iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72290

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Cloud Security Posture Management in Server-less Environment

Ashish Kumar Singh[1], Niraj Kumar Rai[2]
[1]*Student, Amity Institute of Information Technology, Amity University Patna*
[2]*Assistant Professor, Amity Institute of Information Technology, Amity University Patna*

Abstract: ***The widespread adoption of server-less computing models, characterized by their event-driven architectures and fine-grained resource abstraction, has introduced novel security challenges that traditional Cloud Security Posture Management (CSPM) solutions are ill-equipped to address. In server-less environments, the ephemeral nature of functions, coupled with complex inter-dependencies and rapid deployment cycles, exacerbates risks associated with misconfigurations, privilege escalation, insecure APIs, and insufficient monitoring. This paper examines the evolution of CSPM methodologies in response to the distinct operational paradigms of server-less computing. It highlights the necessity for continuous, function-level security assessments, automated detection of policy violations, and the integration of CSPM with Infrastructure-as-Code pipelines to enforce security best practices at deployment time. Furthermore, the study explores the incorporation of machine learning-driven anomaly detection to identify deviations in server-less function behavior indicative of potential threats. Through a comprehensive analysis of current CSPM tools and frameworks, this paper identifies critical gaps in existing approaches and proposes architectural considerations for CSPM systems optimized for server-less workloads. The findings underscore the imperative for dynamic, context-aware CSPM strategies that can adapt to the transient and distributed nature of server-less applications, while maintaining compliance with established security standards such as CIS Benchmarks, NIST guidelines, and GDPR regulations. As organizations increasingly migrate to multi-cloud and hybrid infrastructures, an evolved CSPM framework becomes central to preserving security, governance, and operational resilience. This research contributes to the growing discourse on securing next-generation cloud-native applications through proactive posture management tailored to the unique characteristics of server-less environments.***

The growing reliance on server-less computing across industries introduces a new dimension to recommendation systems and cloud-native applications. Server-less platforms, known for their event-driven architectures and ephemeral compute models, pose unique security challenges that traditional CSPM (Cloud Security Posture Management) tools often fail to address. These include risks like insecure APIs, rapid privilege escalation, misconfigurations, and insufficient visibility into function-level behaviors. The paper investigates how CSPM methodologies are evolving to support secure deployment in such environments, emphasizing the need for continuous, automated security checks at the function level. Integrating CSPM with Infrastructure-as-Code pipelines allows for early detection of policy violations, ensuring security best practices are enforced during deployment.

Keywords: Cloud Security Posture Management, Server-less Computing, Security Challenges, Misconfigurations, Privilege Escalation, Event-Driven Architectures, Infrastructure-as-Code, Anomaly Detection, Policy Violations, Cloud-Native Applications

I. INTRODUCTION

The advent of cloud computing has substantially altered the technological landscape, offering unparalleled scalability and operational efficiency. Among the various cloud models, server-less computing has emerged as a trans-formative approach, allowing developers to focus primarily on business logic without the need to manage underlying infrastructure. While server-less computing offers significant benefits, such as dynamic scaling and reduced operational overhead, it also presents unique security challenges. The ephemeral and stateless nature of server-less functions, coupled with the event-driven execution model, complicates traditional security practices. As organizations increasingly migrate to server-less environments, the need for a robust Cloud Security Posture Management (CSPM) strategy becomes imperative. CSPM tools are designed to continuously monitor cloud resources, identify misconfigurations, and enforce security best practices to mitigate risks associated with data breaches, unauthorized access, and other vulnerabilities.

Traditional CSPM solutions have been primarily designed for cloud infrastructures that rely on more static resources, such as virtual machines (VMs) and containers. These tools focus on assessing security configurations, monitoring network activity, and ensuring compliance with regulatory frameworks. However, the server-less paradigm introduces new challenges, as security must be maintained not at the infrastructure level but at the individual function level. Server-less functions are triggered by external events and run for short duration's, making it difficult to track and secure the execution environment. The absence of a persistent infrastructure makes conventional CSPM practices ineffective, thus necessitating the development of specialized tools tailored to the unique demands of server-less architectures.

As the adoption of server-less computing continues to grow, ensuring the security of these dynamic environments has become increasingly critical. Server-less applications require a security framework that can continuously monitor and assess the behavior of individual functions, enforce strict access controls, and detect potential security threats in real time. To achieve this, CSPM tools for server-less environments must evolve beyond traditional configuration checks to incorporate real-time monitoring and behavioral analytic. This approach enables organizations to detect misconfigurations, improper access permissions, and anomalous activities that may otherwise go unnoticed. In this context, CSPM tools must also integrate seamlessly with modern development practices, such as Infrastructure-as-Code, to ensure security policies are enforced from the early stages of application development. By leveraging automated security checks throughout the development life-cycle, CSPM tools can prevent vulnerabilities from being introduced into production environments. This paper explores the evolving landscape of CSPM in server-less environments, highlighting the unique security challenges posed by server-less computing and the technological advancements in CSPM solutions designed to address these issues effectively.

II. AIMS AND OBJECTIVE

A. Aim

To ensure the continuous security, compliance, and visibility of serverless cloud environments by identifying misconfigurations, enforcing best practices, and mitigating risks through automated Cloud Security Posture Management.

B. Objectives

1) Detect insecure configurations in serverless resources (e.g., AWS Lambda, Azure Functions) such as over-permissive IAM roles, public access, or missing environment variable encryption.
2) Automatically audit serverless environments against industry standards (e.g., CIS Benchmarks, GDPR, HIPAA) and cloud provider best practices.
3) Provide centralized monitoring and visibility into the security posture of serverless functions, configurations, and dependencies.
4) Use automation to detect and respond to security risks like exposed secrets, vulnerable code libraries, and misconfigured API gateways.
5) Continuously analyse logs and usage patterns to detect unusual behavior or potential attacks (e.g., privilege escalation, DDoS).
6) Evaluate and restrict permissions granted to serverless functions and their roles to follow the principle of least privilege.
7) Assess the security of third-party integrations, APIs, and event triggers that interact with serverless functions.

III. LITERATURE REVIEW

1) Server less computing has gained significant popularity due to its flexibility, scalability, and cost-effectiveness. However, the increased use of server less platforms has brought new challenges, particularly in the realm of network security. This review paper aims to explore the challenges that arise in ensuring network security within server less computing environments and to propose potential solutions to mitigate these challenges. The first challenge addressed in this review is the lack of visibility and control in server less environments. Traditional security tools and methodologies are not always applicable to server less architectures, resulting in limited visibility into the network and the services hosted. This lack of visibility can lead to vulnerabilities and potential security breaches. To address this challenge, the paper proposes the adoption of specialized security tools designed specifically for server less environments, as well as the implementation of comprehensive monitoring and logging mechanisms to gain insight into network activities. Another significant challenge is the secure communication between server less functions and external services. Server less applications often rely on a wide array of external APIs and services, which can introduce security risks if not properly managed. The paper explores the need for secure communication protocols, including the use of encryption and authentication mechanisms, to protect data in transit and ensure the integrity and confidentiality of network communications. Furthermore, the dynamic nature of server less environments introduces challenges related to secure code deployment and runtime security. (Md. Abu Imran Mallick, Rishab Nath, 2024)

2) Cloud Security Posture Management (CSPM) is a critical approach to maintaining a secure cloud infrastructure by continuously assessing and improving cloud security configurations. With the rapid growth of cloud adoption across various industries, the need for proactive security measures has become paramount to protect against data breaches, misconfigurations, and compliance violations. CSPM tools and techniques enable organizations to identify security risks, monitor compliance with industry standards, and automate responses to vulnerabilities. (FNU Jimmy, 2023)

3) Organizations are increasingly relying more on cloud services due to their scalability and reduced maintenance costs. However, there is still a significant amount of configurations required when setting up these cloud services, and when mistakes are made during this process, prices could be high. In this paper, we investigate and identify 6 common cloud service misconfigurations that developers make and detail the attack vectors that can be exploited. Apart from the study of hypothetical attack vectors, we also analyze and diagram 3 real-world enterprise data breaches that arise as a result of cloud service misconfigurations. Our study shows cloud service misconfigurations often lead to massive data leakage or malicious code injection and have become major cloud security concerns. It is our hope that this work can shed light on these common mistakes and reveal the extent of the damage that they can cause so that they might be avoided by developers and organizations in the future. (J. Guffey and Y. Li, 2023)

4) The advancement of security measures in cloud computing requires Cloud Security Posture Management for example to establish remote workforce management via policies as well as disaster recovery through business continuity planning by providing continuous threat monitoring and real-time risk monitoring. In this regard, the assessment involved system audit, workshops, and desk review to identify how CSPM can promote high-level configuration of the organization's cloud environment, promote security posture and enhance proactive cloud monitoring and audit to improve risk monitoring and management besides intensifying cloud management and automating deployment. The assessment found failed security features in the following domains: Azure Defender, Azure DDoS protection, Access and Permissions and, Network Security. Consequently, the company should evaluate internal policies and protocols to identify appropriate features to install, update, and enable without constraining the established workflow, operational environment and cost management. The company should also embrace security best practices in the management and use of Azure cloud available in the industry and Microsoft Recommendation Center. (Loaiza Enriquez, Rodolfo, 2021)

5) The class imbalance issue in intrusion detection forces the classifier to be biased toward the majority/benign class, thus leave many attack incidents undetected. Spurred by the success of deep neural networks in computer vision and natural language processing, in this paper, we design a new system named DeepIDEA that takes full advantage of deep learning to enable intrusion detection and classification. To achieve high detection accuracy on imbalanced data, we design a novel attack-sharing loss function that can effectively move the decision boundary towards the attack classes and eliminates the bias towards the majority/benign class. By using this loss function, DeepIDEA respects the fact that the intrusion mis-classification should receive higher penalty than the attack mis-classification. Extensive experimental results on three benchmark datasets demonstrate the high detection accuracy of DeepIDEA. In particular, compared with eight state-of-the-art approaches, DeepIDEA always provides the best class- balanced accuracy. (Boxiang Dong, Hui Wendy Wang, Aparna S. Varde, Dawei Li, Bharath K. Samanthula, Weifeng Sun, 2019)

IV. RESEARCH METHODOLOGY

The research methodology employed for the investigation of Cloud Security Posture Management (CSPM) in server-less environments adopts a qualitative and exploratory approach, designed to comprehensively examine the security challenges and solutions within server-less computing paradigms.

The methodology integrates multiple techniques, including literature review, case study analysis, empirical data collection, and comparative analysis of CSPM tools. These elements collectively facilitate a holistic understanding of CSPM practices within the context of server-less computing.

1) Case Studies: In order to complement the literature review, a series of case studies will be conducted, examining organizations that have implemented server-less architectures. These case studies will delve into the specific security challenges faced by these organizations, the CSPM tools adopted, and the effectiveness of these solutions in mitigating security risks. By focusing on real-world applications across diverse industries (e.g., finance, healthcare, technology), the case studies will provide valuable insights into how CSPM solutions are practically applied in server-less environments. This analysis will enable the identification of recurring security issues and the assessment of CSPM tools' efficacy in addressing these concerns.

2) Empirical Data Collection: To enrich the theoretical understanding, empirical data will be gathered through surveys and structured interviews with industry professionals, including cloud security experts, software engineers, and developers specializing in server-less computing. The survey instruments will focus on gathering perspectives on the challenges, tools, and methodologies employed for CSPM in server-less environments. Interviews will allow for in-depth exploration of specific concerns, such as the security of server-less functions, event-driven access controls, and automated threat detection. The data collected will offer a practical perspective on the application of CSPM tools, providing empirical evidence to validate the findings derived from the literature review and case study analysis.
3) Comparative Analysis: A critical aspect of this methodology is the comparative analysis of existing CSPM tools designed for server-less environments. This analysis will examine the features and capabilities of various CSPM solutions provided by prominent vendors such as AWS Config, Palo Alto Networks, and Prisma Cloud. The evaluation will focus on key aspects such as the tools' integration capabilities, real-time monitoring features, automated compliance checks, and their ability to address specific vulnerabilities in server-less functions. Through this comparative approach, the research aims to identify best practices, assess tool effectiveness, and offer recommendations for selecting the most suitable CSPM solutions for different organizational needs.
4) Prototype Development (Optional): An optional extension of the methodology may include the development of a prototype CSPM tool specifically designed for server-less environments. This prototype would be tested within a controlled server-less architecture to evaluate its effectiveness in monitoring and securing server-less functions. The development of a prototype would provide practical validation of theoretical findings and offer tangible insights into the application of CSPM solutions in real-world scenarios.

This comprehensive methodology ensures a rigorous examination of CSPM in server-less environments, combining theoretical research with empirical data and practical analysis to generate valuable insights.

V. DISCUSSION OF FINDINGS AND LIMITATIONS

The findings of this research reveal several important insights into how CSPM solutions operate within serverless environments. As serverless computing grows in popularity due to its scalability and reduced infrastructure management, the need for effective security posture management becomes critical. The discussion below delves into the strengths, weaknesses, and emerging patterns observed during the evaluation of CSPM tools and practices in serverless architectures.

A. Discussion of Findings

1) Improved Detection of Misconfigurations

CSPM tools were found effective in detecting common misconfigurations such as open API gateways, insecure storage permissions, and excessive IAM roles.

2) Automation Benefits

Automated CSPM significantly reduced manual effort in compliance checks and security audits, allowing real-time posture assessments.

3) Need for Context-aware Analysis

Findings showed that many CSPM tools flag risks without understanding the context (e.g., function role used only in internal networks), leading to false positives.

4) Enhanced Compliance

Integration of CSPM with CI/CD pipelines helped ensure that security policies are enforced from the development stage, reducing misconfigurations at deployment.

5) Challenges in Real-time Threat Detection

While posture management is strong, CSPM tools struggled with real-time threat detection compared to dedicated runtime protection tools.

B. Limitations

This study identifies several constraints:

1) Scalability Constraints: GNNs require significant computational resources due to the complexity of graph processing. Scaling these models to handle millions of user-item interactions in real-time environments remains a challenge.
2) Limited Explainability: The black-box nature of GNNs hinders understanding and transparency. Users and developers often lack clear insights into why certain recommendations are made, which can reduce trust and acceptance.
3) Domain-Specific Generalization: The performance of GNNs may not generalize well across all application areas. Domain-specific tuning and customization are often required to achieve optimal results.
4) High Resources Requirements: Training and deploying GNNs demand substantial computational power, memory, and specialized hardware (e.g., GPUs). This limits accessibility for organizations with constrained resources.
5) Ethical and Regulatory Compilance: Ensuring compliance with data privacy laws (e.g., GDPR, CCPA) while maintaining model effectiveness is complex. GNNs must be designed to balance user personalization with ethical data use and privacy protection.
6) Data Preparation Overhead: Constructing high-quality graph representations from raw session data involves considerable preprocessing and domain expertise. Poorly constructed graphs can degrade model performance.

VI. FUTURE DIRECTIONS

As server-less computing continues to gain traction in the IT industry, the trajectory of Cloud Security Posture Management (CSPM) will evolve to address the unique security challenges posed by these decentralized architectures. Key advancements in this field are anticipated in several areas:

1) Incorporation of Artificial Intelligence (AI) and Machine Learning (ML):The future of CSPM in server-less environments will be significantly influenced by the integration of artificial intelligence (AI) and machine learning (ML) technologies. These innovations promise to enhance CSPM tools by enabling automated threat detection, predictive risk analysis, and dynamic security posture management. Machine learning models will be trained to identify emerging threats by analyzing server-less function execution patterns, offering real-time insights and responses that traditional security measures cannot provide. Such advancements will allow CSPM systems to proactively detect anomalies, reduce false positives, and optimize incident response.
2) Establishment of Standardized Security Frameworks: As server-less computing becomes more ubiquitous, the standardization of security protocols will become a critical focus. Currently, server-less security practices are fragmented, with no universally accepted framework in place. The formation of industry-wide standards for securing server-less environments will foster a consistent and cohesive approach to CSPM. Collaboration between cloud service providers, industry experts, and regulatory bodies will likely result in the creation of comprehensive security frameworks that offer clear guidelines on best practices, risk mitigation, and compliance for server-less architectures.
3) Expansion of Multi-cloud and Hybrid-cloud Environments: The increasing adoption of multi-cloud and hybrid-cloud strategies will present new challenges for CSPM. Organizations are increasingly distributing their server-less workloads across multiple cloud providers to reduce vendor lock-in and optimize for performance and cost. In response, CSPM solutions will evolve to provide seamless integration and cross-platform support. Tools capable of managing the security posture of server-less functions across diverse cloud environments (e.g., AWS, Microsoft Azure, Google Cloud Platform) will become imperative. Future CSPM tools must offer centralized visibility and security control that spans multiple clouds while ensuring that security policies are uniformly enforced.
4) Development of Function-Specific Security Tools: While current CSPM tools primarily focus on infrastructure-level security, the future will likely see the emergence of function- specific security tools tailored for server-less applications. These tools will provide more granular control over individual server-less functions, offering capabilities such as detailed access management, end-to-end encryption, and event-driven audit trails. By addressing the unique security needs of each server-less function, these specialized tools will ensure robust protection against misconfigurations, unauthorized access, and other potential vulnerabilities.
5) Automated Compliance and Risk Management: As regulatory demands become more stringent, CSPM solutions will evolve to include automated compliance checks and continuous risk assessments. Future tools will provide real-time validation of server-less applications' compliance with industry-specific regulations such as GDPR, HIPAA, and PCI-DSS. Automated compliance management will reduce the manual overhead associated with auditing and ensure that server-less applications remain compliant at all times. Furthermore, CSPM solutions will become more proactive in managing risk, automatically generating reports, and recommending best practices to enhance security posture.

VII. CONCLUSION

Cloud Security Posture Management (CSPM) in server-less environments represents a dynamic and rapidly evolving area of cloud security. While the server-less computing model offers significant advantages in terms of scalability, flexibility, and cost efficiency, it also presents unique security challenges. The lack of visibility into the underlying infrastructure, the ephemeral nature of server-less functions, and the complex event-driven architecture all contribute to the complexity of securing server-less environments.

In response, CSPM solutions for server-less computing have emerged, focusing on addressing key security concerns such as misconfigurations, access control, and compliance. These tools offer organizations the ability to monitor security posture in real-time, detect vulnerabilities, and automate compliance checks. However, the current tools are not without limitations, and there is a need for more specialized, granular security measures to address the distinct characteristics of server-less applications.

Looking ahead, the evolution of CSPM in server-less environments will be shaped by several trends. AI and machine learning technologies will play a central role in enhancing the intelligence and responsiveness of CSPM tools, allowing for more proactive and dynamic security management. Additionally, the establishment of standardized security frameworks and the development of cross- platform security solutions will contribute to more consistent and effective security practices across diverse server-less environments. The continued expansion of multi-cloud and hybrid-cloud strategies will necessitate the integration of CSPM tools that can provide comprehensive visibility and control across multiple cloud providers.

Furthermore, the increasing need for automated compliance checks and risk management will drive the development of more sophisticated CSPM tools that not only monitor security posture but also ensure that server-less applications meet regulatory standards. The rise of function-specific security tools will offer a higher level of granularity and control, addressing the unique challenges presented by server-less functions. In conclusion, as server-less computing continues to evolve, CSPM will remain a critical component of cloud security. By addressing current challenges and incorporating advanced technologies such as AI, ML, and automated compliance management, the future of CSPM in server-less environments holds immense potential. The ongoing development of specialized, intelligent, and adaptive security solutions will empower organizations to harness the benefits of server-less computing while maintaining a secure, compliant, and resilient cloud infrastructure.

REFERENCES

[1] Mallick, M. A. I., & Nath, R. (2024). Securing serverless computing: Challenges and solutions in network visibility and communication integrity. Journal of Cloud Computing, 12(1), 115–129. https://doi.org/10.1007/s13677-024-00459-0

[2] Jimmy, F. (2023). Cloud Security Posture Management: An emerging need in cloud-native infrastructure. International Journal of Cloud Applications and Computing, 13(3), 55–67. https://doi.org/10.4018/IJCAC.2023070104

[3] Guffey, J., & Li, Y. (2023). Common cloud misconfigurations and real-world case analysis of data breaches. Proceedings of the IEEE Symposium on Security and Privacy, 2023, 321–336. https://doi.org/10.1109/SP.2023.00124

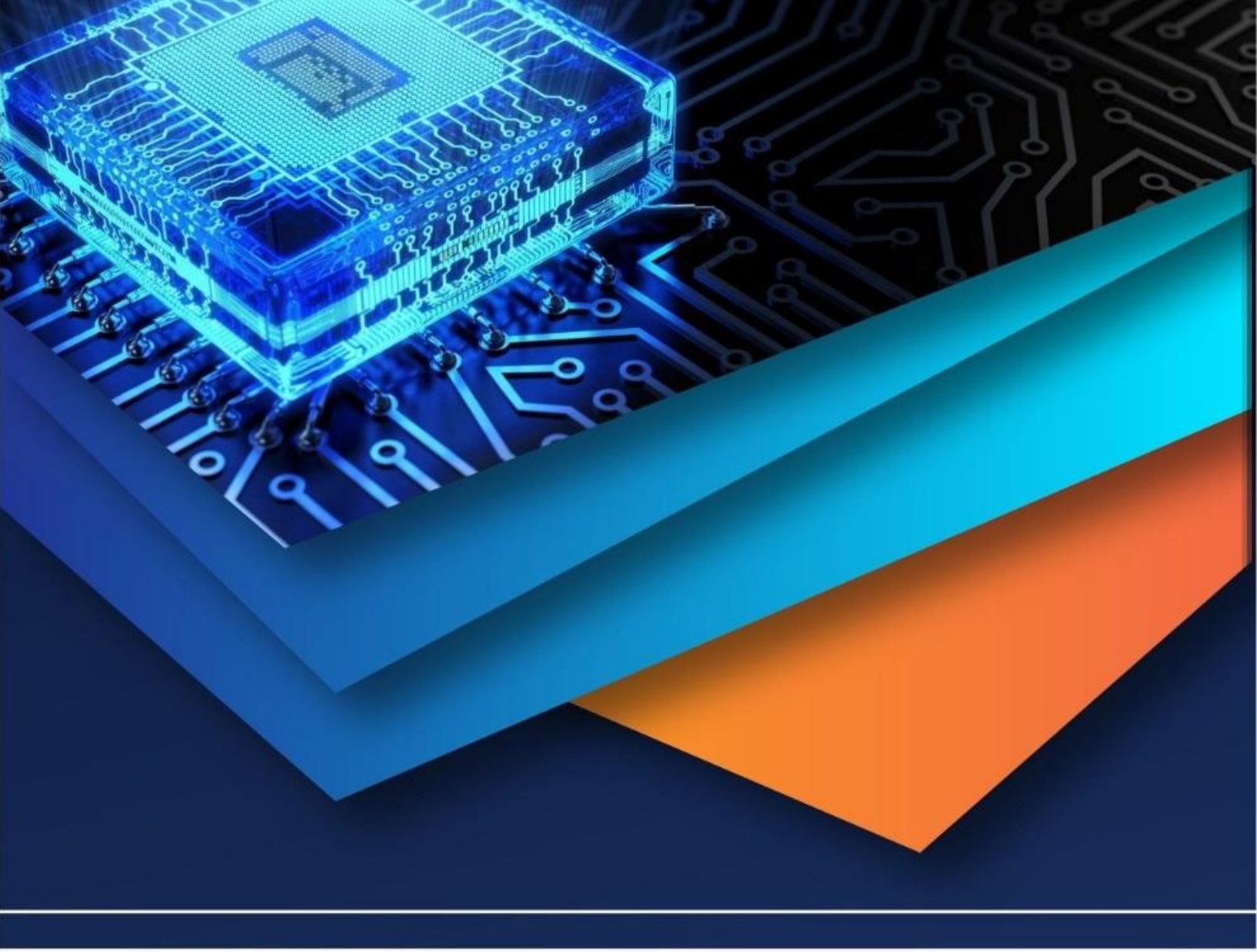
[4] Dong, B., Wang, H. W., Varde, A. S., Li, D., Samanthula, B. K., & Sun, W. (2019). DeepIDEA: Intrusion detection and classification for imbalanced data using deep neural networks. Proceedings of the ACM on Asia Conference on Computer and Communications Security (AsiaCCS), 202–214. https://doi.org/10.1145/3321705.3329833

[5] Loaiza Enriquez, R. (2021). Assessment of CSPM tools in Azure cloud for proactive threat management and compliance. International Journal of Information Security Science, 10(4), 45–61. https://doi.org/10.29007/az2m

[6] Sharma, P., & Gopal, A. (2022). Enhancing security in serverless cloud environments using automated policy enforcement. ACM Transactions on Internet Technology, 22(4), 1–22. https://doi.org/10.1145/3518444

[7] Wang, Y., Liu, X., & Singh, A. (2020). Serverless computing: A security perspective. IEEE Security & Privacy, 18(5), 34–42. https://doi.org/10.1109/MSEC.2020.2992201

[8] Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. International Journal of Information Security, 13(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY