IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13702

ADVARSARY CLOUD PENETRATION TESTING FRAMEWORK

Ebin T Thomas[1], Megha Agesh[2], Tuna Job[3], Vishnu K[4], Ojus Thomas Lee[5]

Dept. of CSE, College of Engineering Kidangoor, Kottayam, Kerala, India[1-5]

Abstract: In today's digital landscape, characterized by widespread cloud adoption, ensuring robust security measures is paramount for organizations of all sizes to protect sensitive data and maintain business integrity. However, small and mid-sized companies often face challenges in implementing comprehensive security solutions due to budget constraints and limited technical expertise.

The paper presents an innovative approach to address these challenges by integrating open source into our cloud security assessment tool, which aligns with the methodologies outlined in the MITRA framework. By leveraging these frameworks, our tool provides comprehensive and cost-effective security assessments, allowing companies to identify and mitigate vulnerabilities within cloud environments efficiently. Through a user-friendly interface and clear recommendations for remediation, our tool empowers organizations to navigate the complexities of cloud security with confidence, ensuring that potential risks are addressed proactively. By harnessing the power of opensource frameworks and adhering to industry best practices outlined in the MITRA framework, we ensure accessibility and affordability, democratizing access to robust security measures for organizations of all sizes. Overall, our approach represents a significant advancement in cloud security assessment, offering practical solutions tailored to the evolving needs of small and mid-sized companies in today's digital landscape.

Index Terms: AWS, Opensource, Security, MITRA Framework, PACU, Cloud Automation.

I. INTRODUCTION

In present times, lots of companies rely on cloud computing to manage digital assets. Our tool makes it easier for security folks to keep cloud systems safe. It automatically checks for problems and helps fix them before hackers can cause trouble. We've made it simple to use and understand, and in this paper, we explain how it works. By making cloud security simpler and better, we're helping companies use cloud technology safely and smoothly. In today's modern business landscape, the reliance on cloud computing has become ubiquitous for countless companies seeking to efficiently manage their digital assets. However, amidst the array of benefits that cloud technology offers, significant security challenges loom large. In response to this pressing concern, our team is diligently developing a sophisticated tool tailored to scrutinize cloud systems for vulnerabilities.

Much like a digital detective, this tool meticulously inspects the configuration of cloud setups, identifying potential weaknesses that could be exploited by malicious actors. By automating the process of security assessment, our tool not only simplifies the arduous task faced by security professionals but also proactively mitigates risks by promptly rectifying identified issues before hackers can exploit them. With a focus on user-friendliness and clarity, we have ensured that our tool is accessible and understandable to all, thereby empowering companies to navigate the cloud computing landscape securely and seamlessly. This paper elucidates the inner workings of our innovative solution, aiming to demystify cloud security while highlighting the transformative impact it holds in safeguarding businesses' digital assets and facilitating the safe adoption of cloud technology.

II. MOTIVATION

Our project is driven by the understanding that many middlerange corporations face a significant barrier to accessing effective cloud security solutions due to their high costs. While open-source options exist, they often lack the comprehensive features and support needed for robust protection. To address this gap, we're developing an in-house automated penetration testing tool tailored specifically for these corporations. This tool allows organizations to conduct thorough security evaluations internally, eliminating the need for expensive external assessments. By keeping everything in-house, we're also enhancing confidentiality and giving organizations full control over their security protocols, ensuring greater flexibility and customization.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13702

Through our project, we aim to democratize cloud security, making it accessible and affordable for middle-range corporations. Our solution empowers these organizations to protect their cloud environments effectively without breaking the bank. By providing a cost-effective alternative with comprehensive features and internal control, we're enabling middle-range corporations to mitigate potential risks and safeguard their data with confidence.

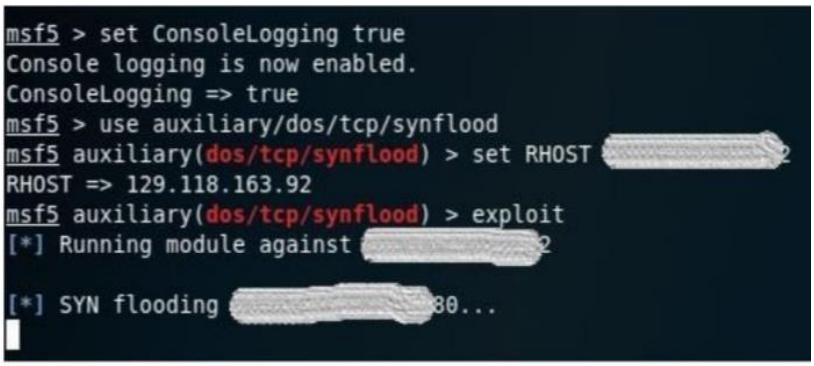
III. LITERATURE SURVEY

Cloud computing has transformed the operational landscape for businesses worldwide, offering scalable infrastructure and convenient on-demand services. Yet, alongside its myriad advantages, the widespread adoption of cloud technologies has ushered in a new era of security challenges. This literature review embarks on an exploration of recent research endeavours aimed at comprehensively understanding and mitigating these challenges. From delving into the tactics employed by cyber attackers to exploit cloud platforms for stealthy assaults, to scrutinizing the detection and prevention techniques necessary to safeguard against abuse in Infrastructure as a Service (IaaS) environments, the review encompasses a broad spectrum of pertinent investigations.

In parallel, the review navigates through a systematic assessment of cloud security concerns, employing a methodical approach to synthesize existing literature and unveil actionable insights. Additionally, it delves into the promising realm of bio-inspired algorithms, probing their application in addressing intricate security dilemmas within cloud computing frameworks. Moreover, it sheds light on the pivotal role of semantic approaches in navigating the labyrinth of cloud security and compliance, offering practical tools to empower cloud consumers in safeguarding their data and ensuring regulatory adherence. Through this review, a nuanced understanding of the multifaceted landscape of cloud security emerges, laying the groundwork for informed strategies and innovative solutions to fortify cloud-based ecosystems against evolving threats.

A. Platform to Launch Stealth Attacks

M. Chatterjee, et al. [1] discusses The document investigates how cyber attackers exploit cloud platforms for stealth cyberattacks. Researchers interviewed hackers to understand their methods and found they heavily use the cloud to mask identities and launch attacks. Case studies demonstrate possible attacks like port scanning and phishing.
Recommendations are provided for cloud providers to enhance security against such abuse.



TCP SYN flood using Metasploit.

Fig 1. DDOS attack

In simple terms, the document explores how cyber attackers are misusing cloud platforms to launch various types of cyberattacks. It discusses how the researcher's interviewed hackers and analysed their methods to understand how they use the cloud for illegal activities. The document also provides suggestions for cloud providers to improve their security measures to prevent such abuse.

B. Abuse Detection and Prevention in IaaS Cloud Computing

Lindemann, et al. [2] addresses abuse detection and prevention in IaaS cloud computing, examining technical and non-technical measures such as intrusion prevention systems and acceptable use policies. It emphasizes the need for further research to enhance IaaS security and highlights the impact on privacy concerns. The document concludes by underscoring the potential and limitations of abuse detection and prevention techniques in improving IaaS cloud service security.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

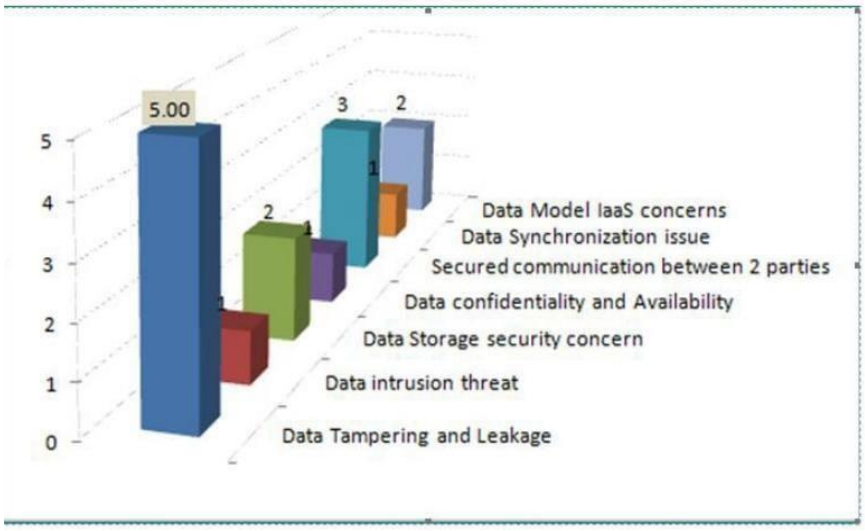
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 7, July 2024

DOI: 10.17148/IJARCCE.2024.13702

C. A Systematic Review on Cloud Security :Threats and Mitigation strategies

B. Alouffi, et al. [3] focuses on addressingThe study addresses security concerns in cloud computing through a systematic literature review, identifying threats, unaddressed issues by providers, consumer concerns, and blockchain's role in security. Using quality assessment criteria, they synthesized data to develop mitigation strategies and categorized findings for clarity.

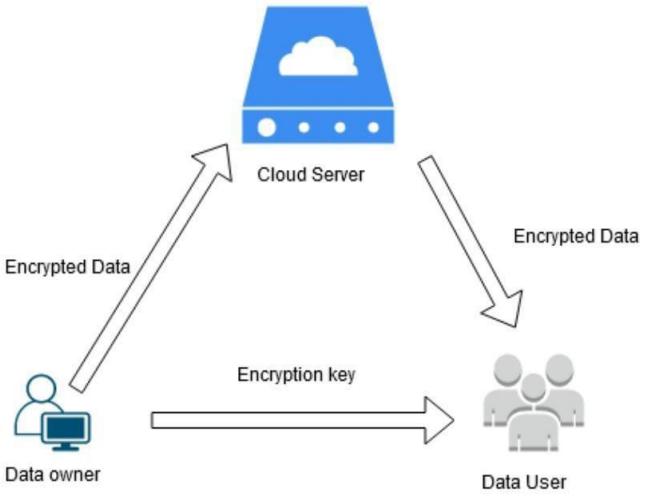


Identified cloud computing security threats.

Fig 2. Cloud Security Threat

D. Applications and Evaluations of Bio-Inspired Approaches in Cloud Security:

M. M. Ahsan, et al. [4]discusses The study explores using bio-inspired algorithms like Evolutionary, Swarm, Immune, and Neural algorithms to address security challenges in cloud computing. It covers areas such as network load, intrusion detection, authentication, and information leakage. Specifically, it focuses on insider threats and API instability, citing examples like the Marriott data breach and British Airways hack. Evolutionary algorithms are applied in access control systems, protocol security, and trust management. Swarm algorithms find use in authentication, forensics, and virtualization. Immune algorithms are utilized for network security and privacy in areas like identity authentication and protocol security. Neural algorithms, inspired by brain function, are effective for intrusion detection using optimized classification techniques.



A simplified encryption based Access Control Systems.

DOI: 10.17148/IJARCCE.2024.13702

IV. METHODOLOGY

The Adversary Penetration Framework simulates how real adversaries can potentially target a cloud environment. It extensively utilizes SDKs from various cloud providers to interact with different services. The tool closely follows various red teaming techniques, also known as Tactics, Techniques, and Procedures (TTPs) from various APT groups and MITRE.

The lifecycle of the process consists of several phases of assessment such as Reconnaissance, Mapping, Vulnerability Testing, Exploitation, and Reporting. Each phase of the assessment has its own significant role.

The system offers different features to its users.
Users: The users are individual entities who can use the tools. Users must be authenticated to access the tool, which is done by registering them along with their organizational details.

AWS Enumerator: The AWS enumerator enumerates the policies and roles attached to the users and user groups to understand the permissions the users have.

Permission Verification: User permissions are checked against potentially dangerous permissions. If there is a match, it is noted as potentially vulnerable permission. Once the permissions are checked, the corresponding exploitation function is invoked to exploit the misconfiguration. After successful exploitation, it checks whether the user's privileges have escalated.

Visual Graph: The result of the scan is stored as JSON and contains all information about the assessment such as attached user permissions, vulnerable permissions, exploited functions, etc. Utilizing this data, a graph is plotted to visualize the attack vector path for the user.

V. CONCLUSION

Our automated penetration testing tool represents a significant leap forward in cloud security. Its user-friendly interface and robust security measures make it accessible and efficient for organizations of all sizes. By systematically identifying vulnerabilities and providing actionable recommendations, it enhances the overall security posture of cloud infrastructures, fostering a culture of proactive security awareness.

The impact of our tool on the cloud environment is substantial. It promotes cost-effectiveness by eliminating the need for expensive external assessments and enables organizations to allocate resources efficiently. Additionally, its visual representations of attack paths and clear remediation recommendations empower organizations to respond swiftly to emerging threats, ensuring the integrity and confidentiality of their digital assets in the cloud.

REFERENCES

[1]. Al-Anzi, F. S., Salman, A. A., Jacob, N. K., & Soni, J. (2014). Towards robust, scalable, and secure network storage in Cloud Computing. In the 2014 Fourth International Conference on Digital Information and Communication Technology and its Application(DICTAP) (pp.51–55)http://doi.org/10.1109/DICTAP.2014.6821656
[2]. Alouffi, Bader, et al. "A systematic literature review on cloud computing security: threats and mitigation strategies." IEEE Access 9 (2021): 5779257807.
[3]. Lindemann, Jens. "Towards abuse detection and prevention in IaaS cloud computing." 2015 10th International Conference on Availability, Reliability, and Security. IEEE, 2015.
[4]. M. Chatterjee, P. Datta, F. Abri, A. Siami Namin and K. S. Jones, "Abuse of the Cloud as an Attack Platform," 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020, pp. 1091-1092, doi: 10.1109/COMPSAC48688.2020.0-125.
[5]. A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, USA, 2015, pp. 1081-1084, doi: 10.1109/CLOUD.2015.157.
[6]. N. Kashyap, A. Rana, V. Kansal and H. Walia, "Improve Cloud Based IoT Architecture Layer Security - A Literature Review," 2021 International Conference on Computing, Communication, and Intelligent Systems (ISIS), Greater Noida, India, 2021, pp. 772-777, doi: 10.1109/ICCCIS51004.2021.9397146.
[7]. M. M. Ahsan, K. D. Gupta, A. K. Nag, S. Poudyal, A. Z. Kouzani and M. A. P. Mahmud, "Applications and Evaluations of Bio-Inspired Approaches in Cloud Security: A Review," in IEEE Access, vol. 8, pp. 180799-180814, 2020, doi: 10.1109/ACCESS.2020.3027841.

DOI: 10.17148/IJARCCE.2024.13702

[8]. Chatterjee, Moitrayee, et al. "Cloud: A Platform to Launch Stealth Attacks." 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2020.

Papers	Evaluation parameter	Technologies used	Merits	Demerits
Platform to launch stealth attacks	Conducting interviews with security professionals and ethical hackers	Anonymity, scalability, cost effectiveness	Anonymity, scalability, cost effectiveness	Increased surveillance, vulnerabilities, difficulty in deletion
Abuse Detection and prevention in Iaas cloud computing	Individual virtual machines, Intrusion detection system	Intrusion prevention systems (IPS), filtering of network traffic	Deterring abuse, allowing providers to take necessary steps to stop abusive behaviour	False positive report, privacy concerns arise, lack of satisfactory solutions
Systematic review on cloud security: Threats and mitigation strategies	Quality assessment criteria (QAC)	Blockchain technology	Convenience, availability of applications and services	Data privacy and Governance challenges. Dependence on external service provider
Applications and Evaluations of Bio-inspired approaches in cloud security	Network load, security intrusion, authentication, biometric identification	Evolutionary algorithms, swarm algorithms	Adaptability, effectiveness, ability to handle large dataset	Time complexity issues, limitations in terms of accuracy, convergence
A semantic approach to cloud security and compliance security	Comprehensive study, Analyzed more than 20 security standards in cloud computing	OWL oniology, PHP, HTML, AJAX web technology	Comprehensive study, security policy recommendations	Complexity and overhead, Dependence on accuracy of data, limited scope

