SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Proposed Framework of Vulnerability Assessment and Penetration Testing (VAPT) in Cloud Computing Environments from Penetration Tester Perspective

Nuur Ezaini Akmar Ismail[1], Noraida Haji Ali[1*], Masita Abdul Jalil[1], Farizah Yunus[1], Ahmad Dahari Jarno[2]

[1] Faculty of Ocean Engineering and Informatics, Universiti Malaysia Terengganu, 21030, Kuala Terengganu, Terengganu
[2] CyberSecurity Malaysia, Level 7 Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor

ARTICLE INFO

Article history:
Received 7 June 2023
Received in revised form 10 December 2023
Accepted 3 Jan 2024
Available online 7 February 2024

Keywords:
Cloud computing; penetration testing; SaaS; PaaS; IaaS; VAPT; Pentesting methodology

ABSTRACT

Penetration testing is a process that focuses on finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer system or steal information. Due to the COVID-19 endemic, most employees still implement working from home or a hybrid approach, even though the number of new cases of COVID-19 is decreasing. However, working from home depends mainly on cloud computing applications that help employees efficiently accomplish their daily work. This situation also increased the number of data generated from various sources, so they may be exposed to different security risks. This research will propose a framework to conduct vulnerability assessment and penetration testing (VAPT) in cloud service models such as SaaS, PaaS, and IaaS from the perspective of penetration testers. This proposed framework is developed through the integration and mapping of existing frameworks and guidelines to conduct VAPT on testing components such as web applications, APIs, network testing, etc. In this proposed framework, the method of conducting VAPT for each cloud service model will be discussed in detail, from the planning and reconnaissance stage until the report is delivered to the cloud subscriber or cloud provider. An advantage of this proposed framework for the penetration tester is that there is still a lack of methods or guidelines for conducting VAPT that cover all the cloud service models in one comprehensive document

1. Introduction

Penetration testing is a process or activity carried out by penetration testers who have no malicious intent other than to discover security vulnerabilities and system flaws in a target environment before the weaknesses are exploited by attackers [1]. This testing is crucial, especially for the financial institution and government sectors, since they store sensitive information such as personal details, banking information, health data, etc. from their end users or customers. The purpose of conducting penetration testing is to discover vulnerabilities and any system flaws in the

[*] *Corresponding author.*
E-mail address: aida@umt.edu.my

https://doi.org/10.37934/araset.39.1.114

system environment, then mitigate the issues before they are exposed to the public, to ensure the system offered is secure and thus gain trust from the customer, to identify and prioritize security risks, and to test security implementation in the configuration to ensure it is working as expected [2,3].

Based on National Institute of Standards and Technology SP800-145 [4], cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or interaction from the service provider. According to Wesley Chai *et al.,* [5], users are allowed to store all data and applications in the cloud, while other processes are managed by a third party known as the Cloud Service Provider (CSP).

There are three (3) benefits of using cloud computing, as mentioned by IBM [5], which are flexibility, efficiency, and strategic value. From a flexibility perspective, the users can create applications, scale services to meet their needs, and use cloud services from anywhere with an internet connection. The users can also choose the option for the storage, either public, private, or hybrid storage, depending on their nature of business or needs and their level of control, such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). IBM [5] also mentioned the security features provided by cloud providers by using virtual private clouds, encryption, and API keys to ensure the secrecy of the data stored in the cloud.

There are three (3) types of cloud users: 1) Cloud providers; 2) Cloud subscribers; and 3) External parties or Penetration testers (penetrators).

However, there are still lacking methods or guidelines for conducting penetration testing on cloud environments apart from the application stored in the cloud environment and not the cloud itself [6]. This research will be focused on the development of a new framework and discovered the best method to conduct Vulnerability Assessment and Penetration Testing (VAPT) to the cloud service models including the Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) from penetration tester perspective.

Throughout this paper, we will discuss the background of this research and provide brief information about the VAPT, which includes the testing components as well as the tools that can be used to conduct the testing in section 2. In section 3, we will elaborate on the research process, including the methodology for this proposed framework. Following that, in section 4, we will explain in detail the proposed framework of VAPT in cloud computing, and in section 5, we will elaborate more on the result and discussion of this research. Finally, in the final section, we will outline our next steps for future research to ensure that this research is ongoing and relevant. In this research, we will focus on the pentester, either hired by the cloud provider or a cloud subscriber. The roles of these cloud users depend on who is engaging with them.

2. Research Background

In this section, we will cover the study in two (2) research fields such as: 1) the cloud computing environment, including the three cloud computing service models and the reported vulnerability in the cloud; and 2) the VAPT, which consists of the testing component, for example, a web application, server, and virtual machine (VM), network security, mobile applications, and APIs, as well as the tools used to conduct the testing.

There are three cloud computing service model [NIST SP 800-145] [7]:

i. Infrastructure as a Service (IaaS) - Hardware and network connectivity are provided by the provider. The subscriber is responsible for the virtual machine and everything that runs within it.
ii. Platform as a Service (PaaS) - The subscriber supplies the application they wish to deploy, and the provider supplies all the components required to run the application.
iii. Software as a Service (SaaS) - The Cloud Provider supplies the application and all the components required to run it. SaaS is designed to be a turnkey solution for the tenant.

There are reported vulnerabilities in existing CC, as mentioned by Cypress Data Defense, such as misconfiguration cloud storage [6,7] and insecure APIs [6-11]. The misconfiguration of cloud storage buckets can result in attackers obtaining access to cloud-based data and stealing secret information, which might have terrible consequences for the company. Meanwhile, insecure APIs might happen due to inadequate authentication because developers often create APIs without proper authentication controls and insufficient authorization. Insufficient authorization occurs because many developers believe it is impossible for attackers to access the backend API calls and do not put too much effort into appropriate authorization control. The impact of this situation is that the backed data might be compromised by the attackers [6].

According to the Security Magazine [12], the research done by 451 researchers, 40% of companies have experienced a cloud-based data breach in the last 12 months. Despite these events, 83 percent of companies fail to encrypt half of their sensitive data stored in the cloud. This is supported by IBM [9], which claims that data breaches are one of the most common weaknesses in the cloud. Cloud computing is also vulnerable to various types of injections, such as malware injection, Cross-Site Scripting (XSS), and SQL injection [7–10]. Based on the Open Web Application Web Application Security Project (OWASP) [13], injection is the process when an attacker tries to inject malicious script (XSS), malicious executable programs such as [dot] exe, [dot] pdf, etc. (malware injection), and SQL queries (SQL injection) to the application inside the cloud with the intention of interfacing with the existing users, compromising the whole cloud, and getting sensitive information from the data stored in the cloud. DDoS (Distributed Denial of Service) is a cloud-specific attack in which the attack source is always more than one; several machines transmit packets with enormous data overhead to a single user. By flooding the network with unnecessary traffic, the attacks make resources inaccessible to the user [7,9].

We can conclude that there are various common vulnerabilities often found in the cloud environment, not to mention the zero-day vulnerability, sometimes written as 0-day, that is reported almost every day. A zero-day vulnerability is something that has been discovered by attackers before the vendor is aware of it [14]. Because vendors are unaware of zero-day vulnerabilities, no workaround exists, making attacks more likely to succeed [15]. We can also observe that common vulnerabilities found in cloud computing come from various perspectives, such as common web application vulnerabilities, insecure APIs, and network penetration testing.

Next, we will discuss Vulnerability Assessment and Penetration Testing (VAPT)**.** The definition of vulnerability assessment, as mentioned in SANS GPEN [16], is the process of finding the vulnerabilities and any flaws in the target system, often without regard to actually exploiting them or trying to get in. Meanwhile, penetration testing is the process of finding security vulnerabilities or any flaws in a target environment that could let an attacker penetrate the network or computer system or steal information. This definition can be found in SANS GPEN [17].

There are three types of penetration testing as mentioned in SANS GPEN [18] and CISA [19] which are white box testing, black box testing and gray box testing. White box testing is also called a full knowledge test of how the system is implemented. It is because penetration testing covers the process of analyzing the data flow and information flow, to verify whether secure coding is practiced, to ensure that the system implements security features and works correctly, and to identify vulnerabilities that could be exploited. The second type of penetration testing is black box testing. Black box testing is based on the software's specifications or requirements, and no details were provided. This type of testing relates more to a real world hacking scenario. The last type of penetration testing is gray box testing. This type of penetration testing combines white box techniques with black box testing and has little or no information regarding the target.

Table 1 illustrates the summary of the literature review for this research, including the purpose of each existing research study and the discussion or limitation.

Table 1
Summary of related works

No	Title, year	Propose	Discussion /limitation
1	Towards a Security Stress-Test for Cloud Configurations, 2022 [20]	This paper proposes a knowledge, and / or graphs approach to model cloud deployment security objects and vulnerabilities as guidelines for the system administration to determine the safer configuration and study the current issues if not properly configured	Before this, system administrators often configure based on their own experience or refer to the good security practices (e.g., CIS Benchmarks). In this paper also discuss the simple attack scenarios and the mitigation plan to fix those issues
2	Data Storage Security System based on Cloud Computing, 2022 [21]	This paper introduces encryption technology when designing the data storage security system to ensure the security of the information on the cloud platform	Discuss the theories of related to the Cloud Computing and Data Storage Security Systems
3	Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services, 2021 [3]	In this paper, only discussed the real-word cloud attack against each type of cloud service model and mentioned the techniques used by hackers to perform those attacks and how to prevent the attack from being exploited by attackers	Not discuss in detail how to perform VAPT but only focus on the type of attack such as security breach, authentication etc.
4	Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications, 2021 [22]	This paper pursues two objectives: to provide a comprehensive systematic literature review (SLR) of the Mobile Cloud Computing (MCC), security and penetration testing domains and to establish the requirements for penetration testing of MCC applications	Focusing on the problem of penetration testing and proposed the requirement of penetration testing for MCC application
5	A Study on security issues in SaaS Cloud Computing, 2021 [22]	This paper focuses more on the major issues in the SaaS which are data confidentiality, integrity, availability and data breach as well as the security challenges faced by the SaaS	Since the cloud is a broad concept, the research and study on the security issues especially data privacy and security still need to be done
6	Security in cloud computing: A survey, 2019 [24]	These are review papers that give a number of problems that impede the momentum of cloud deployment and heighten customer worries when utilizing cloud services	These papers discuss the specific issue why the user is still not able to use the cloud service
7	An insight into service model specific security in cloud computing, 2018 [25]		

8	Experimental analysis of DDoS attack and it's detection in Eucalyptus private cloud platform, 2016 [26]	This paper provides an overview of the experimental evaluation of DDoS in Eucalyptus as a cloud. The experiments were carried out using the open-source Eucalyptus platform as a private cloud model	This experiment was conducted in a simulation environment by using Kali as an attacker machine with two cloned Ubuntu VMs serving as botnets. Then using various tools to simulate the DDoS attack and monitoring using cloud-based traffic analysis tools to analyze the traffic pattern.
9	Security Issues in SaaS Delivery Model of Cloud Computing, 2014 [27]	This paper discusses more on the security issue in the SaaS model including data security, data breach, network security, backup and many more. Here also provides the solution to mitigate those security issues	Even though the SaaS service model have many advantages but still the tenant or user still concern about the security and privacy issues
10	A survey on security issues in service delivery models of cloud computing, 2010 [28]	A survey of the different security risks that pose a threat to the cloud is based on the service delivery models presented in this paper	Here mentioned that since the security concern is not properly handled and managed, the end user does not trust to use the cloud computing

Table 2 discusses the details of testing components for VAPT such as web application, server and virtual machine (VM), network security, mobile applications and APIs including the platform that is used for testing, related standards and framework for each of the testing components.

Table 2
The detail of the VAPT testing components

Testing components	Description	Standard or framework
Web application	This refers to the web application deployed in the cloud. The testing for the web application can be done using gray box testing, black-box testing or whitebox testing. For the gray box testing and black box testing, the pentester only tested at the application level (dynamic testing). The difference between both techniques is how much information is provided to the pentester before performing the testing. Meanwhile, the white-box testing is the combination of dynamic testing and static analysis including the web application and source code review	OWASP Top 10 2021 for web [29] OWASP Code Review Guide [30]
Server & Virtual Machine (VM)	To test the server in the cloud environment and the created VM by a subscriber. The task or activities to conducting VAPT against server and VM as follow: a. Full port scan i. The testing for the servers and VM uses running network mapping tools such as Nmap, Nessus, etc. to discover the open ports and its services. Using Nmap also will identify if any malicious services or application is implemented in the server or host b. Service identification i. Determine and identify the services of the open port based on the previous scanning results and plan the next action accordingly, such as using searchsploit or a Google search to see if the service is running using outdated versions, published public exploits etc. c. Host vulnerability scanning i. Determine and identify any flaws or vulnerabilities in the host	NIST SP 800-123 [31] OSSTMM Framework [32]

	or server using the previous scanning results in task 1, then plan the next action to verify the result. Here, the malicious application or spyware, such as a keylogger, backdoor, or VM rootkit, might be able to be detected and removed from the server and VMs d. Misconfigured security settings i. Determine and identify any misconfiguration in the security setting, such as a shared clipboard. Shared clipboard is the feature for buffer sharing between the VM and host, including copy and paste operations. If this feature is not properly configured, a malicious cloud user will be able to read the buffer between VM and host, thus compromising the shared data	
Network security	This testing was conducted to ensure that each subscriber in the cloud provider was configured properly and to test the data as it passed through the application and into the database. The activities done by penetration testing while conducting VAPT on the network are described below: a. Full port scan and service identification i. The testing for the Cloud data centers and central manager components by using running network mapping tools such as Nmap, Nessus, etc. to discover the open ports and its services This technique searches for specific open ports and gathers information about the system or services running on the identified ports before any network attacks can be exploited ii. This testing also covered the use of SSL/TLS versions to ensure secure communication in the cloud network and prevent malicious subscribers from compromising the secure traffic b. Network segmentation i. The network segmentation tests are performed using tools such as traceroute, ping, and Nmap (to discover if any port is open). The aim of this testing is to ensure that the network segmentation is configured properly, and the routing restrictions are in place to avoid any unwanted traffic across the tenant in the cloud environment c. Packet Sniffer i. The tools such as Address Resolution Protocol (ARP) and Round-Trip Time (RTT) to detect any capturing the important and sensitive information transmitted in the cloud network are used to prevent the data leaking to the malicious subscriber d. Network monitoring tool i. This monitoring will prevent any eavesdropping to the data transmitted inside the cloud network and data or packet modification by the malicious cloud subscriber to destroy the real data or packet before resubmitted to the authentic destination	NIST SP 800-123 [31]
Mobile Apps	This refers to the mobile apps deployed in the cloud. The testing for mobile will include static analysis using APKs or IPAs files from the authorized platform or provided by the subscriber to the pentester (either an internal pentester or an external party hired by them) and dynamic testing using a combination of tools such as Burp Suite Pro and Firefox add-ons. It is strongly recommended to do both types of testing to ensure all flaws will be discovered at the source code level and at the application level	OWASP Top 10 for mobile apps [33] OWASP Top 10 2021 for web [29]

APIs	APIs are widely used in cloud services to share information across various applications	OWASP API Security Project [34]

There are various tools that can be used to conduct VAPT, including commercial tools and free tools. Each testing component requires a different set of skills and tools, specific technical training to ensure that any flaws or vulnerabilities are able to be discovered before they are exposed to the public or exploited by an attacker. The list of tools mentioned below includes, but is not limited to:

i. Web Application - Burp Suite Pro, Acunetix, Owasp ZAP, etc.
ii. Source Code review - Veracode, Checkmark
iii. Server and Virtual Machine - Nmap, Sparta, Nessus
iv. Mobile Apps - MobSF, Burp Suite Pro
v. APIs - Burp Suite Pro., Postman Collection, Curl, OWASP ZAP, WebScarab
vi. Network security- Ping, Traceroute, Nmap, Sparta, Nessus, Wireshark etc.

3. Methodology

The process flow of this proposed framework development involves two (2) stages of process as discussed in Figure 1 and the details for the process will be elaborate in Table 3.

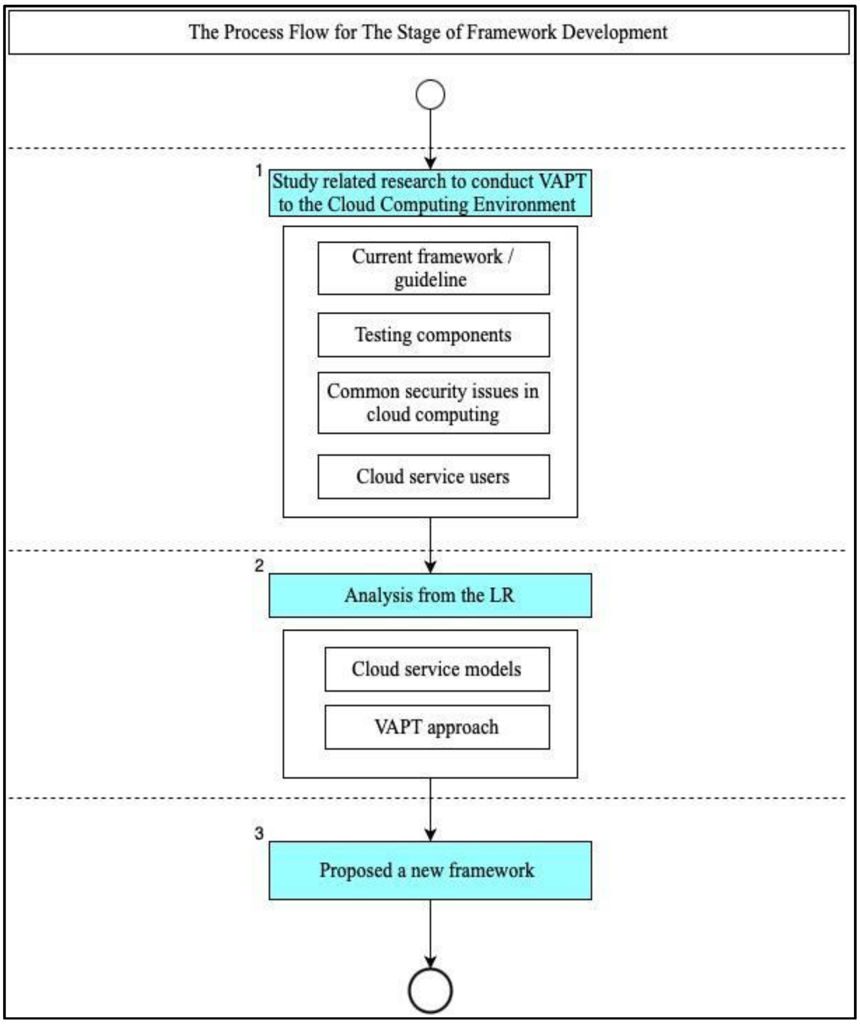
The Process Flow for The Stage of Framework Development
1
Study related research to conduct VAPT to the Cloud Computing Environment
Current framework / guideline
Testing components
Common security issues in cloud computing
Cloud service users
2
Analysis from the LR
Cloud service models
VAPT approach
3
Proposed a new framework

Fig. 1. The overview of process flow for each stage of framework development

Table 3
The detail of the process for each stage of framework development

Process	Details of the process
1	Study the related research to conduct VAPT in cloud computing environments: i. To gather related information before starting the research ii. To conduct research and study the existing framework or guideline for pentesting web applications, APIs, and networks, as well as how it relates to the current cloud computing issue iii. To identify elements in the framework, including the relevant testing components, the restricted or pre-engagement needed before the VAPT will be conducted, as well as related standards and guidelines iv. To identify the cloud user, such as the cloud provider or subscriber, and the roles of the penetration tester, either hired by the cloud provider or subscriber
2	Analysis from the LR a. Cloud service models: i. Gather related information, such as the existing study about the common reported issues or vulnerabilities for each type of cloud service model ii. The restricted or pre-engagement required before performing the VAPT or the limitations of the testing for each cloud service model iii. Determine the tools required to simulate each of the vulnerabilities b. VAPT approach: i. Confirmed related needs of VAPT before the VAPT will be conducted, such as the cloud service model in use for the testing since it requires a different approach, the scope of testing components, who is engaged with the pentester (subscriber or cloud provider), got the proper permission before starting the testing, etc. ii. Identify the relevant penetration testing methodology that is applicable for the testing based on the testing scope for each cloud service model
3	To propose a framework to conduct VAPT in a cloud computing environment that covers all three (3) types of cloud service models with relevant testing components such as web applications, APIs, network testing, etc. based on the penetration testing methodology

4. Proposed Framework for VAPT in Cloud Computing from Penetration Tester Perspective

This section will briefly explain the proposed framework of VAPT in the cloud computing environment for each type of cloud service model. Figure 2 illustrates the proposed framework to conduct VAPT in the cloud computing environment for identified cloud service models such as IaaS, SaaS, and PaaS based on each type of cloud user. The roles and responsibilities of the pentesters or external parties depend on who is engaging with them.

For example, if the pentester is hired by the subscriber to test the IaaS model, all the testing components can be tested by the pentester (but the scope of testing needs to be determined during the pre-engagement between the pentester and subscriber). However, if the pentester is hired by the cloud provider to conduct the testing on the SaaS model, they can do the testing on all the testing components except for APIs.

To propose a framework to conduct VAPT in a cloud computing environment that covers all three (3) types of cloud service models with relevant testing components such as web applications, APIs, network testing, etc. based on the penetration testing methodology.

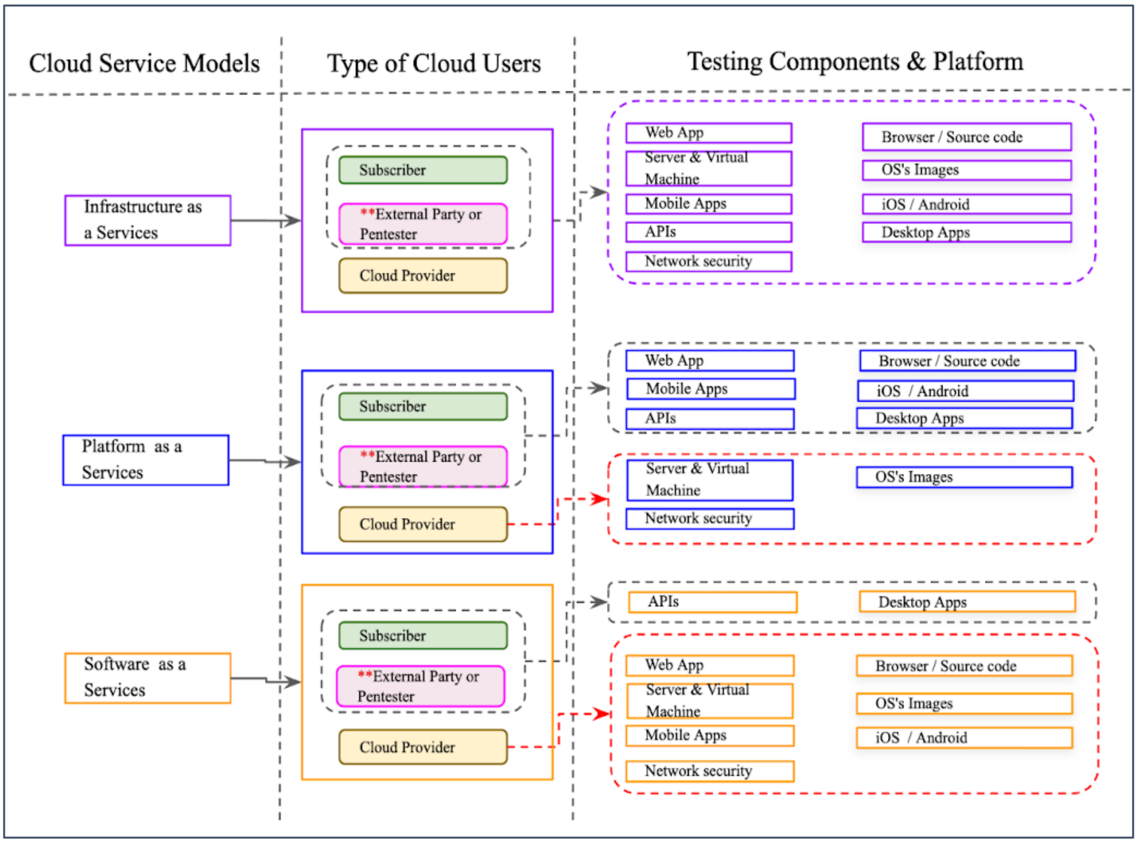

Fig. 2. The overall of the proposed framework for VAPT in the Cloud Computing environment

5. Results and Discussions

This section will discuss in detail the proposed framework of VAPT in the cloud computing environment for each type of cloud service model. Throughout this section, we will state the basic penetration testing often used by the penetration tester to conduct the testing, then we will discuss the summarization or mapping of penetration testing methodology to conducting VAPT for each type of cloud service model in Table 4. And lastly, we will state in Table 5 the common issues or vulnerabilities found in each of the testing components.

The basic penetration testing methodology is as follows:

a. Planning and scoping

i. The initial stage of testing includes all earlier engagement between the target's owner and pentester.
ii. Need to determine the scope of penetration testing and what to avoid during the testing as example DDOS testing or stress testing.
iii. Before the pentester can start the testing, they need to get the proper permission from the target's owner, finalize the scope of testing and sign of Non-Disclosure Agreement (NDA) or any relevant agreement.

b. Footprinting & reconnaissance

i. This is a process to gather all the information about the target.
ii. This process can be done either in passive using search engines (Google, Bing, etc.)

or active techniques such as command line interfaces (nslookup, dig, whois, etc.)

c. Scanning & enumeration

   i. In this step, the pentester will use the proper tools to do the scanning to find out any flaws and vulnerabilities inside the target and enumerate as much information as possible regarding the target.

d. Exploiting & verifying

   i. Do the manual verification and exploitation for each test case based on the results from the previous steps to ensure that there are no false positives or false negatives.
   ii. Manual testing is crucial since certain vulnerabilities cannot be discovered by using any automatic tools especially if related to logic functions or process flow.

e. Reporting

   i. The report represents the testing that was performed by the pentester. The pentester must demonstrate how they discovered all the issues in detail in the report. The project owner should be able to replicate or reproduce the testing steps as mentioned in the report provided by the penetration tester.

In the following Table 4, we give more detail the penetration testing methodology based on cloud service models, as well as the activities involved in each methodology phase, from planning to report delivery by pentesters to their clients (either a cloud provider or a cloud subscriber).

Table 4
The methodology of VAPT to the cloud service model

Phase	Cloud service model	Activities	
Planning and scoping	IaaS	I.	All the testing components can be tested without requiring proper permission from the cloud provider as long as it's still under the terms and conditions between the subscriber and the cloud provider (if a pentester is hired by the cloud subscriber)
		II.	Determine the scope of VAPT, such as which components need to be tested or need to be excluded from the testing, the type of testing (black, white, or gray box testing), the sign of agreement between subscriber and pentester (internal or external party), and the testing activities that need to be approved by the respective person
	PaaS	I.	Only web applications, mobile apps, and APIs can be tested without requiring proper permission from the cloud provider, as long as they're still under the terms and conditions between the subscriber and the cloud provider
		II.	The testing component is limited due to the possibility that network traffic from the testing can affect other subscribers or cloud providers
		III.	The best way to cater this is to conduct white box testing, including source code review, to ensure that more flaws and issues will be discovered at the source code level as well as at the application level, including the APIs
	SaaS		Only the interaction between web applications and APIs can be tested. However, if the cloud provider does the testing itself, they can do the pentest as mentioned in the IaaS and PaaS

Footprinting and reconnaissance	IaaS and PaaS	i.	Normally, for grey and white box testing, all the information required is already provided by the subscriber to the pentester. However, to ensure the testing is covered as much as possible, the pentester still needs to go through this process
		ii.	If pentester is provided with the source code, it can speed up the process of footprinting and recon
		iii.	The pentester can use various mechanism and tools to get all the information needed as described below: a) Command line interface b) Web based interface c) Script and software based d) Firefox add-ons
	SaaS		This stage of methodology is not relevant for the testing of SaaS except it is done by the cloud provider or pentester hired by them
Scanning and enumeration	IaaS and PaaS	i.	The aim for the scanning and enumeration is to identify in depth about the target and find any flaws and vulnerabilities that can be exploite
		ii.	The tools, techniques, skills, and testing methods depend on the testing component because we cannot use the same tools to cover everything
		iii.	Since this testing is conducted in the cloud environment, the pentester needs to do some research on the command vulnerabilities that are already exposed on the internet, to ensure all the software or hardware used the latest version or patched, the security advisory provided by the cloud provider and any relevant issues or testing that are related to the testing component
	SaaS		Nothing much can be done by the pentester since the scope is very limited. They only need to ensure that the communication with the web application is properly configured, APIs key managed appropriately and not disclosing any unencrypted data during the transmission. The pentester can use the proxy tools such as Burp Suite, OWASP ZAP and Webscarab to intercept and analyze the transaction
Exploitation and proof of concept (POC)	IaaS, PaaS and SaaS	i.	This is the last stage of the testing before the report of VAPT is developed and delivered to the subscriber by the pentester
		ii.	All the findings and issues discovered during the testing activities need to be manually verified and confirmed to ensure that it is not false positives
		iii.	The pentester also needs to provide and show in the report evidence of how the system or target will be compromised
Reporting	IaaS, PaaS and SaaS		The report represents the testing that was performed by the pentester. Here, the pentester needs to show how they find all the issues as illustrated in the report. The steps of testing should be able to be reproduced by the subscriber

From our literature review, the summary of the relationship between each testing component (web application, server and virtual machine, mobile application, APIs, and network) with the type of cloud service model and cloud user is as described in Table 5.

Table 6 discusses the common issues and critical vulnerabilities found in cloud computing for each testing component such as web applications, servers and virtual machines, mobile applications, network security and APIs including the tools used to conduct the testing.

Table 5
The mapping between testing components with cloud services model based on the cloud user

Cloud service model	Type of cloud users	Testing component				
		Web App	Server & VM	Mobile Apps	APIs	Network
IaaS	Subscriber	/	/	/	/	/
	Cloud Provider	/	/	/	/	/
	*Pentester	/	/	/	/	/
PaaS	Subscriber	/	x	/	/	x
	Cloud Provider	x	/	x	x	/
	*Pentester	x	/	x	x	/
SaaS	Subscriber	x	x	x	/	x
	Cloud Provider	/	/	/	/	/
	*Pentester	/	/	/	/	/

*The scope of testing components for the pentester depends on who is engaged with them. If a pentester is hired by a subscriber, the testing components are the same with the subscriber

Table 6
The mapping of each testing component with the related findings

The Testing Component	Related findings	Tools used (but not limited to)
Web Application	i. Path Traversal ii. Horizontal Privilege Escalation iii. Missing Authentication/Authorization for Critical Functions iv. Injection (SQL Injection, XSS) v. Broken Authentication vi. Insecure Direct Object Reference (IDOR)	Burp Suite Pro, Acunetix, Owasp ZAP, Veracode, Checkmark, Sonarqube
Server & virtual machine	Outdated Components with Known Vulnerabilities	Nmap, Sparta, Nessus
Mobile Apps	i. Sensitive Data Exposed in the Source Code ii. Insecure Data Storage	MobSF, Burp Suite Pro, etc.
APIs	i. Google api key disclosure that lead sensitive information ii. IDOR in the API	Burp Suite Pro., Postman Collection, Curl
Network security	i. Sensitive Data Disclosure through Unprotected Configuration File ii. Inadequate Transport Layer Protection iii. Exposed sensitive information	Ping, Traceroute, Nmap, Nessus, Wireshark, Spart

6. Conclusions

In conclusion, from this research, we proposed a new framework for VAPT in the cloud computing environment that covers three (3) types of cloud service models, such as IaaS, PaaS, and SaaS, from the perspective of a penetration tester. We chose this cloud user due to the nature of the responsibilities of penetration testers who will perform the VAPT according to who is engaged with them. So, basically, we cover all the cloud users' perspectives. This framework also discusses the common issues or vulnerabilities found in cloud environments as well as in the identified testing components. For future research, we could do simulation testing to ensure the effectiveness of this proposed framework of VAPT and discover the vulnerabilities and system flaws in the cloud computing environment. The simulation testing should be done in a closed environment since we will deploy vulnerable machines in the cloud before we can use the same testing method in the production environment.

Acknowledgement

This research was supported by Universiti Malaysia (UMT/PPRG/2020/53389). Thank you to CyberSecurity Malaysia as a collaboration partner for this research.

References

[1] GPEN SANS. *560.1 Comprehensive Pen Test Planning, Scoping, and Recon* (SANS Institute,2017).

[2] Soon Bock, Loh. "4 Reasons Why Penetration Testing Is Important." Horangi Cyber Security. https://www.horangi.com/blog/4-reasons-why-penetration-testing-is-important.

[3] Tiwari, Anjani, P. Patel, and D. Sharma. "Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services." *International Journal of Scientific Research in Science, Engineering and Technology* (2021): 395-403. https://doi.org/10.32628/IJSRSET218346

[4] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011). https://doi.org/10.6028/NIST.SP.800-145

[5] Wesley Chai, Stephen J. Bigelow, "What is Cloud Computing". https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing.

[6] "An overview of cloud security." What is cloud security, IBM, https://www.ibm.com/cloud/learn/cloud-security.

[7] "7 Cloud Computing Security Vulnerabilities and What to Do About Them". https://towardsdatascience.com/7-cloud-computing-security-vulnerabilities-and-what-to-do-about-them-e061bbe0faee

[8] "How Does Cloud Penetration Testing Differ from Standard Penetration Testing? ". https://www.guidepointsecurity.com/education-center/cloud-penetration-testing/

[9] "Cloud Application Security Checklist and Best Practices". https://www.rishabhsoft.com/blog/cloud-application-security-best-practices

[10] "Cloud security" https://www.ibm.com/cloud/learn/cloud-security

[11] "What is cloud penetration testing". https://www.nettitude.com/uk/penetration-testing/cloud-service-testing/

[12] "Cloud Computing Penetration Testing Checklist & Important Considerations". https://gbhackers.com/cloud-computing-penetration-testing-checklist-important-considerations/

[13] Maria Henriquez "40% of organizations have suffered a cloud-based data breach" https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-data-breach

[14] Williams, Jeff. "Injection Theory." OWASP. https://owasp.org/www-community/Injection_Theory

[15] Karpersky "What is a Zero-day Attack? - Definition and Explanation. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

[16] Bo Si Chua, "An Introduction to Pentesting Cloud Computing Environments" https://www.horangi.com/blog/introduction-to-pentesting-cloud-computing-environments

[17] SANS GPEN 2013 (Page 12, 560.1)

[18] SANS GPEN 2013 (Page 11, 560.1)

[19] "White Box Testing | CISA." US-CERT, 26 September 2005. https://www.cisa.gov/uscert/bsi/articles/best-practices/white-box-testing/white-box-testing

[20] Minna, Francesco, Fabio Massacci, and Katja Tuma. "Towards a Security Stress-Test for Cloud Configurations." In *2022 IEEE 15th International Conference on Cloud Computing (CLOUD)*, pp. 191-196. IEEE, 2022. https://doi.org/10.1109/CLOUD55607.2022.00038

[21] Yao, Haosila. "Data storage security system based on cloud computing." In *2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI)*, pp. 1220-1223. IEEE, 2022. https://doi.org/10.1109/ICETCI55101.2022.9832390

[22] Al-Ahmad, Ahmad Salah, Hasan Kahtan, Fadhl Hujainah, and Hamid A. Jalab. "Systematic literature review on penetration testing for mobile cloud computing applications." *IEEE Access* 7 (2019): 173524-173540. https://doi.org/10.1109/ACCESS.2019.2956770

[23] Prabhu, Adarsh G., Adithya Narayanan, and Claijo Kurian. "A STUDY on SECURITY ISSUES in SaaS CLOUD COMPUTING." (2021). https://doi.org/10.47760/ijcsmc.2021.v10i03.008

[24] Alhenaki, Lubna, Alaa Alwatban, Bashaer Alahmri, and Noof Alarifi. "Security in cloud computing: a survey." *International Journal of Computer Science and Information Security (IJCSIS)* 17, no. 4 (2019).

[25] Singh, Kulvinder, and Sarita Negi. "Service model specific security requirements and threats in cloud computing." *International Journal* 5, no. 7 (2015).

[26] Dar, Ashaq Hussain, Beenish Habib, Farida Khurshid, and M. Tariq Banday. "Experimental analysis of DDoS attack and it's detection in Eucalyptus private cloud platform." In *2016 International Conference on Advances in*

Computing, Communications and Informatics (ICACCI), pp. 1718-1724. IEEE, 2016. https://doi.org/10.1109/ICACCI.2016.7732295

[27] Soofi, Aized Amin, M. Irfan Khan, Ramzan Talib, and Umer Sarwar. "Security issues in SaaS delivery model of cloud computing." *International journal of computer science and mobile computing* 3, no. 3 (2014): 15-21.

[28] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." *Journal of network and computer applications* 34, no. 1 (2011): 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[29] OWASP Top 10. https://owasp.org/www-project-top-ten/

[30] OWASP Code Review Guide 2.0. https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf

[31] Guide to General Server Security. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

[32] OSSTMM Framework. https://www.isecom.org/OSSTMM.3.pdf

[33] OWASP Mobile Top 10. https://owasp.org/www-project-mobile-top-10/

[34] OWASP API Security Project. https://owasp.org/www-project-api-security/