https://doi.org/10.2352/EI.2024.36.3.MOBMU-319

Automated Tools for Cloud Security Testing

Hamid Ghazizadeh[1], Gerrit Tamm[1,3], Reiner Creutzburg[1,2]

[1]SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany
[2]TH Brandenburg, Department of Informatics and Media, Magdeburger Str. 50, D-14770 Brandenburg, Germany
[3]University of Stellenbosch, Department of Information Science, Stellenbosch 7600, South Africa

Email: hamid.ghz3373@gmail.com, reiner.creutzburg@srh.de, creutzburg@th-brandenburg.de, gerrit.tamm@srh.de

Abstract

The fast growth of cloud computing technology has led to immense development in the public and private sectors. Cloud computing provides a high level of virtualization, massive scalability, multitenancy, and elasticity. This has enabled organizations, academia, government departments, and the public to advance with this technology. However, they cannot assuredly place their information in the cloud due to many security threats. Cloud security plays a vital role in establishing confidence between the cloud service providers, consumers, and multi-users to maintain the security levels of their data.
Moreover, in the scope of cloud computing, the importance of security testing must be considered. Security testing involves evaluating the cloud infrastructure and applications for vulnerabilities, ensuring that sensitive data remains protected. This paper focused on the challenges, tools, techniques, and methodologies for cloud security testing. Furthermore, the paper introduces the tools offered by three significant CSPs for cloud security testing and the most critical cloud vulnerabilities. It explains some published vulnerabilities around these three major CSPs. Between these three significant CSPs, we focused on Azure offerings for securing their clouds and some known tools for security testing in the cloud. Lastly, we introduced and explained the most essential API vulnerabilities according to OWASP and a suggested way to mitigate them.

Introduction

Utilizing cloud computing has become an integral component of contemporary business operations, granting organizations the capacity to store, process, and manage data cost-efficient and scalable [13]. However, the adoption of cloud services also exposes businesses to an array of security risks and vulnerabilities. Consequently, there is an escalating requirement for cloud security testing that effectively safeguards sensitive information and upholds the integrity of cloud-based systems. One method to address this necessity involves employing open-source tools for cloud security testing, which automate the process and yield cost-effective and efficient results [1]. demonstrated that automation significantly enhances the efficiency and accuracy of security testing by reducing manual efforts and minimizing human errors. Organizations can streamline their security protocols by automating penetration testing and establishing a more robust defense against potential threats. The development and utilization of open-source tools for cloud security testing have experienced a noteworthy upsurge in recent years. These tools encompass various features and capabilities, including vulnerability scanning, penetration testing, and threat detection [2]. discovered the effectiveness of open-source tools such as Kali Linux, Metasploit, and OWASP ZAP in identifying and mitigating cloud vulnerabilities. Furthermore, the study acknowledged the high level of customization these tools offer, enabling organizations to tailor them to their specific requirements. Despite the advantages presented by automation open-source tools for cloud security testing, challenges do exist in their implementation. For instance, the intricacy of cloud environments and the ever-evolving threat landscape can make it challenging to stay alongside the latest security trends and techniques. Nonetheless, by remaining informed about current research and adhering to best practices, organizations can ensure the adoption of the most effective tools and methodologies to safeguard their cloud environments. The increasing reliance on cloud computing necessitates enhanced security strategies to safeguard applications and data hosted in the cloud. Traditional manual methods of cloud penetration testing are often labor-intensive, costly, and potentially inadequate in uncovering all vulnerabilities. Consequently, there is an escalating demand for automated cloud penetration testing tools. These tools aim to diminish expenses, augment efficiency and precision in detecting and ranking vulnerabilities, and proactively mitigate security threats. Various tools are available for automating cloud security, with some outperforming others in efficiency and accuracy. Adopting automated penetration testing techniques is crucial for strengthening cloud security measures. The primary aim of this study is to explore tools designed for automating cloud penetration testing, focusing on identifying key vulnerabilities and challenges associated with cloud infrastructure and APIs. Additionally, this research delves into the Azure cloud environment, examining the security tools it provides to facilitate automated security testing within its cloud framework.

Literature Review

In the realm of cloud security testing, significant advancements have been made, particularly in the development of automated testing systems. Tao, Lin, and Lu (2015) designed a cloud platform-based automated testing system specifically for the mobile internet environment. This system leverages virtualization and automation technology to integrate mobile terminals into the cloud platform, offering a novel service known as Testing as a Service (TaaS). The system's ability to flexibly

configure various testing environments and perform security testing automatically is a notable advancement in addressing the unique challenges posed by mobile internet security. The use of the Metasploit tool in their experiments demonstrated the system's efficacy in correctly identifying vulnerable apps and their vulnerability levels, highlighting the potential of automated tools in enhancing cloud security testing practices [3]. Furthering the discussion on automated vulnerability scanning and security testing, Jayakody, A. Perera, and G. Perera (2019) explored a cloud-native solution that automates these processes. Their approach simplifies the setup of scanners and configuration settings, addressing the time-consuming nature of manual web application security testing. This research underscores the importance of confirming the security of web applications, especially in the context of sensitive data protection. The advanced research tool they developed is capable of running dynamic security scans and dependency checks, identifying security loopholes without prior knowledge in security testing [4]. This innovation represents a significant step forward in automating cloud security testing, offering a more efficient and effective means of identifying and addressing vulnerabilities. Krishnaveni, Prabakaran, and Sivamohan (2016) focused on the security testing of Cloud SaaS, which is particularly vulnerable due to shared application access and data among various tenants. Their research highlights the prevalence of SQL injection and Cross-Site Scripting (XSS) as serious vulnerabilities in cloud-based applications. They proposed an automated security testing approach that includes vulnerability detection and prediction models, utilizing both static and dynamic attributes. This approach aims to improve the prediction of vulnerabilities in cloud-based applications, emphasizing the need for developers to ensure the delivery of safe applications and identify potential security issues before deployment in the cloud environment [5]. Lastly, Zhang, Xie, Tillmann, Halleux, Ma, and Iv explored automated testing of cloud applications, with a focus on Microsoft Azure. They addressed the challenge of manual developer testing being time-consuming and labor-intensive by proposing an approach that uses parameterized mock objects and dynamic symbolic execution (DSE). This technique not only generates test inputs but also mocks cloud states to achieve high structural coverage of cloud applications. Their work on open-source Azure cloud applications demonstrates the effectiveness of this approach in automatically generating test inputs and achieving high structural coverage, underscoring the potential of automated tools in enhancing the testing of cloud applications [6].

Challenges in Cloud Security Testing, [3.3]

In the realm of cloud security testing, several intricate challenges persist, each necessitating careful consideration and strategic response. A primary concern is the lack of control and visibility that users face in cloud environments. As Yang and Cao (2022) elucidate, this limitation significantly hampers the ability to effectively monitor and manage security threats, a predicament exacerbated by the inherent complexities of cloud computing models. Furthermore, the shared responsibility model, a staple in cloud computing, introduces additional layers of complexity [7]. Moreover, The integration of various technologies like SOA (Service-Oriented Architecture), virtualization, and Web 2.0 in cloud computing introduces inherited security issues. Each of these technologies brings its own set of vulnerabilities, thereby compounding the security challenges in cloud environments. For instance, virtualization, a core component of cloud services, introduces risks such as VM (Virtual Machine) escape, where an attacker gains access to the host machine, and inter-VM attacks, where one VM attacks another. Similarly, SOA and Web 2.0 technologies, which facilitate the development of scalable and flexible web applications, also expose cloud services to web-based attacks like SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) [8]. These challenges collectively underscore the multifaceted and evolving nature of cloud security testing, necessitating ongoing research and innovation to ensure the security and integrity of cloud-based systems and data.

Overview of common vulnerabilities in cloud environments, [5.1]

In the dynamic and complex landscape of cloud computing, a spectrum of vulnerabilities poses significant risks to data security and operational integrity, necessitating robust security measures [9]. Data breaches, a predominant concern, involve storing and processing data from numerous users and organizations in a shared space, making it a lucrative target for breaches stemming from human error, malicious attacks, or vulnerabilities in cloud applications. Factors such as weak authentication, insecure APIs, and inadequate encryption are key contributors to these breaches, highlighting the critical need for enhanced security protocols.

Access control in cloud environments is equally crucial, as traditional models may not adequately address the unique challenges of the cloud. Inadequate access controls can lead to unauthorized access to cloud resources, resulting in data breaches or manipulation of cloud services. This vulnerability underscores the necessity for improved authentication mechanisms and proper configuration of permissions, emphasizing the importance of stringent security measures. Denial of Service (DoS) attacks, particularly disruptive in cloud environments, impair the availability of services for both providers and users. These attacks aim to overwhelm cloud services with excessive traffic, significantly impacting user experience and business operations. The need for proactive measures to mitigate such threats is paramount in maintaining the integrity and availability of cloud services. Misconfigurations in cloud settings can inadvertently open doors to security threats, where proper configuration

management is crucial to prevent such risks. These misconfigurations, involving access controls, network settings, or encryption protocols, can be exploited by attackers to gain unauthorized access or disrupt services, further emphasizing the need for vigilant security practices. Application Programming Interface (API) security is vital in protecting cloud environments against vulnerabilities in their design or implementation, which can be exploited to manipulate data or execute unauthorized actions on cloud services[14]. Similarly, side-channel attacks, exploiting indirect information leakage such as power consumption or timing, pose a sophisticated threat that can compromise data confidentiality, even with robust encryption. Given the fundamental role of virtualization in cloud computing, virtualization vulnerabilities can have far-reaching consequences, potentially allowing attackers to escape from virtual machines, access other VMs or the hypervisor, or conduct privilege escalation attacks. The potential for cross-VM attacks is a particular concern, highlighting the need for robust security measures in the virtualization layer. Insider threats from individuals within an organization who misuse their authorized access can lead to serious security breaches, necessitating stringent access controls and continuous monitoring. These threats, including malicious and unintentional insiders, further compound the security challenges in cloud environments. Lastly, Cloud Malware Injection Attacks (CMIAs) target the data stored and processed in the cloud, exploiting vulnerabilities in cloud service providers. The susceptibility of platforms like OpenStack to such attacks due to design flaws in modern mainframes is a critical concern, underscoring the ongoing need for vigilance and adaptation in cloud security measures. In conclusion, the cloud computing landscape is fraught with interconnected vulnerabilities requiring specific attention and mitigation strategies. From data breaches to sophisticated malware attacks, the security challenges in cloud environments are complex and evolving, necessitating a comprehensive and continuous approach to security.

Vulnerabilities associated with each cloud service provider [5.2]

In the rapidly evolving cloud computing domain, recent disclosures have underscored the critical importance of identifying and mitigating vulnerabilities within major cloud service platforms [10]. These vulnerabilities, spanning across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, highlight the complex security challenges inherent in cloud environments and the necessity for continuous vigilance and proactive security measures. A notable vulnerability in AWS, CVE-2023-35165, affected the AWS Cloud Development Kit (AWS CDK), particularly impacting eks.Cluster and eks.FargateCluster constructs. These constructs created roles with overly permissive settings, leading to potential unauthorized access or misuse of resources. This issue was addressed in subsequent AWS CDK releases, with patches for affected versions, and users were advised to update their systems. Another vulnerability, CVE-2023-36467, targeted the AWS data.all framework, allowing authenticated users to inject Python commands into a 'Template' field, enabling remote code execution. This vulnerability was rectified in version 1.5.2 of the data. All users strongly recommended updating to this version for enhanced security.

In Microsoft Azure, CVE-2023-30514 was identified in the "Jenkins Azure Key Vault Plugin," where sensitive information was not adequately masked in the build log, posing a risk of exposing sensitive data. This vulnerability, classified as "CWE-319 Cleartext Transmission of Sensitive Information," necessitated an update to the plugin to ensure the secure handling of sensitive data. CVE-2022-30187, associated with the Azure Storage Library, also allowed unintended access to resources, classified as "CWE-668 Exposure of Resource to Wrong Sphere." The resolution involved a corrective update to the Azure Storage Library, emphasizing the importance of timely software updates for security.

Google Cloud Platform also faced its share of vulnerabilities. CVE-2022-36916, affecting the "Jenkins Google Cloud Backup Plugin," related to Cross-Site Request Forgery (CSRF) attacks, enabling unauthorized actions without user consent. The resolution involved updating the plugin to incorporate CSRF preventative measures. Another vulnerability, CVE-2021-20191, in the "ansible" tool on GCP, exposed sensitive information in the console log. This issue, classified as "CWE-532 Insertion of Sensitive Information into Log File," was resolved in Ansible version 2.9.18, safeguarding credentials from being logged.

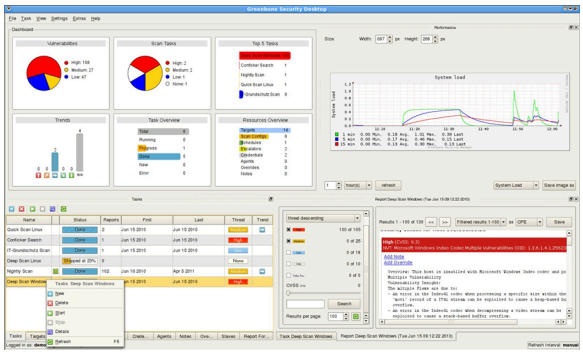
These vulnerabilities across AWS, Microsoft Azure, and Google Cloud Platform illustrate the ongoing and multifaceted security challenges in cloud computing. They emphasize the need for continuous monitoring, regular updates, and the adoption of best practices in security to protect against evolving threats. As cloud technologies advance, maintaining robust and resilient cloud security architectures becomes increasingly crucial for safeguarding data and ensuring the integrity of cloud-based systems.

Automated tools for vulnerability scanning and assessment [6.2]

In cloud computing, deploying automated tools for vulnerability scanning and assessment is crucial for maintaining robust security. These tools offer diverse capabilities, from identifying known vulnerabilities to simulating real-world attacks, thus playing a pivotal role in safeguarding cloud environments. Nessus by Tenable stands out as a widely utilized tool for vulnerability scanning. It offers comprehensive scanning capabilities, enabling the identification of known vulnerabilities in cloud environments. Nessus is particularly valued for its detailed reporting and the ability to prioritize vulnerabilities based on severity, aiding organizations in focusing their remediation efforts effectively.

The Qualys Cloud Platform is another significant player, offering a cloud-based vulnerability management solution. It provides real-time visibility into security risks, compliance issues, and policy violations, making it an essential tool for cloud infrastructure and application security assessments.

OpenVAS, the Open Vulnerability Assessment System, is an open-source tool that offers customizable vulnerability scanning capabilities. Its adaptability makes it a popular choice for integration into larger security testing frameworks, particularly for identifying security weaknesses in cloud environments.



Metasploit by Rapid7, a leading penetration testing framework, enables security professionals to simulate real-world attacks. This helps in identifying and exploiting vulnerabilities within cloud environments. Its extensive collection of pre-built exploits and payloads renders it a powerful resource for ethical hacking. Burp Suite Professional is preferred for web application security testing in cloud environments. It encompasses a suite of tools for web vulnerability scanning, manual testing, and automated exploitation of identified vulnerabilities, making it a comprehensive solution for penetration testing. Lastly, Kali Linux, renowned for its use in penetration testing and ethical hacking, has many pre-installed tools. Its suitability for cloud security assessments is well-recognized, making it a staple in the toolkit of security professionals focusing on cloud environments. Collectively, these tools provide a robust framework for identifying, assessing, and mitigating vulnerabilities in cloud environments, thereby playing a critical role in maintaining cloud security.

Comprehensive Security Features and Services in Microsoft Azure Cloud [8]

Microsoft Azure, a leading cloud service provider, offers a comprehensive array of security features and services designed to protect customer data and applications in the cloud. These offerings span various aspects of cloud security, addressing vulnerabilities and enhancing the overall security posture of cloud environments.

[11]Azure's security begins with Microsoft Defender for Cloud, which provides security management and advanced threat protection across hybrid cloud workloads. Microsoft Sentinel, a scalable, cloud-native solution, delivers intelligent security analytics and threat intelligence. Azure Key Vault secures sensitive information like passwords and connection strings, while Azure Monitor Logs offers a monitoring service for operational insights. Azure Dev/Test Labs aids developers and testers in creating environments in Azure efficiently and cost-effectively. In the realm of storage security, Azure Storage Service Encryption automatically encrypts data in Azure storage. Azure StorSimple Virtual Array manages storage tasks between on-premises arrays and Azure cloud storage. Client-side encryption for blobs enhances data security before uploading to Azure Storage. Azure Storage shared access signatures, and Account Keys provide controlled access to storage resources, while Azure File Shares offer fully managed file shares accessible via standard protocols. Azure Storage Analytics generates logs and metrics for data in storage accounts.

For database security, Azure SQL Firewall and Connection Encryption protect against network-based attacks and unauthorized access. Azure SQL Always Encrypted and Transparent Data Encryption safeguards sensitive data and encrypts data at rest. Azure SQL Database Auditing tracks database events, and Virtual Network Rules control communications to database servers. In identity and access management, Azure Role-Based Access Control ensures users access only necessary resources. Azure Active Directory, a cloud-based identity service, supports multiple identity management services. Azure Active Directory B2C is a customer identity access management solution, while Azure Active Directory Domain Services provides managed domain services. Azure AD Multi-Factor Authentication adds an extra layer of security.

Azure Backup and Azure Site Recovery are pivotal in data backup and recovery, ensuring data integrity and availability in case of failures. Azure's networking security features include Network Security Groups for traffic filtering, Azure VPN Gateway for cross-premises access, and Azure Application Gateway for web traffic management. The Web Application Firewall (WAF) protects against common exploits, and Azure Load

Balancer and ExpressRoute manage network traffic. Azure Traffic Manager is a DNS-based traffic load balancer, while Azure Active Directory Application Proxy secures remote access to on-premises web applications. Azure Firewall and DDoS protection provide network-level security, and Virtual Network service endpoints ensure secure connectivity to Azure services. Azure Private Link offers private connectivity to Azure services, Azure Bastion enables secure VM connections, and Azure Front Door provides web application protection.

In evaluating these offerings, it's evident that Azure's security capabilities are extensive. However, their effectiveness hinges on proper configuration, monitoring, and adherence to best practices. Regular security assessments, appropriate access controls, and staying updated with Azure's security recommendations are crucial for leveraging the full potential of Azure's security features.

Implementations and Tools, [10,2]

In the realm of automating security testing in Microsoft Azure, a suite of tools and implementations significantly enhances the security posture and streamlines the identification and remediation of vulnerabilities. Azure Security Center, pivotal in Azure, is enabled at the subscription level to assess the security posture of resources automatically. Users utilize the dashboard to access security recommendations and configure notifications for alerts, with the ability to integrate with vulnerability scanners and security assessment tools for automated testing and remediation.

Complementing this, Azure DevOps is a comprehensive cloud-based platform for development and deployment, including configuring CI/CD pipelines using Azure Pipelines. It allows for incorporating security testing tasks such as Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), or vulnerability scanning. This integration, achievable using tools like SonarQube or OWASP ZAP or Azure services like Azure Pipelines or Azure Container Registry, is configured to run automatically, identifying security issues during pipeline execution. Further enhancing Azure's security capabilities, Azure Advisor, a built-in service within the Azure portal, analyzes resources and provides best practice recommendations. Users can access these recommendations, prioritizing them based on impact and relevance, and follow detailed insights for enhancing resource security through configuration adjustments or applying specific security controls. Additionally, Azure Policy is managed via the Azure portal and set up at the subscription or management group level, allowing users to define and assign policies based on security requirements, compliance standards, or best practices. This tool automatically enforces these policies, ensuring resources adhere to specified security configurations and facilitating compliance monitoring and remediation of non-compliant resources. Lastly, Azure Sentinel, a cloud-native service configured in the Azure portal, connects various data sources like Azure activity logs, security logs, and external threat intelligence. Users can configure alert rules and detection mechanisms tailored to their security needs, utilizing machine learning and analytics for detecting security incidents and anomalies. Azure Sentinel provides dashboards, workbooks, and investigation tools for real-time visualization and response to security events. For detailed guidance on implementing and using these tools, the Azure documentation offers comprehensive step-by-step guides and tutorials. Users are encouraged to refer to the Azure portal and specific tool documentation for in-depth instructions and best practices in automating security testing within Microsoft Azure.

Mitigating Common Vulnerabilities in Cloud APIs: Strategies and Solutions, [9.3.]

The OWASP 2023 list of common vulnerabilities in APIs presents a range of concerns in cloud environments [12], each with specific mitigation strategies. Broken object-level authorization, where endpoints manage object identifiers, creates a wide attack surface, addressed by using an API gateway and implementing object-level authorization checks with mandatory access tokens. Similarly, Broken Authentication stemming from compromised systems or exposed API keys, necessitates secure user authentication, recommending OAuth flows and Mutual TLS for machine-to-machine access. Issues like excessive data exposure and mass assignment, categorized under Broken Object Property Level Authorization, are tackled by limiting data exposure to authorized parties and using OAuth Scopes and Claims for access control.

Unrestricted Resource Consumption, a precursor to DoS incidents, can be controlled by setting rate limits and response restrictions through an API gateway or management solution. Complex access control policies leading to Broken Function Level Authorization are best managed by adopting OpenID Connect and outsourcing access management to specialized tools. Unrestricted Access to Sensitive Business Flows, which risks automated exploitation of business processes, requires a hacker mindset for threat analysis, implementation of authorization rules, and multi-factor authentication. Server-side request Forgery (SSRF) vulnerabilities, resulting from unvalidated user-provided URIs, are mitigated through OAuth and OpenID Connect designs and stringent URI validation.

Security Misconfiguration issues, often due to neglected configurations or non-adherence to best practices, call for tailored configurations and careful handling of error messages to avoid data leaks. Managing many API endpoints, as in Improper Inventory Management, involves planning API versions, aligning documentation with live endpoints, and relying on an API Specification as a reliable reference. Finally, the Unsafe Consumption of APIs, where developers overly trust third-party API data, is addressed by using an API Gateway, avoiding vulnerable input formats, and monitoring for abnormal API request behaviors. Collectively, these solutions aim to bolster the security and integrity of APIs in cloud environments, ensuring robust protection against various threats.

Result, [10.2]

In Microsoft Azure, the implementation of various tools for automating security testing is streamlined and user-friendly, each tool serving a specific purpose in enhancing security. Azure Security Center, enabled at the subscription level,

automatically assesses the security posture of resources, offering recommendations on its dashboard. Users can configure and integrate alerts with vulnerability scanners for comprehensive automated testing. Complementing this, Azure DevOps, a versatile cloud-based platform, facilitates creating projects and configuring CI/CD pipelines. It includes security testing tasks such as SAST, DAST, or vulnerability scanning by integrating tools like SonarQube or OWASP ZAP, ensuring security issues are automatically identified during pipeline execution.

Further enhancing Azure's security capabilities, Azure Advisor, accessible within the Azure portal, analyzes resources to provide best practice recommendations. Users can review, prioritize, and act on these suggestions to bolster their security posture. In parallel, Azure Policy, managed through the Azure portal, enables users to define and enforce policies at the subscription or management group level, ensuring compliance and facilitating the remediation of non-compliant resources.

Azure Sentinel, a cloud-native service, is adept at connecting to various data sources, including Azure activity logs and security logs. It allows for configuring alert rules and detection mechanisms, utilizing machine learning and analytics to detect and respond to real-time security incidents. Azure's documentation provides detailed step-by-step guides and tutorials for each tool, offering users comprehensive instructions and best practices for effective implementation and usage, thereby ensuring a robust security framework within the Azure environment.

Conclusion

The research presented in this paper has comprehensively explored the realm of automated tools for cloud security testing, underscoring their indispensable role in the modern landscape of cloud computing. These tools, characterized by their efficiency, accuracy, and cost-effectiveness, represent a significant advancement over traditional manual testing methods. They adeptly address the complexity and scale of cloud operations, reducing manual efforts and minimizing human errors, which are crucial in the intricate and dynamic environment of cloud computing. However, deploying and effectively utilizing these automated tools are not without challenges. The complexity of cloud environments, the need for continuous updates and refinements to tackle evolving threats, and integration issues pose significant challenges. These challenges necessitate a strategic approach that includes ongoing maintenance, adherence to best practices, and staying informed about the latest trends and techniques in cloud security.

Looking ahead, automated cloud security testing is poised for significant advancements. The potential incorporation of advanced machine learning and AI technologies promises to enhance the capabilities of these tools further, enabling more effective detection and response to emerging threats. Additionally, as the landscape of legal and regulatory requirements evolves, particularly concerning data privacy and compliance, automated tools must adapt to help organizations meet these standards. The importance of collaboration and information sharing within the cloud security community cannot be overstated. The collective security posture can significantly strengthen by pooling knowledge about vulnerabilities and threats. Moreover, as tools become more sophisticated, the emphasis on user education and training will become increasingly important. Ensuring that security teams are well-versed in the latest tools and techniques is essential for maximizing the effectiveness of these solutions.

Acknowledgments

This work was supported partially by the European Union in the framework of ERASMUS MUNDUS, Project CyberMACS (Project #101082683) (https://cybermacs.eu).

References

[1] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[2] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of network and computer applications, 36(1), 42-57.

[3] Tao, D., Lin, Z., & Lu, C. (2015). Cloud platform based automated security testing system for mobile internet. Tsinghua Science and Technology, 20(6), 537-544.

[4] Jayakody, J. A. D. C. A., Perera, A. K. A., & Perera, G. L. A. K. N. (2019, December). Web-application security evaluation as a service with cloud native environment support. In 2019 International Conference on Advancements in Computing (ICAC) (pp. 357-362). IEEE.

[5] Krishnaveni, S., Prabakaran, S., & Sivamohan, S. (2016). Automated vulnerability detection and prediction by security testing for cloud SAAS. Indian Journal of Science and Technology, 9(1).

[6] Zhang, L., Xie, T., Tillmann, N., de Halleux, P., Ma, X., & Lv, J. (2012). Environment modeling for automated testing of cloud applications. IEEE Software, Special Issue on Software Engineering for Cloud Computing, 1(20).

[7] Yang, Y., Dong, X., Cao, Z., Shen, J., Li, R., Yang, Y., & Dou, S. (2024). EMPSI: Efficient multiparty private set intersection (with cardinality). Frontiers of Computer Science, 18(1), 181804.

[8] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4, 1-13.

[9] Cyber security threats, challenges and defence mechanisms in cloud computing (2020) by Abdullah Aljumah and Tariq Ahamed Ahanger. https://doi.org/10.1049/iet-com.2019.0040

[10] https://www.cvedetails.com/vulnerability-list/

[11]https://learn.microsoft.com/en-us/azure/security/fundamentals/ official Microsoft Azure fundamental pdf

[12]https://github.com/OWASP/www-project-api-security/blob/master/index.md

[13] NIST Cloud Computing Standards Roadmap Working Group by Michael Hogan Fang Liu Annie Sokol Jin Tong in July 2011

[14] Comprehensive review on intelligent security defenses in cloud by Mohamad Mulham Belal and Divya Meena Sundaram in November 2022, Pages 9102-9131

[15] MoniLog: An Automated Log-Based Anomaly Detection System for Cloud Computing Infrastructures, Arthur Vervaet (2021) 2021 IEEE 37th International Conference on Data Engineering (ICDE)

[16] Casola, V., De Benedictis, A., Rak, M. and Villano, U. (2020) 'A methodology for automated penetration testing of cloud applications', Int. J. Grid and Utility Computing, Vol. 11, No. 2, pp.267–277 https://doi.org/10.1504/IJGUC.2020.105541

[17] An Open-Source Cloud Testbed for Security Experimentation by Francesco Minna; Fabio Massacci. Published in: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid) DOI: 10.1109/CCGrid54584.2022.00086

[18] Security in Cloud Computing: A Systematic Literature Review by Babak Bashari Rad, Article in International Journal of Control Theory and Applications · August 2016

Biography

Hamid Ghazizadeh received his Master's in Computer Science, focusing on Cyber Security in 2023 from SRH University. His research interests include computer security, cloud security, security analysis, software security and Open Source Intelligence (OSINT).

Gerrit Tamm is a Professor of Economics, Computer Science, and Information Systems at SRH University Berlin and University Stellenbosch South Africa.
After studying industrial engineering and business administration at the TU Berlin and the UCB he received his doctoral degree at the Humboldt-University Berlin with a scholarship from the German Research Foundation (DFG). He has published 8 books, 16 journal articles and over 30 conference papers on the topic of cloud computing. After a post doc at the University St. Gallen, Switzerland he got his first full professorship at the Erfurt University of Applied Sciences. He was the executive director of the BMBF-funded Berlin Research Center on Internet Economics "Internet and Value Chains - InterVal" and the BMWi-funded Research Center of Collaboration and RFID "Ko-RFID" in Berlin. He was founder and executive director of the electronic business forum, absolvent.de and the Asperado GmbH. Prof. Tamm is an assessor and expert for the European Commission, four German federal ministries and the Association of the German Internet Industry.

Reiner Creutzburg is a retired Professor of Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019, he has been a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology.
He has been a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005.
In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.