International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

Cloud Security: Challenges and Best Practices in Penetration Testing

Azrul Enuar Samsudin, Mohamad Fadli Zolkipli
School of Computing, College of Arts and Sciences, Universiti Utara Malaysia
06010 Sintok Kedah, MALAYSIA.

Date of Submission: 10-07-2024 Date of Acceptance: 20-07-2024

ABSTRACT
The evolution of cloud computing is increasingly highlighting the benefits of cloud infrastructure and the integration of network technology capabilities, resource structure and guideline compliance. This paradigm harmonizes in detail the objective of strengthening the security of data protection, applications and services [2] [11]. The continued integration of these components also translates the importance of data maintenance in the cloud environment. This development provides a guarantee of a level of confidentiality, integrity and availability without exception to ensure perfect compliance with the standards [17]. Opportunity to implement and plan proactive action through penetration tests to enhance the security level of defense systems, and at the same time define improvements to key cloud security components [22]. How penetration test suitability can be effectively integrated into the cloud computing environment in addition to understanding the challenges of ensuring that data security assurance requirements are implemented is among the purposes of this paper.

KEYWORD : Vulnerability, Data Breach, Mitigation, Confidentiality

I. INTRODUCTION

Securing the Cloud

The evolution of cloud computing changes the specific method according to the setting of standards, supporting infrastructure and applications to stay in control. As referred to [19] related to the global standards developed to support the security management system and the emphasis on improving the clauses especially referring to the main needs of organizations in information security management. Starting from the stage of creation to the stage of improvement, the standards developed are in line with the importance of controlling risk through appropriate and continuous guidelines.

A variety of aspects are involved in the existence of new challenges, including the emphasis on entity protection in cloud computing through resource management, systems, and networks [17]. Consistent security of data, applications, and services relies on cloud security, that includes operational compliance, technology capabilities, and resources. According to [12], cloud computing provides a level of efficiency, which clarifies the components of resource sharing that facilitate network access in the integration of online information communication.

Cloud computing justifies the need for flexible resources. The advantages offered open up because of the unlimited control space. This opportunity allows the exploration of resources that can be adapted according to the needs of use [14]. This flexibility factor however gives pressure due to unforeseen control capacity constraints. Then there will be a weakness in identifying the risk of hacking. This situation places importance on compliance with standards and standards that help facilitate security control processes that support operational requirements as needed. In [4] emphasis on the importance of design and complex elements that can protect the privacy and security of applications systematically including compliance with guidelines and policies.

Offering multiple benefits does not prevent risk reduction if awareness and proper and continuous safety measures are implemented. Operational assessment, strengthening of energy resource efficiency that is constantly updated according to the development trend of cloud computing improves compatibility to the innovation of today's computing technology.

The Evolution of Cloud Security

The transition to cloud computing aims to overcome the complexities that are often encountered especially in relation to online data communication. Primitive measures of data protection and application continuity have changed to the needs of today's increasingly viable technology-based solutions. The uniqueness of the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

challenges in the operation must always emphasize the security aspect covering comprehensive control measures [18]. This indirectly involves the creation of advanced security frameworks, such as multi-factor authentication, identity and access management and data encryption. This will facilitate the assurance that data remains safe and secure.

Increased efficiency levels involve operational monitoring processes and changing security workloads based on dynamic cloud environment factors. The approach of using monitoring mechanisms needs to be streamlined such as more advanced threat detection including improvement methods involving continuous operations. As in [1] which explains the balance of benefits and the burden of difficulties through a cloud computing environment that needs to be emphasized. This balance reflects the strength necessary for organizations to establish control settings and the impact of weaknesses that can invite risks including application damage and data breaches.

The development of the latest technologies such as artificial intelligence and machine learning has started to become an approach. Research and innovation through both technologies is an opportunity for improvement and efficiency. At the same time, the openness of technology also increases the role and responsibility of the organization to deal with security aspects more deeply.

Around 2023, increasing levels of concern about cloud security will trigger the need for better governance [19]. This is due to increased standardization and increased rate of cyber threats as operations rely on cloud service resources. The term "forest standard" symbolizes how the need to drastically improve the capabilities of the entire support system of the cloud environment. In general, the challenge of securing security practices is increasing due to the speed of innovation and the diversity of cloud services.

The Role Penetration Testing

Penetration testing is an ethical hacking activity. This is one of the methods of checking the security system and through testing the availability of installed components as penetration control. White hat hackers [15], perform hacking ethically according to the requirements and scope agreed with the organization concerned. The main purpose is to prevent exploits that could result in unauthorized security breaches. This group, which is also classified as a red team, will look for weaknesses and then offer insights in the form of improvements that benefit the continuity and security of information.

The importance of penetration testing is an extension of the lack of specialist manpower in the organization. The transformation of methods and the improvement of technology is one of the reasons for the high skills in the network security team. In the rapid pace of cloud computing technology, adapting a penetration testing approach is critical. The settings and methods of working involve complex competition to be the backbone of the robustness of the cloud infrastructure. Assessment of cloud security integrity reveals the development of online security-related control frameworks. The required rating method can be translated as [19] details the importance of security and information assessment in threat management. Through it, a consistent and secure deployment foundation includes improvements to a unique but threat-free cloud landscape. This determination is synonymous with compliance efforts with industry standards and regulations.

Essential Components of Cloud Security: Data Encryption, Access Control, and Identity Management

Data encryption involves the important process of converting the original data into a hard-to-read format without using an encryption key. This setting is to ensure that data in the cloud environment meets data security protection standards. As stated through [17] regarding the security aspect of information flow that emphasizes security and protection. The use of reliable and suitable elements is necessary to ensure the stability and the resilience of the system regardless of a disaster. The advantages of data encryption include protection during the data transfer process and data downtime as shown in Figure 1. In this way, data can be ensured to only be reached and meaningful to the concerned individual safely. Data encryption uses automatic protocols and privacy to maintain data integrity.

Data integrity gets verified through an encrypted and automated mechanism. According to [13], issues related to data transfer and associated applications are additionally highlighted, demonstrating compliance to the security requirements of data transfer using cloud computing.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

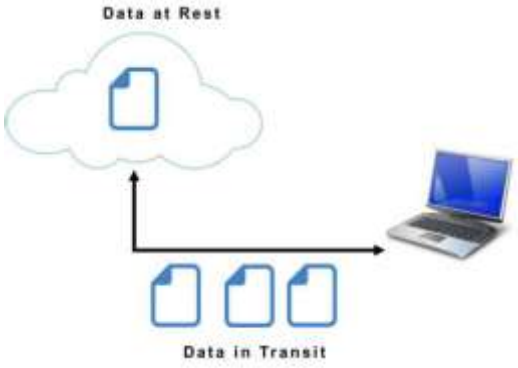

Figure 1: Data at Rest and in Transit.

The importance of data encryption is prioritized for confidentiality, protection, compliance and trust. At the same time, the emphasis is on compliance with standards according to the compliance regulations for data collection and storage. This definition refers to the security controls of information sharing. For example, the Personal Data Protection Act (PDPA) is enforced to regulate the handling of individual data in Malaysia. The PDPA regulation, as referenced in [16], establishes the responsibility for protecting the privacy of personal data for commercial purposes. The Health Insurance Portability and Accountability Act (HIPAA) refers to standards-based regulations involving patient data privacy. This control is to ensure patient data intrusion does not occur. The Payment Card Industry Data Security Standard (PCI DSS) refers to security standards in financial transactions. Every transaction involving the processing, storage and transmission of cardholder data must meet the security capacity based on the standards set by PCI DSS. Acts and standards mentioned are among the protection and security control mechanisms enforced on data to remain consistent to improve confidentiality, protection, compliance and trust.

Access permission control is a strategic approach to ensure access to resources is monitored to prevent unauthorized access. The proactive approach aims to prioritize safety at the highest level. Among the access control methods are Role-Based Access Control (RBAC) referring to access rights based on roles, Attribute-Based Access Control (ABAC) referring to access rights based on the consideration of multiple attributes, Policy-Based Access Control (PBAC) which is access rights based on certain conditions and Access Control Mandatory (MAC) refers to the ability to access based on a security label or classification.

Component	**Description**
Identity and Access Management (IAM)	Manages user identities, access permissions, and authentication.
Access Control	Controls distribution of privileges for accessing cloud resources and services.
Multi-Factor Authentication (MFA)	Enhances access integrity by requiring multiple security layers (Example : Password, One Time Password, Biometric).
Privileged Access Management (PAM)	Time-based access and password rotation / Protect special accounts (Example : Administrator, Super User).
Single Sign-On (SSO)	Single authentication point for multiple methods.
User Lifecycle Management	Ensures smooth onboarding/offboarding of users, maintaining role continuity and permissions.
Zero Trust Network Access (ZTNA)	Security based on context, identity, and device posture, rather than fixed perimeters.

Table 1 : Identity management component

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

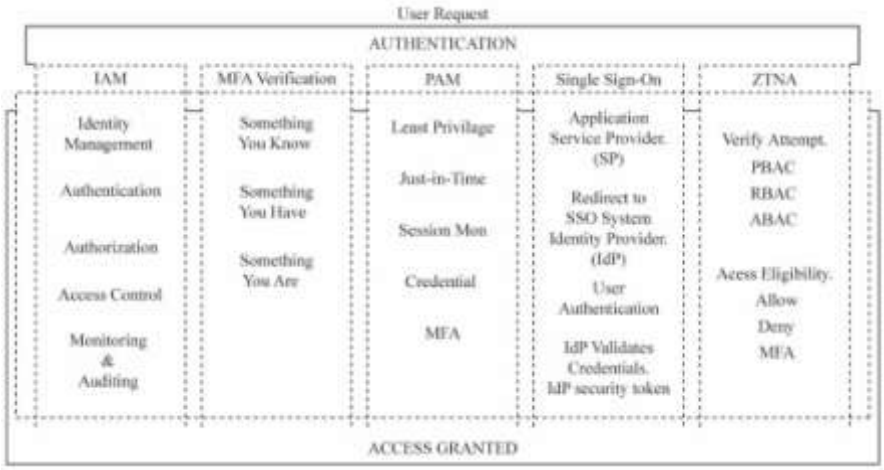

Figure 2 : Access Control and Authentication Methods

Cloud security is also concerned with the coordination of user identity management which emphasizes the aspects of authentication and authorization. Table 1 outlines the elements of user identity management. Among the component are Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Private Access Management (PAM), Single Sign-On (SSO), User Lifelong Management and Zero Trust Network Access (ZTNA). Figure 2 illustrates the access control flow, which relates to the approaches via user identity management approaches.This part guarantees user security, regulates access distribution, and preserves user roles and rights.

Role of Penetration Testing in Proactive Security Measures.

A robust effort to strengthen and stabilize the level of cloud security through proactive measures helps improve defence preparedness against cyber threats. The ongoing process involves monitoring and analyzing every activity including logging on suspicious anomalies, giving room for preventing cloud security breaches.

Proactive security measures through penetration tests are essential for systematic cloud environment control. This approach is especially helpful in identifying new weaknesses, adapting defences to complex environments, meeting procedural and policy compliance requirements, detecting early-stage vulnerabilities and balancing security requirements with cost savings [18]. Penetration testing should be positioned as an important initiative to cloud assets that involves improving the security strategy of the cloud environment. This function is considered an exercise in identifying capabilities and detecting system vulnerabilities that may be exploited by malicious actors. Cyber attacks using simulation techniques on systems or networks help organizations understand how their systems would react to a real attack. Through this proactive approach, preparations and processes update more appropriate methods to help prevent the risk of an attack before it occurs. This control method is particularly relevant in complex and changing cloud environments. Indirectly can speed up the process of identifying improvement areas such as authentication protocols, access control policies and enforcement procedures accurately. As stated [15], the conclusion about the advantages of detecting small vulnerabilities before they progress to critical ones, ensuring a high level of cyber hygiene and reducing risk exposure over time makes penetration testing a continuous practice.

This is an alternative that can build confidence with customers and stakeholders in the operation. This situation shows how important the data needs are to be protected. Continuous improvement ensures long-term security and stability in the cloud environment while effectively reducing the risk of data breaches.

The following components improve the effectiveness of the penetration test and ensure a stable safety posture for the organization.

Security Information and Event Management (SIEM): Collects and analyzes security data to identify suspicious activity.

- Security Information and Event Management (SIEM) systems play a role in providing a platform that facilitates real-time monitoring and detection. The method of centralizing operations through the process of log analysis, directly monitored through resources in the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

system support infrastructure. Rapid response to threats is implemented through this approach. This advantage facilitates compliance with event-based auditing by facilitating the analysis and discovery of generated logs. Activity insights obtained through logs facilitate the systematic identification of compliance with regulatory and policy-related standards

User and Entity Behavior Analytics (UEBA) : Analyzes user and entity behavior to identify security threats.

- User and Entity Behavior Analytics (UEBA) is the capacity to monitor and analyze through the generation of machine learning and behavioral analytics in the operational environment against users and other resources in the operation. This technology approach facilitates the control function to identify and respond to breaches involving risk through automated, intelligent, accurate and fast information generation.

Endpoint Detection and Response (EDR) : Monitors and responds to threats at endpoints.

- Endpoint Detection and Response (EDR) is the ability to monitor and respond to threats at the endpoint of resources involving IT infrastructure. Collection and analysis allows for more accurate detection of unexpected activities. EDR is able to examine threat behavior based on the ability to perform advanced analytics and machine learning. Thus the process of detecting, studying and interpreting attacks can be accelerated.

Network Segmentation : Segments the network to limit the spread of attacks.

- Network segmentation is the distribution of network resources into more detailed segment breakdowns. Through this approach threat propagation becomes more difficult as scope and policy settings are more detailed based on smaller specializations. By minimizing access to specific segments, control over security is easier. A more specific focus leaves ample scope for reducing the spread of threats.

Multi-Factor Authentication (MFA) : Requires multiple forms of authentication for authorized access.

- Multi-Factor Authentication (MFA) ensures the security rating of user accounts to improve advantages in dealing with the effects of data breaches such as theft of personal information, roles and compliance with regulatory frameworks such as PDPA, HIPAA and PCI DSS. These additional settings support the Zero Trust security model by strengthening controls and making penetration as difficult as possible.

II. CLOUD SECURITY RISKS : VULNERABILITIES AND MISCONFIGURATION

Among the weaknesses of the cloud environment is the risk of facing continuous threats involving breaches of data, interfaces and applications. For that, the assessment involves vulnerability and the implementation of frequent redemption tests that can open the way to improving security and reducing threats. Coding and specification review needs to be streamlined so that defense credibility is strengthened.

Table 2 shows the weaknesses and misconfigurations raised through previous studies based on cloud environments. Many of the issues raised highlight the importance of identifying and mitigating common vulnerabilities that should not be taken lightly in cloud computing settings. Among them, the emphasis on vulnerability assessment methods, coding practices, authentication configuration management that should be refined because it involves the formation of the posture of the cloud environment as a whole.

Most of the issues raised highlighted the importance of identifying and reducing common weaknesses that could not be overlooked in cloud computing settings. Among them, the emphasis on vulnerability assessment methods, encoding practices [2], management of authentication configurations that need to be refined because it involves forming the posture of the entire cloud environment.

Misconfigurations in cloud systems will open up opportunities for attackers to strategize and facilitate attacks.Insufficient expertise in advanced technical matters can pose challenges and lead to serious issues, including serious security breaches.Table 2 presents an overview summary, based on 10 previous research, outlining the various hazards linked to system vulnerabilities and misconfigurations. In order to enhance defense capabilities and comply with requirements to address cyber threats, it is necessary to have a comprehensive plan and strategy that includes continuous operational monitoring, ongoing audit implementation, and appropriate use of automation.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

References	Vulnerabilities	Misconfigurations
[1]	Cloud applications; ● Emphasizing the need for regular vulnerability assessments. ● Penetration testing to identify and mitigate these issues.	The risks associated with misconfigurations; ● Improper access controls. ● Exposed endpoints, which can lead to significant security breaches
[2]	Security posture from code to cloud secure coding practices and regular code reviews. ● Vulnerabilities that arise during the development and deployment phases.	Misconfigurations in cloud environments and provides strategies to avoid ● Automated configuration management Continuous monitoring.
[3]	Challenges in intelligent cloud systems ● Recommends best practices ● Configuration management to ensure security and compliance.	Cyber resilience and security issues in intelligent cloud computing systems ● Implementing robust security measures to enhance resilience against cyber threats.
[4]	Inherent in cloud computing environments ; ● Data breaches ● Insecure interfaces, and APIs.	Improper configuration of cloud resources ● Regular audits ● Automated configuration management.
[5]	Cloud computing educational Weak authentication mechanisms ● Lack of encryption. ● Insufficient access controls that can be exploited by malicious actors.	The cloud services expose sensitive educational data. ● Lack of Advanced technical knowledge.
[6]	Cloud computing and virtualization ; Exploited to compromise cloud security ● Multi-tenancy. ● Data integrity.	Proper configuration and continuous monitoring ; ● Misconfigured cloud settings ● Incorrect access controls and exposed data storage.
[7]	Cloud computing and virtualization ; ● Data breaches. ● Insecure APIs.	Configuration of cloud services can lead to security gaps ● Regular audits. ● Automated tools to manage configurations effectively.
[8]	Assessing through penetration testing in cloud environments ● Weak authentication. ● Insufficient access controls. ● Unpatched software that can be exploited by attackers.	Severe security breaches (cloud settings} ● Incorrect access controls and exposed data storage. ● importance of proper configuration. ● Continuous monitoring.
[9]	Securing sensitive construction data against potential cyber threats. ● Data breaches and insecure data storage.	Cloud computing (Construction industry) The paper discusses how misconfigured ● Data leaks. ● Unauthorized access. ● Proper configuration management.
[10]	Fault tolerance in cloud computing. It Single points of failure. ● Inadequate redundancy.	Fault tolerance mechanisms. ● Proper configuration. ● Regular testing.

Table 2: Discussion related to vulnerabilities and misconfigurations in cloud application security

Emphasis on the risk of security configuration vulnerabilities in cloud environments . Through understanding and accurate configuration methods, cloud security posture is

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

more secure and robust. Proactive actions can increase protection capacity and prevent data breaches. Weaknesses that are identified as risks not only open the way to data breaches, but also affect the credibility of organizations that rely entirely on the possession of sensitive information.

Vulnerability in Infrastructure

Cloud infrastructure vulnerabilities can pose a significant risk to the operational stability of an organization's systems. This is one of the aspects that need to be paid attention to because the complexity and unlimited nature of the cloud environment puts pressure and challenges on the continuity of operations. If configuration settings are not properly adjusted, the vulnerability to the defense will be more significant. These deficiencies may not be sufficient to properly place system readiness that will fail to protect against potential threats effectively.

Infrastructure in cloud services as discussed [14] [21] gives an explanation related to computing resources namely Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and Software as a Service (SaaS). The existence of these resources requires control methods based on the responsibility model. The main challenge is to ensure the compatibility of cooperation which can affect the performance of the service. Cooperation between service providers and users needs to be streamlined. The utilization of Information Technology (IT) services in a cloud environment is subject to risk reductions that prioritize data security. As pointed out [7] illustrates the truth of close cooperation between the two sides guided by mutual responsibility and trust. Satisfaction dependency offers an extensive evaluation of the extent to which a level of trust is both acceptable and beneficial for the sustainability objective. As defined in [10], reliability comprises the entire cloud-based service-oriented practice, with particular focus on availability. Availability in the sense of facilitating the flow of services to be more convincing, generally conducive, and fast.

This variety of opportunities also has the effect of an increasing concentration of control. Choosing the wrong security control method can have unexpected effects. This includes opportunities for fraud, vulnerabilities in the environment that are easy to exploit and so on.

Security Risk Mitigation Strategies

The strengthening of cloud security controls needs to be refined to improve the current security posture to the best level in order to always be ready to face cyber risks and threats. For that purpose, a comprehensive approach in ensuring defense is always at the forefront and is made a priority. Requirements in [3] identify considerations and preparations as reference sources for security, durability, platform management, technological infrastructure, and services in order to support cloud computing security. A comprehensive strategy is useful in ensuring transparency of the implications of the development of cyber attacks.

In order to effectively manage the constantly evolving attack environment, it is crucial to put in place an integrated cloud security control strategy, among other aspects are;

- Managing environments that are susceptible to attack.
- Detecting and acknowledging human error.
- Resolving configuration errors.
- Conducting assessments of risk for data breaches.
- Minimizing the duration of recovery.
- Creating strategies for business continuity.

In addition to maintaining the robustness of infrastructure and resources centrally, data security breaches can also be controlled by practicing routine security assessments. In the meantime, it is important that organizations make coordinated efforts to strengthen the technical capabilities of employees to ensure that these assets are consistently accessible to deal with unexpected situations. In [4], the security of the data is ensured through the use of encryption as a security measure, which serves as an alternative to risks that require access to sensitive data.

III. LITERATURE REVIEW

Based on knowledge and previous references can give explanations about the aspects that need to be emphasized. This shows how important it is to evaluate the implications of increasing computing technology that can undermine confidence in the implementation of a comprehensive cloud-based environment

Referring to [11] the need for compatibility of activity implications and the failure of approaches that arise are related to cloud security issues through the integration of service delivery models in cloud computing. According to the findings, in general, the benefits of communication technology through cloud computing are more focused on increasing popularity than the aspect of supporting infrastructure preparation. The advantages and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

opportunities for transformation and unlimited operational scalability are the main drivers.

The question is, what is the emphasis on the need to interpret concerns involving the existence of a reputation that constrains the stability in terms of the security of the cloud computing approach. The rate of technological development that is discussed is related to progress, achievements and directions that meet the level of availability, especially aspects of control that can be planned and integrated. There is no doubt that public computing offers a variety of conveniences and opportunities but appropriate threat protection methods need to be in line with the offerings. The concern, according to the study, is due to the resource flow factor in the cloud environment always facing the risk of intrusion and breach of privacy. To that end, the projected lack of flexibility in dealing with threats still requires a comprehensive set-up to meet certified security standards and guidelines. Consistent technical ability, especially the gap to the technical aspect, is still unclear. This is important because the value of real defense capabilities in dealing with conflicts that arise will shine through.

The scope of analysis was also developed for the diversification of the analysis approach through the STRIDE model. The use of this model is one of the threat flow-based evaluation methods [1] that can be used in cloud computing. In addition, the analysis of the previous literature covers the scope of the study of settings to the specifications of Security, Privacy and Technical Approaches implemented on cloud infrastructure resources, i.e. IaaS, PaaS and SaaS. Clearly, this method provides a clear view of the level of implementation of the settings and the sensitivity of the infrastructure security settings that have been implemented. The measurement of relevant parameters can be a guide to obtain the best and accurate justification according to the control of stable cloud environment security practices.

The disaggregated perspective [21] covers cloud computing environments, and vulnerability assessment and penetration testing (VAPT). Based on the availability of cloud computing in data communication that is invaluable in terms of generating capacity, the risk of increasing support is increasing. Based on the situation, the definition of the study suggests a framework suitable for the cloud environment through vulnerability assessment and penetration testing. The implementation of VAPT on the cloud service model is refined according to the implementation phase for testing the resources involved. Typically, resource testing involves components such as web applications, Application Programming Interface (API) and network..

The establishment of an essential framework refers to a comprehensive approach of strengthening the security posture of the infrastructure in depth and in a targeted manner. The study describes by explaining the advantages of the cloud environment which are;

- Flexibility based on application development factors, flexible developer justification and large geographical limitations.
- Efficiency refers to flexible information storage methods.
- Strategic Values enable provision of security features to every source including private cloud, encryption and API keys to preserve data confidentiality.

Referring to the research approach, the implementation of Vulnerability Assessment and Penetration Testing (VAPT) aims to identify security weaknesses or vulnerabilities in the target environment, such as a network or computer system, that could potentially be exploited by attackers. Testing is conducted using different approaches, including white box testing, black box testing, and gray box testing.

White box testing refers to the technique of covering full knowledge testing. Testers have complete knowledge of how the system is implemented. The process of analyzing data flow and information flow is carried out to ensure safe coding, the details of security aspects are implemented in an organized manner aimed at potential exploitation that exists [20]. For black box testing techniques the implementation process is based only on the specifications or requirements of the software, without any knowledge of the internal details of the system. This approach is more geared toward translating and deconstructing real-world hacking scenarios, as it simulates an outside attacker's perspective. Gray box testing refers to a combination of white box testing and black box testing techniques. This testing is likely to lack information or not show any response related to the target.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 07 July 2024, pp: 475-485 www.ijaem.net ISSN: 2395-5252

Cloud Computing Infrastructure Resources	Vulnerability	
	● Misconfiguration ● API is not secure	Type of Injection
Infrastructure as a Service (IaaS) Platform as a Service (PaaS) Software as a Service (SaaS)	Causing attackers to gain access to data and steal sensitive information. Inadequate authentication and insufficient authorization, affecting backed-up data. More than 40% of companies experienced cloud-based data breaches within the last year. Nevertheless, the figure of 83% is concerning.	Malware injection: ● Cross Site Scripting (XSS) ● SQL injection DDoS (Distributed Denial of Service) ● Attacks through multi-machine attack Sends packets with high data overhead to a single user. Zero-day vulnerability, increase the likelihood of an attack. ● The vulnerability of various perspectives. ● Disadvantages of common web applications. ● Insecure APIs and network penetration testing.

Table 3 : Cloud Vulnerabilities: Understanding and Mitigating Risks

The framework as proposed through the study of the implementation of the VAPT provides an explanation related to the requirements of the redemption test that is specific to the goals of planning and scoping, footprint and reconnaissance, scanning and enumeration, exploiting and verifying, and reporting involving the interweaving of cloud service models. The use of testing, analysis and reporting components enables the development of appropriate response programs that benefit the cloud ecosystem exposed to external possibilities

IV. CONCLUSION

Continuous efforts to improve security robustness, especially operational continuity in a cloud environment. The uniqueness of the challenges that arise in cloud infrastructure include shared responsibility models, dynamic scaling, planning methods, understanding the diversity of threats and the benefits of an approach through equipment, which can be used as a measure of strength to improve security as a whole.

Cloud penetration testing is basically the backbone of practice in setting up strategies to curb threats, especially for cloud environments. Security posture can be strengthened through a proactive approach in addressing vulnerabilities using simulated attacks. This approach opens up space and opportunities for the continuous development and evaluation of beneficial control methods involving cyber threats.

V. ACKNOWLEDGEMENT

The authors would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. E. J. Oyitso and E. D. Ordia, “Best Practices to Implement and Pitfalls to Avoid in Cloud Application Security,” Advances in Multidisciplinary and Scientific Research Journal, vol. 2, no. 2, pp. 41–48, Jul. 2023, doi: 10.22624/aims/csean-smart2023p6.

[2].]O. Afolabi, “Rethinking Your Application Security Posture from Code to Cloud,” Advances in Multidisciplinary and Scientific Research Journal, vol. 2, no. 2, pp. 27–32,

Jul. 2023, doi: 10.22624/aims/csean-smart2023p5.

[3]. F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," Results in Control and Optimization, vol. 12, p. 100268, Sep. 2023, doi: 10.1016/j.rico.2023.100268.

[4]. F. A. AlSelami, "Major Cloud Computing Security Challenges with Innovative Approaches," TehničKi Glasnik, vol. 17, no. 1, pp. 141–145, Feb. 2023, doi: 10.31803/tg-20220826124655.

[5]. R. Agrawal and S. Bansal, "Cloud Computing: Security with Educational Usage," Journal of ISMAC the Journal of IoT in Social, Mobile, Analytics, and Cloud, vol. 4, no. 3, pp. 165–173, Sep. 2022, doi: 10.36548/jismac.2022.3.003.

[6]. M. Abdelrazek, J. Grundy, and I. Mueller, "An analysis of the cloud computing security problem," Asia-Pacific Software Engineering Conference, pp. 1–6, Jan. 2010, [Online]. Available: https://researchbank.swinburne.edu.au/file/60eb29b0-2722-45df-b713-f55108d8206a/1/PDF (Accepted manuscript).pdf

[7]. G. R. Tsochev and R. I. Trifonov, "Cloud computing security requirements: A Review," IOP Conference Series. Materials Science and Engineering, vol. 1216, no. 1, p. 012001, Jan. 2022, doi: 10.1088/1757-899x/1216/1/012001.

[8]. I. Yurtseven and S. Bagriyanik, "A Review of Penetration Testing and Vulnerability Assessment in Cloud Environment," Oct. 2020, doi: 10.1109/uyms50627.2020.9247071.

[9]. S. A. Bello et al., "Cloud computing in construction industry: Use cases, benefits and challenges," Automation in Construction, vol. 122, p. 103441, Feb. 2021, doi: 10.1016/j.autcon.2020.103441.

[10]. P. Kumari and P. Kaur, "A survey of fault tolerance in cloud computing," Journal of King Saud University. Computer and Information Sciences/Mağalaẗ Ğam'aẗ Al-malīk Saud : Ùlm Al-ḥasib Wa Al-ma'lumat, vol. 33, no. 10, pp. 1159–1176, Dec. 2021, doi: 10.1016/j.jksuci.2018.09.021.

[11]. Y. S. Abdulsalam and M. Hedabou, "Security and Privacy in Cloud Computing: Technical Review," Future Internet, vol. 14, no. 1, p. 11, Dec. 2021, doi: 10.3390/fi14010011.

[12]. M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," Network, vol. 3, no. 3, pp. 422–450, Sep. 2023, doi: 10.3390/network3030018.

[13]. B. R. Rao and B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security," Measurement. Sensors, vol. 29, p. 100870, Oct. 2023, doi: 10.1016/j.measen.2023.100870.

[14]. A. S. George and S.Sagayarajan, "Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments," Zenodo (CERN European Organization for Nuclear Research), Mar. 2023, doi: 10.5281/zenodo.7723187.

[15]. R. Al-Khannak and S. S. Nehal, "Penetration Testing for the Cloud-Based Web Application," WSEAS Transactions on Computers, vol. 22, pp. 104–113, Aug. 2023, doi: 10.37394/23205.2023.22.13.

[16]. Baskaran, H., Yussof, S., Bakar, A. A., & Rahim, F. A. (2023). Data Sharing using PDPA-Compliant Blockchain Architecture in Malaysia. International Journal of Advanced Computer Science and Applications/International Journal of Advanced Computer Science & Applications, 14(5). https://doi.org/10.14569/ijacsa.2023.0140515

[17]. M. N. U. Haq and M. K. Sharma, "Mastering Cloud Security ; Techniques And Best Practices," in GRF BOOKS, 2023. doi: 10.52458/9788196869434.2023.eb.grf.ch-07.

[18]. S. Achar, "Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape," Zenodo (CERN European Organization for Nuclear Research), Sep. 2022, doi: 10.5281/zenodo.7084251.

[19]. T. Hegde, J. Gangl, S. Babenko, and J. Coffman, "Cloud Security Frameworks," Dec. 2023, doi: 10.1145/3603166.3632553.

[20]. A. A. Almutairi, S. Mishra, and M. Alshehri, "Web Security: Emerging Threats and Defense," Computer Systems Science and Engineering, vol. 40, no. 3, pp. 1233–1248, Jan. 2022, doi: 10.32604/csse.2022.019427.

[21]. N. N. E. A. Ismail, N. N. H. Ali, N. M. A. Jalil, N. F. Yunus, and N. A. D. Jarno, "A Proposed Framework of Vulnerability

Assessment and Penetration Testing (VAPT) in Cloud Computing Environments from Penetration Tester Perspective," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 39, no. 1, pp. 1–14, Feb. 2024, doi: 10.37934/araset.39.1.114.

[22]. S. A. Altayaran and W. Elmedany, "Integrating Web Application Security Penetration Testing into the Software Development Life Cycle: A Systematic Literature Review," 2021 International Conference on Data Analytics for Business and Industry (ICDABI), Oct. 2021, doi: 10.1109/icdabi53623.2021.9655950.