ISSN: 2959-6386 (Online), Vol. 2, Issue 3, December 2023

Journal of Knowledge Learning and Science Technology

journal homepage: https://jklst.org/index.php/home

JKLST

EXPLORING THE INTERSECTION OF
KNOWLEDGE, LEARNING, AND SCIENCE & TECHNOLOGY:

UNLEASHING THE POWER OF SYNERGY
IN THE 21ST CENTURY

Cloud security posture management: tools and techniques

FNU Jimmy

Senior Cloud consultant, Deloitte USA

Abstract

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. This paper explores the evolving landscape of CSPM, highlighting essential tools and techniques used to safeguard cloud environments. Key tools discussed include cloud-native security services, third-party CSPM solutions, and artificial intelligence-driven automation. Techniques covered include continuous monitoring, threat detection, and compliance management. The paper aims to provide a comprehensive overview of CSPM's role in enhancing cloud security and guiding organizations toward adopting robust practices for a secure cloud posture.

Keywords: Cloud Security Posture Management (CSPM), cloud security, security configurations, misconfiguration detection, compliance monitoring, continuous monitoring, threat detection, cloud-native security, CSPM tools, automated security

Article Information:
Article history: *Received:* 04/10/2023 *Accepted:* 30/10/2023 *Online:* 04/11/2023 *Published*: 20/11/2023
DOI: https://doi.org/10.60087/jklst.vol2.n3.p622
[i] **Correspondence author:** FNU Jimmy **Email:** Fnujim1810@gmail.com

1. INTRODUCTION

As organizations increasingly adopt cloud computing to improve scalability, efficiency, and agility, ensuring robust security in these environments has become a top priority. The dynamic and distributed nature of cloud platforms, however, presents unique security challenges that differ from traditional on-premises systems. Misconfigurations, unauthorized access, data leaks, and compliance risks are among the most common vulnerabilities that can compromise cloud infrastructure [1]. To address these risks, Cloud Security Posture Management (CSPM) has emerged as a strategic approach, helping organizations proactively manage and enhance their cloud security posture.

CSPM encompasses a set of tools and techniques aimed at continuously identifying, assessing, and remediating security risks within cloud environments. These tools work by scanning cloud configurations to detect vulnerabilities, providing insights on compliance issues, and enabling automation to reduce human error. For instance, CSPM solutions can help organizations detect misconfigurations in Identity and Access Management (IAM) settings, data storage permissions, network configurations, and other critical areas where errors are frequently introduced. Moreover, CSPM tools align with industry standards and regulatory requirements, offering automated checks against frameworks such as GDPR, HIPAA, and ISO 27001 [2].

Beyond compliance and configuration assessments, modern CSPM solutions integrate advanced technologies, such as machine learning and artificial intelligence, to enhance threat detection and response capabilities. By analyzing vast amounts of cloud data, these tools can identify patterns, detect anomalies, and provide real-time alerts for potential threats. Additionally, CSPM enables organizations to adopt a proactive, rather than reactive, security approach, making it an essential component of a comprehensive cloud security strategy.

This paper explores the essential tools and techniques involved in CSPM, emphasizing their roles in enhancing cloud security. It discusses cloud-native and third-party CSPM solutions, compares their features, and examines how CSPM enables organizations to maintain a strong security posture while embracing the benefits of cloud technology.

Objectives

1. To explore the concept and importance of Cloud Security Posture Management (CSPM):
   Investigate the role of CSPM in securing cloud environments and why it is essential for organizations to adopt proactive security measures in cloud computing.
2. To identify and analyze key CSPM tools:
   Examine widely used CSPM tools, both cloud-native and third-party solutions, discussing their features, functionalities, and suitability for different cloud environments and business needs.
3. To outline critical CSPM techniques for threat detection and compliance:
   Review effective techniques employed in CSPM for identifying misconfigurations, managing compliance, and detecting potential threats within cloud infrastructures.
4. To evaluate the benefits of automation and AI in CSPM:
   Assess how automation and artificial intelligence enhance CSPM capabilities, streamline security processes, and reduce human error in managing cloud security.
5. To provide guidelines for adopting CSPM practices effectively:
   Offer recommendations for organizations seeking to integrate CSPM into their security framework, emphasizing best practices for a secure and compliant cloud posture.
6. To analyze CSPM's role in regulatory compliance:
   Discuss CSPM's effectiveness in maintaining adherence to industry regulations (such as GDPR, HIPAA, and ISO 27001) and ensuring a secure cloud infrastructure.

2. RESEARCH METHOD

This research employs a mixed-method approach to provide a comprehensive analysis of Cloud Security Posture Management (CSPM), including its tools, techniques, and their effectiveness in enhancing cloud security. The research method involves two primary stages: a systematic literature review and a comparative analysis of CSPM tools.

1. Systematic Literature Review:

To establish a foundational understanding of CSPM, an extensive literature review was conducted. Academic papers, industry reports, and case studies from reputable databases such as IEEE Xplore, Google Scholar, and ACM Digital Library were analyzed. The review focused on identifying key CSPM techniques, common security issues addressed by CSPM, and industry best practices for cloud security management. Studies covering cloud misconfiguration, compliance monitoring, automated threat detection, and remediation strategies were included to capture the full scope of CSPM practices.

2. Comparative Analysis of CSPM Tools:

To evaluate CSPM tools, a comparative analysis was performed on a selection of widely used cloud security tools. This analysis included both cloud-native solutions (such as AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center) and third-party CSPM providers (like Prisma Cloud, Dome9, and Lacework). Each tool was assessed based on criteria such as:

- Functionality: The range of features offered, including configuration assessments, compliance monitoring, and threat detection.
- Automation Capabilities: The level of automation available for tasks like configuration scanning, alerting, and remediation.
- Integration with Cloud Platforms: The tool's compatibility with popular cloud service providers (e.g., AWS, Azure, Google Cloud).
- User-Friendliness: The ease of use and accessibility for security teams.
- Compliance Support: Alignment with regulatory frameworks such as GDPR, HIPAA, and SOC 2.

3. Case Studies and Practical Applications:

To further assess the effectiveness of CSPM tools and techniques, case studies from organizations in various industries were examined. These cases provide practical insights into how CSPM is implemented, the challenges organizations face in securing cloud environments, and the outcomes achieved. By analyzing real-world applications, this research highlights how CSPM practices help organizations detect and mitigate vulnerabilities, reduce cloud security risks, and enhance compliance efforts.

3. 4. DATA ANALYSIS:

The data gathered from the literature review, tool comparison, and case studies was analyzed to identify trends, common challenges, and emerging best practices in CSPM. Qualitative analysis was used to interpret findings from the literature, while a quantitative scoring system helped compare CSPM tools based on predefined criteria. The combined insights provide a holistic view of CSPM, offering guidance for organizations seeking to implement robust cloud security strategies.

This mixed-method approach ensures a well-rounded exploration of CSPM tools and techniques, bridging theoretical understanding with practical implications and offering actionable insights for cloud security practitioners.

Background Study

In today's digital landscape, technology is evolving at an unprecedented pace, making cloud security a top priority for organizations worldwide. As more businesses transition to cloud infrastructure, new security challenges and vulnerabilities arise, necessitating robust strategies to protect sensitive data and ensure compliance. Cloud Security Posture Management (CSPM), when aligned with cybersecurity standards like the NIST Cybersecurity Framework (CSF) v1.1, is instrumental in maintaining secure and compliant cloud environments [1]. This approach emphasizes the need for advanced, CSF-based CSPM tools that leverage Big Data and AI, particularly for cloud service providers such as Amazon Web Services (AWS).

As organizations expand their reliance on cloud services for critical operations, the demand for CSPM solutions intensifies. CSPM is crucial for identifying, assessing, and mitigating security risks within cloud ecosystems, supporting data protection efforts and adherence to regulatory requirements. An organization with a well-managed cloud security posture significantly reduces its risk of data breaches, unauthorized access, and other security incidents. By proactively addressing threats, CSPM tools enhance customer trust, broaden client bases, and fundamentally safeguard organizational data [3].

The National Institute of Standards and Technology (NIST) recognizes the value of cybersecurity research, as seen in initiatives like its Technology Innovations Program (TIP), which includes resources like white papers on sustainability. The NIST CSF, a comprehensive set of cybersecurity best practices, assists organizations in enhancing their security posture by reducing risks. This adaptable framework allows organizations to tailor its five main functions—Identify, Protect, Detect, Respond, and Recover—to their specific needs, risks, and regulatory demands [4].

A CSF-based CSPM tool, equipped with Big Data and AI capabilities, offers a powerful solution for organizations leveraging cloud services. With continuous monitoring, automated threat detection, misconfiguration alerts, and integrated threat intelligence, such a tool effectively analyzes large volumes of security data, identifying patterns and trends indicative of potential threats. AI integration accelerates risk identification and response, enhancing automation and reducing human error for faster incident resolution. Following NIST CSF v1.1, a CSPM tool can guide organizations in proactively managing cloud security risks, establishing a stronger security foundation and achieving regulatory compliance. Utilizing Big Data and AI alongside a CSPM tool offers a robust solution for strengthening cloud security, enabling organizations to handle the complexity of cloud data with greater confidence and agility [5]. Driven by this potential, we propose a CSPM tool designed to enhance the security posture of cloud-based assets, focusing particularly on the AWS environment. Grounded in the NIST CSF v1.1 framework, this tool is poised to make a significant contribution to cybersecurity research. Our primary contributions are as follows:

1. Developing a CSPM tool capable of advanced threat detection, proactive monitoring, and real-time misconfiguration alerts.

2. Demonstrating the integration of AI and Big Data management within CSPM to illustrate their impact on cloud security posture.
3. Implementing the tool within the AWS environment to evaluate its practical application and effectiveness for secure, ubiquitous data access.

Cloud Security Posture Management (CSPM) and related security challenges in cloud environments have been explored extensively due to the rapid increase in cloud adoption, which has introduced potential vulnerabilities. Early research in 2010 by Johnson et al. [6] examined weaknesses in cloud security using commercial security tools, proposing new methods and tools to strengthen cloud security practices. This study provided some of the first insights into the limitations of commercially available security solutions for cloud environments.

Dong et al. [7] introduced DeepIDEA, a system leveraging deep learning for high-accuracy intrusion detection in imbalanced datasets. By employing a specialized attack-sharing loss function, their system reduced biases associated with majority/benign classes, enhancing classification performance. This method has valuable implications for cloud security.

Enriquez et al. [8] focused on vulnerabilities in cloud environments caused by misconfigurations and inadequate change control. Their research emphasized CSPM as a viable solution to enhance cloud security configurations and organizational monitoring. Specifically, they examined security flaws in Azure services, including Azure Defender, Azure DDoS protection, and access permissions, recommending internal protocol adjustments to improve security without impacting workflows or cost efficiency. Limitations of the study included restricted data collection due to reliance on interviews with a single organization.

An et al. [9] addressed the unique threats cloud environments face, evaluating existing graphical security models such as Attack Graphs and Attack Trees, which lacked automation and comprehensive scope. To address these limitations, they proposed "CloudSafe," a system integrating various tools for automating cloud security assessments. Testing on AWS demonstrated that CloudSafe could gather security data and generate detailed security reports to inform users and providers of cloud security posture.

Research by Chandra et al. discussed the need for scalable infrastructure to manage and analyze big data within cloud environments, comparing data management technologies SQL and Hive. The study evaluated their effectiveness in cloud data management, offering recommendations for cloud-based data analytics across real-world applications.

Pawlish et al. presented a survey [9] on the rising adoption of the DevOps paradigm for cloud-based data management and analytics, emphasizing the benefits for creating sustainable "green" businesses. Using Geographic Information Systems (GIS) as an example, the paper noted a shift to cloud and hybrid models to reduce environmental impact and addressed privacy and security challenges associated with cloud adoption. In earlier work [9], the author explored using cloud services to improve data center efficiency, focusing on security, privacy, and accessibility.

Our research goes a step further by developing a CSPM tool that integrates Big Data analytics and AI to enhance cloud security posture in real-time. While prior studies have explored CSPM tools and methods, our approach uniquely combines large-scale data analysis with AI-driven capabilities to proactively manage security in cloud environments. This tool is designed to provide a more comprehensive, adaptive security posture management system, utilizing advanced data insights to assist organizations in addressing cloud security risks proactively.

Scope of Our CSPM Tool

As organizations adopt multi-cloud and hybrid-cloud environments, managing security posture across these diverse platforms presents a significant challenge. The massive volumes of data handled by cloud services today reach the scale of yottabytes (10^24 bytes), with the emerging unit, brontobyte (10^27 bytes), anticipated as data volumes continue to grow. This explosion of big data adds to the complexity of managing security configurations and policies. Therefore, the scope of our CSPM tool includes integrating Big Data and AI capabilities to streamline and strengthen security posture management [10].

Equipped with these capabilities, our tool aims to provide a centralized system for monitoring and managing security across multiple platforms. Leveraging AI, the CSPM tool can autonomously identify misconfigurations, reduce human error, and enhance security through data-driven decision-making. As cloud environments evolve to include edge computing, the tool's design will allow for compatibility with edge AI technologies, further extending its scope and effectiveness.

The landscape of cybersecurity threats continues to evolve, with attackers gaining increasingly sophisticated capabilities. Advances in technology and the rise of cloud environments have enabled attackers to exploit cloud-specific vulnerabilities, such as weak access controls, misconfigured resources, and insecure APIs. One of the most impactful advances in their tactics is the ability to automate attacks, allowing them to launch large-scale assaults using scripts and tools. By incorporating machine learning and AI, attackers are making their strategies harder to detect and counter [11].

However, as the complexity of security measures advances, attackers face growing challenges. This is where the scope of our CSPM tool comes into play. By using AI and machine learning, our tool can detect and respond to threats in real time, making it increasingly difficult for attackers to exploit cloud vulnerabilities. This proactive approach strengthens cloud security posture and helps organizations stay ahead of potential threats in an ever-evolving digital landscape.

Attack Type	**Attack Method**
DDoS (Distributed Denial of Service) Attacks	Flooding-Based Attacks
	Zero-Day DDoS Attacks
Side Channel Attacks	Attacks exploiting communication channels
	Attacks exploiting power consumption
Malware Injection Attacks	Server-Side Injections
	Device Side Injections
Authentication and Authorization Attacks	Dictionary Attacks
	Exploiting Weaknesses in Authentication
	Exploiting Weaknesses in Authorization Protocols
	Over-Privilege Attacks

Cloud service providers like AWS have invested heavily in enhancing their security infrastructure. AWS environments come with built-in security features [12], and when properly configured with security tools, they can significantly strengthen defenses against attacks. Our CSPM tool builds on this foundation by integrating AWS technologies into its framework, allowing it to utilize existing AWS security measures while addressing new and evolving cyber threats. As organizations increasingly migrate to the cloud, attackers have turned their focus to this target-rich environment. With advanced threat and intelligence monitoring, our CSPM tool enables security teams to rapidly detect and respond to incidents, helping organizations stay ahead of potential threats. Table I outlines some common cloud-based attacks that our tool is designed to address.

With tightening privacy regulations, maintaining compliance has become a top concern for many organizations. Our CSPM tool helps organizations demonstrate compliance with government standards, such as the NIST CSF v1.1, by providing comprehensive visibility across cloud configurations. Misconfigurations, often due to simple mistakes, inadequate security controls, or a failure to keep up with cloud changes, are a leading cause of cloud breaches [13]. By identifying and correcting misconfigurations, our CSPM tool reduces the attack surface, preventing incidents like data breaches or unauthorized access that could compromise compliance with frameworks like NIST CSF v1.1.

The transformative power of Big Data and AI extends to cybersecurity. Big Data offers vast raw information for analysis, while AI learns from this data to enhance threat detection and remediation. AI-based learning helps reduce human error and accelerates response times. Algorithms within our CSPM tool analyze data to detect patterns that may signal potential risks, making continuous threat monitoring more efficient. As data volumes grow, Big Data analytics becomes essential for effective threat detection, enabling organizations to improve their security posture by spotting risks early through trend analysis.

For instance, in a recent AAAI conference on Artificial Intelligence, Kalvakurthi et al. presented “Hey, Dona!”—an AI-driven virtual assistant for student course registration [12]. This system processes large volumes of sensitive data, which introduces potential security risks. By utilizing AI and Big Data, our CSPM tool can support similar systems by providing proactive protection of sensitive data in academic settings, safeguarding user privacy and maintaining trust.

The complex nature of cloud environments, evolving threat landscapes, frequent types of attacks, and the high impact of misconfigurations define the scope of our CSPM tool. Through advanced monitoring, automated remediation of misconfigurations, and compliance support, our tool can be an indispensable asset in managing and securing an organization’s cloud posture in today’s AI- and data-driven era.

Features and Capabilities of the CSPM Tool

For any security tool to be effective, it must provide comprehensive features and capabilities to manage data thoroughly. Our proposed CSF-based CSPM tool incorporates advanced threat intelligence monitoring and misconfiguration alerting, empowering organizations to identify and remediate security risks while staying compliant with frameworks like NIST CSF v1.1.

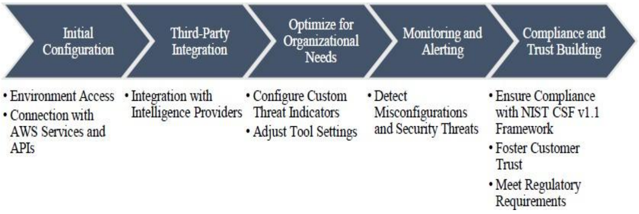
The CSPM tool is designed for continuous monitoring of an organization’s entire AWS infrastructure, including instances, storage, databases, and network configurations. By analyzing AWS logs and other intelligence data, the tool provides real-time detection of threats and vulnerabilities, ensuring that security teams are actively informed about security incidents and potential risks. This continuous monitoring strengthens the organization’s cloud security posture. Advanced analytics and monitoring techniques enable the tool to analyze data across AWS services, logs, and third-party threat intelligence sources.

The architecture of our CSPM tool, shown in Fig. 1, builds on research in OpenCPSM [13]. This architecture showcases several stages of CSPM tool design, including how cloud logs and data buckets are utilized. By leveraging AI, the tool can detect anomalies across assets and execute machine learning techniques—such as multiple classifiers—to recognize patterns in the data. Explainable AI methods, like decision trees, enhance the tool’s interpretability, while deep learning models improve accuracy in detecting threats. This layered approach allows our CSPM tool to identify potential security breaches or attacks early, sending alerts so organizations can respond quickly and mitigate risks.

Our CSPM tool also integrates seamlessly with AWS services, including Amazon GuardDuty, AWS Security Hub, and AWS Inspector, to further enhance its capabilities. These AWS technologies consolidate big data security insights, ensuring the tool has up-to-date information for a holistic view of the organization’s security posture.

Misconfigurations are a common and significant security risk in cloud environments, especially in AWS. As shown in Table II, various types of misconfigurations can occur in AWS, each presenting unique vulnerabilities. With AI-driven capabilities, our CSPM tool can automatically detect these misconfigurations and immediately notify the organization, enabling swift action to prevent potential security incidents.

Design for Implementation


Initial Configuration
Third-Party Integration
Optimize for Organizational Needs
Monitoring and Alerting
Compliance and Trust Building
• Environment Access
• Connection with AWS Services and APIs
• Integration with Intelligence Providers
• Configure Custom Threat Indicators
• Adjust Tool Settings
• Detect Misconfigurations and Security Threats
• Ensure Compliance with NIST CSF v1.1 Framework
• Foster Customer Trust
• Meet Regulatory Requirements

In this section, we outline the key methods for configuring and customizing our CSPM tool to meet the specific needs of an organization. A crucial aspect of our tool is its ability to integrate with third-party threat intelligence providers, enabling it to stay up-to-date with the latest security threats. The overall implementation framework is illustrated in Fig. 2.

By following the configuration steps outlined here, organizations can fully leverage the capabilities of the CSPM tool, securing their AWS assets and proactively addressing security risks.

To ensure the CSPM tool has the necessary access to monitor and analyze AWS assets, it must be set up with the correct Identity and Access Management (IAM) role and permissions. The integration role for the tool should include read-only access to AWS services and resources, enabling it to retrieve configuration data and security findings without making any changes to the infrastructure. Adhering to the principle of least privilege, the CSPM tool is designed to minimize the risk of security incidents while providing essential monitoring capabilities [15]. The tool can be configured to connect with various AWS APIs and services, including Amazon EC2, Amazon S3, AWS Lambda, and AWS Security Hub. These connections allow the tool to access the necessary information to perform accurate scans and gain visibility into the security posture of the organization's cloud environment.

To maximize the CSPM tool's performance, it is designed to integrate with third-party threat intelligence providers. This integration enables the tool to stay current with the latest security threats, offering a more comprehensive view of the threat landscape. By incorporating external threat intelligence, the CSPM tool enhances its detection capabilities and provides deeper insights into emerging security risks.

Given that each organization has unique security requirements, our CSPM tool is designed with flexibility in mind. It allows security teams to configure custom threat indicators, enabling them to focus on specific risks relevant to their industry, region, or infrastructure. This customization ensures that the tool can be tailored to meet the specific security needs of any organization.

Moreover, to accommodate varying organizational priorities, the CSPM tool offers the ability to adjust settings such as alert thresholds, monitoring frequency, and data retention policies. This flexibility allows security teams to strike a balance between robust security measures and operational efficiency, aligning the tool with the organization's cloud security posture and risk management strategies. In addition to detecting misconfigurations and threats, the CSPM tool provides actionable remediation recommendations, which are sourced from AWS's knowledge center for each triggered alert.

The successful implementation and optimization of the CSPM tool are essential for strengthening an organization's cloud security posture and ensuring compliance with the NIST CSF v1.1 framework. By configuring access management, customizing threat intelligence feeds, and aligning the tool with organizational security policies, security teams can fully harness the tool's capabilities to mitigate security threats and incidents. Effective implementation of the CSPM tool will not only help organizations protect their cloud environments but also build customer trust and ensure compliance with regulatory requirements.

Monitoring and Reporting

Our Cloud Security Posture Management (CPSM) tool is designed with a user-friendly dashboard that provides key insights, alerts, and security findings related to AWS assets within an organization. This dashboard offers real-time visibility into the cloud security posture, helping security teams assess their infrastructure, identify potential risks, and prioritize remediation efforts. The tool enables security teams to generate customizable reports that align with their specific reporting needs, aiding organizations in complying with the NIST CSF v1.1 framework. Additionally, these reports provide stakeholders with clear information on the organization's security posture.

To enhance the utility of our CSPM tool for reporting, seamless integration with the organization's existing Security Information and Event Management (SIEM) systems is essential. Fig. 3 provides an excerpt from an initial demo of the CSPM tool, highlighting its monitoring capabilities. As shown, the severity of non-compliance is categorized (low, high, critical), and the specific rule and resource type (e.g., EC2 volume) are identified. A short description of the issue is provided, with an option to expand for more details. Furthermore, the tool offers remediation suggestions, leveraging big data analytics from AWS resources. The integration of AI enables the tool to autonomously assess the severity level of non-compliance and automatically generate relevant reports.

To ensure the effectiveness of our CSPM tool, organizations should regularly review and update their configurations and settings. This includes adjusting alert thresholds, updating custom threat indicators, and refining IAM roles and permissions to match evolving security needs and infrastructure changes. Organizations should conduct regular audits to evaluate their compliance with the NIST CSF v1.1 framework, as recommended in several studies [16] These audits will also be beneficial as organizations adopt emerging technologies, such as edge computing, AI, and robotics, to further enhance cloud security management.

4. CONCLUSION

Cloud Security Posture Management (CSPM) has become an essential discipline for organizations seeking to safeguard their cloud environments and ensure compliance with industry standards, such as the NIST CSF v1.1 framework. As more organizations adopt cloud services, the complexity and scale of managing cloud security risks continue to grow, making the need for advanced CSPM tools even more critical. By leveraging Big Data, AI, and machine learning, CSPM tools can significantly enhance an organization's ability to detect and respond to security threats, misconfigurations, and vulnerabilities in real-time, providing proactive protection for cloud-based assets.

The proposed CSPM tool in this study, built on the NIST CSF v1.1 framework, offers a comprehensive solution to continuously monitor and analyze cloud environments, particularly AWS services. By integrating third-party threat intelligence, automating threat detection, and offering customizable reporting capabilities, this tool can not only help organizations improve their security posture but also streamline compliance with regulatory requirements. Moreover, its ability to autonomously assess and mitigate risks reduces human error, making it a vital resource for organizations of all sizes.

In conclusion, the evolving landscape of cloud computing demands advanced, automated security solutions that can adapt to ever-changing threats. The integration of AI and Big Data into CSPM tools ensures a robust defense against security breaches, data loss, and unauthorized access, while also enabling better decision-making and faster incident response. As organizations continue to expand their cloud adoption, investing in effective CSPM tools will be crucial for maintaining a secure, compliant, and resilient cloud environment.

REFERENCES

[1] Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. *World Congress on Information and Communication Technologies*, 217–222.

[2] Chandra, S., Varde, A. S., & Wang, J. (2018). A Hive and SQL case study in cloud data analytics. *IEEE UEMCON*, 112–118.

[3] Dong, B., Varde, A., Li, D., Samanthula, B., Sun, W., & Zhao, L. (2019). Cyber intrusion detection by using deep neural networks with attack-sharing loss. *IEEE DataCom*. arXiv preprint arXiv:2103.09713.

[4] Enriquez, R. L. (2021). Cloud security posture management (CSPM) in Azure. *Theseus*. https://www.theseus.fi/handle/10024/504136

[5] Guffey, J., & Li, Y. (2023). Cloud service misconfigurations: Emerging threats, enterprise data breaches & solutions. *IEEE CCWC*, 806–812.

[6] Johnson, R. E. (2010). Cloud computing security challenges and methods to remotely augment a cloud's security posture. *International Conference on Information Society*, 179–181.

[7] Kalvakurthi, V., Varde, A., & Jenq, J. (2023). Hey Dona! Can you help me with student course registration? *AAAI 2023 Conference, Workshop on AI for Education*. https://doi.org/10.48550/arXiv.2303.13548

[8] Khasuntsev, N. A. (2022). Automatic detection of misconfigurations of AWS Identity and Access Management Policies. *University of Twente, NL*.

[9] Radakovic, D., Singh, A., Varde, A., & Lal, P. (2022). Enriching smart cities by optimizing electric vehicle ride-sharing through game theory. *IEEE ICTAI*, 755–759. https://doi.org/10.1109/ICTAI56018.2022.00116

[10] Sari, A. (2015). A review of anomaly detection systems in cloud networks and survey of cloud security measures in cloud storage applications. *Journal of Information Security, 6*(2), 15–28. https://doi.org/10.4236/jis.2015.62015

[11] Sanders, M., & Yue, C. (2019). Mining least privilege attribute-based access control policies. *ACM 35th Annual Computer Security Applications Conference (ACSAC)*, 404–416.

[12] Varghese, C., Pathak, D., & Varde, A. S. (2020). SeVa: A food donation app for smart living. *IEEE CCWC Conference*, 408–413.

[13] Varde, A., Robila, S., & Weinstein, M. (2011). Energy: Green data centers for sustainability. *White Paper by NIST-TIP: National Institute of Standards and Technology - Technology Innovations Program*. https://www.researchgate.net/publication/268208144

[14] Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of IEEE, 107*(8), 1608–1631. https://doi.org/10.1109/JPROC.2019.2918437

[15] Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for cloud computing environments. *IEEE International Conference on Computer and Information Technology*, 1328–1334.

[16] Zhao, Zion3R. (2021). OpenCSPM - Open Cloud Security Posture Management Engine. *KitPloit*. https://www.kitploit.com/2021/02/opencspm-open-cloud-security-posture.html