.
47. InstaSafe, 2017. Security Concern: Insecure interfaces and APIs. Available at https://instasafe.com/blog/2017/06/08/security-concern-insecure-interfaces-apis/, 8 June.
48. Iqra Sattar, Muhammad Shahid and Younis Abbas, 2015. A review of techniques to detect and prevent Distributed Denial of service (DDoS) attack in cloud computing environment. International journal of computer application. Volume 115, Issue 8, April, p.23.
49. Jaydip Sen, 2014. Security and privacy issues in cloud computing. p.1-34.
50. Jinpeng Wei, et al., 2009. Managing Security of virtual machine images in a Cloud environment. In Proceedings of the 2009 ACM workshop. ACM 978-1-60558-784-4/09/1, 13 November.
51. Jenni Susan Reuben JS, 2007. A survey on virtual machine Security. Seminar on Network Security; Technical report. By Helsinki University of Technology in a seminar on network security, October.
52. Jiehui Ju, Jianqing Fu, Ya Wang and Zhijie Lin, 2010. Research on Key Technology in SaaS, 10.1109/ICICCI.2010.120, December, p.384-387.
53. John Rittinghouse and James Ransome, 2009. Cloud Computing: Implementation, Management, and Security. ISBN 9781439806807 – CAT#K10347, 17 August, p.57-181, November.
54. John Viega, Li, et al., 2009, Cloud Computing and the common Man. P.106-108. Volume 42, Issue 8.
55. Jon Brodkin, 2010. 5 problems with SaaS security – Security tops customer concern on software-as-a-service. By Network World, 27 September, 8:00AM.
56. Jose Moura & David Hutchison, 2016. Review and analysis of networking challenges in cloud computing, by Lancaster University, Infolab21, available at https://arxiv.org/ftp/arxiv/papers/1601/1601.05329.pdf, p.6-10.
57. Joseph Granneman, 2012. Virtualization vulnerabilities and virtualization security threats. By Technology Target, research on cloud security, 10 July.
58. Kannan Subbiah, 2012. SaaS challenge & security concerns. By Knowledg Universe Technologies India Pvt ltd, 15 January.

59. Keiko Hashizume, David G Rosado, Fernandez Medina and Eduardo B Fernandez, 2013. An analysis of security issues for cloud computing. by SpingerOpen - Journal of Internet Services and application. 27 February.
60. Keiko Hashizume, Nobukazu Yoshioka and Eduardo B. Fernandez, 2013. In Security engineering for Cloud Computing: approaches and Tools*:* Three misuse patterns for Cloud Computing. DOI: 10.4018/978-1-4666-2125-1.ch003.
61. Larry Dragich, 2012. AP conceptual Framework – Prioritizing Gartner's APM Model, March.
62. Jaydip Sen, 2014. Security and privacy issues in cloud computing. Available at https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf, p.5
63. Lena Griebel, et al., 2015. A scoping review f cloud computing in healthcare. https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-015-0145-7, Licensee BioMed Central, 19 March, 15:17pm.
64. Leona Richter Bays, Rodrigo Ruas Oliveira, Marinho Pilla Barcellos, Luciano Paschoal Gaspary and Edmundo Roberto Mauro Madeira, 2014. Virtual network security: threats, countermeasures, and challenges. In the Journal of Internet services and application, .8 December.
65. Leonardo Richter Bays et al., 2015. Virtual network security: threats, countermeasure, and challenges. 08 December.
66. Margaret Rouse, 2010. SPI model (SaaS, PaaS, IaaS).
67. Marko Holbi, 2011. CEPIS -Cloud computing security and privacy issues. Version 17, 15 March, p.1-4.
68. Meiko Jensen, Jorg Schwenk, Nils Gruschka and Luigi Lo Iacono, 2009. On technical Security issues in Cloud Computing. *By* IEEE, DOI 10.1109/Cloud.2009.60, 21 September.
69. Mike Chapple, 2016. How to prevent DoS attacks in the enterprise. By Technology Target, research on cloud security, 28 December.
70. Microsoft, 2002. Microsoft virtual machine multiple JDBC vulnerabilities, 19 September.
71. Microsoft, 2012. Developer Nework- Developing multi-tenat applications for the cloud, 3rd edition.
72. Microsoft, 2018. The future Computed: Artificial intelligence and its roles in society. Foreword by Brad Smith and Harry Shum. Publish by Microsoft Corporation One Microsoft Way, ISBN 977-0-999-7508-1-0.
73. Microsoft TechNet, 2018. Virtual Machine Monitor. Available at https://technet.microsoft.com/en-us/library/cc708265(v=ws.10).aspx
74. Mohamed A. Morsy, John Grundy and Ingo Muller, 2010. An analysis of the Cloud Computing Security problem. Available at https://arxiv.org/ftp/arxiv/papers/1609/1609.01107.pdf
75. Monjur Ahmed and Mohammed Ashraf Hossain, 2014. Cloud computing and security issue in the cloud. By International Journal of network security & its applications, Volume6, issue 1, January.
76. Neil MacDonald, 2011. Garnet- Yes, Hypervisor are vulnerable. Blog Network. 26 January.
77. Nilanjan Dey, 2009. International Journal of ambient of computing and intelligence. Volume 1, Issue 4.

78. Philip Loranger & Rober Ingwalson. Session 30- IT security: threats, vulnerabilities and countermeasure. Retrieved from https://ifap.ed.gov/presentations/attachments/30ITSecurityThreatsVulnerabilitiesandCountermeasuresV1.pdf
79. Prof. Sushikumar, Holambe, Dr. Ulhas and Archana Bhosales, 2015. Data detection using cloud computing. International journal of scientific and engineering research, volume 6, Issue 3.
80. R. Chandramouli and Peter Mell, 2010. State of Security readiness. Crossroads, Volume 16, Issue 3, 1 March.
81. Raia El-Gazzar, 2014. A Literature Review on Cloud Computing Adoption Issues in Enterprises. DOI 10.1007/978-3-662-43459-8_14, ISSN 1868-4238. June.
82. Rajani Sharma and Rajender Kumar Trivedi, 2014. Literature review: cloud computing – security issues, solution and technologies. International Journal of Engineering Research, Volume 3, Issue 4, p.221-225.
83. Ranjith Poliyedath, Shalini Kaleeswaren and Chandran Priya, 2012. On covert channels between virtual machines. August, Journal in Computer Virology and Jour Springer. 9.10.1007.
84. Riber B. John and James Tobias, Cloud Computing and Accessibility Considerations. By NIST- Special Publication 500-317. Retrieved from https://www.nist.gov/sites/default/files/documents/itl/cloud/sp500-317_v01-draft.pdf, March.
85. Rob McShinsky, 2009. Virtualization don'ts: Neglecting VM resource allocation. By technology target, research on cloud security, 29 September.
86. S. Geetha, et al., 2016. Data leakage detection and security using cloud computing. Journal of engineering research and applictions. Volume 6, Issue3-2, March, p.1-4.
87. Sagar Sanjay, Prasana, Akshay and Amey. Cloud computing: Virtualization utility computing Software as a Service. Available at https://www.scribd.com/presentation/17847855/Cloud-Computing
88. Santosh Kumar Majhi, 2016. Threat modelling of virtual machine migration auction. By Technology Target, research on cloud security. Volume 78, p.107-113.
89. Serdar Cabuk, Chris I. Dalton, HariGovind Ramasamy and Matthias Schunter, 2007. Towards automated provisioning of secure virtualized networks. In ACM 978-1-59593-703-2/07/001, 3 September.
90. Shilpi Chandna, Rohit Singh and Fazil Akhtar, 2014. Data scavenging threat in cloud computing. Volume 2, Issue 2, 2 November, p.107.
91. SK Prashanth and N. Sambasive Rao, 2015. Vulnerability, threats and its countermeasure in cloud computing. International Journal of computer science and mobile computing, Volume 4, Issue 6, June, p.126-130.
92. Subashini S, Kavitha V: A survey on Security issues in service delivery models of Cloud Computing, Volume 34, Issue 1, 1 January, p.1-11
93. T.N. Sandeep Kumar and G.Harish Kumar, 2018. Abstarct on cloud computing. available at https://www.scribd.com/doc/29896057/Cloud-Computing-Abstract
94. Tal Garfinkel and Mendel Rosenblum, 2005. When virtual is harder than real: Security
95. challenges in virtual machine-based computing environments, 12 June.
96. TechRepublic, 2014. Data scavenging threat in cloud computing. by institute of Research and Journal (IRAJ), November.

42

97. Tim Mather, Subra Kumaraswamy and Shahed Latif, 2009. Cloud Security and Privacy-chapter 2- What is cloud computing? Chapter 6-Security management in the cloud, Chapter 9- Examples of cloud service providers and chapter 11= The impact of cloud computing on the roles of corporate IT, by O'Reilly, September.
98. Townsend, 2009. Managing a security program in a cloud computing environment. In Information Security Curriculum Development Conference, p.128-133.
99. Thomas Ristenpart, Eran Tromer, Hovav Shacham and Stefan Savage, 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, 09 November.
100. Thomas W Shinder, 2011. Security consideration for infrastructufe as a Service (IaaS). 14 July, 3:46pm.
101. Vic. Winkler, 2011. *Securing the Cloud: Cloud computer Security techniques and tactics*. Waltham, 13 May.
102. Viveknayyar, 2013. How to rollback VMware virtual machine to a previous point. Retrieved from http://www.tomshardware.com/faq/id-1820729/rollback-vmware-virtual-machine-previous-point.html
103. Wayne A Jansen, 2011. Cloud Hooks: Security and Privacy Issues in Cloud Computing. In Proceedings of the 44th Hawaii International Conference on System Sciences,16 May, p.1-9.
104. Wayne Jansen & Timothy Grance, 2011. Guidelines on security and privacy in public cloud computing. by NIST- Special publication 800-144. December, p.5-7 & p.19.
105. Wesam Dawoud, C. Meinel and Ibrahim Takouna, 2010: Infrastructure as a service security: Challenges and solutions, April, p.1–8.
106. Whit Andrews, 2017. Where should use artificial intelligence and why, 03 July.
107. Yiqian Zhang, Ari Juels, Michael K. Reiter and Thomas Ristenpart, 2012. The ACM guide to computing literature, ACM Digital Library: Cross-VM side channels and their use to extract private keys, 16 October.
108. Zhi Wang and Xuxian Jiang, 2011. HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity.