Enhancing Cloud Security Posture for Ubiquitous Data Access with a Cybersecurity Framework Based Management Tool

Gregory Coppola
Cybersecurity Program
Montclair State University
Montclair, New Jersey, United States
coppolag3@montclair.edu

Aparna S. Varde
School of Computing, and CESAC
Montclair State University, NJ, USA
ORCID ID: 0000-0002-3170-2510
vardea@montclair.edu

Jiacheng Shang
School of Computing
Montclair State University, NJ, USA
ORCID ID: 0000-0003-3695-0991
shangj@montclair.edu

Abstract— **Cloud security has become an important issue for many organizations that utilize cloud services, e.g. Amazon Web Services (AWS), especially as they have to manage the massive volumes of data (i.e. big data) and the application of artificial intelligence (AI) technologies. Ensuring that the security posture of the given environment protects sensitive data and maintains compliance can be challenging, particularly as ubiquitous data access is typically desirable. This paper discusses the design of a Cloud Security Posture Management (CSPM) tool, to monitor assets with emphasis on Amazon Web Services (AWS) for exemplification. The CPSM tool aims to monitor AWS assets based on the NIST Cybersecurity Framework v1.1 (NIST CSF). It focuses on continuous threat and intelligence monitoring along with misconfiguration alerting as needed. Leveraging AI capabilities, the CSPM tool can help identify risks and provide remediation recommendations. AWS services, such as VPC traffic logs, GuardDuty, and CloudTrail, can be used so that the tool can be modified to fit organizational security requirements. This paper discusses the CPSM tool design, monitoring, and reporting features, in order to enhance security and compliance for cloud computing. Proper planning and implementation via the power of AI and Big Data can enable organizations to utilize this CPSM tool to increase their cloud security posture along with reducing risks appearing in the environment. This work directly impacts cloud data management and ubiquitous data access for digital connectivity, and consequently makes broader impacts on smart mobility, a vital facet of smart cities.**

Keywords — AI tools, big data, cloud services, cybersecurity, data mining, smart mobility, ubiquitous computing

I. Introduction

In the digital world of today, technology has been growing like wildfire, making cloud security a top priority for many organizations across the globe. More businesses are moving their technology to the cloud, increasing security challenges and potential new vulnerabilities. Cloud Security Posture Management (CPSM) based on cybersecurity standards, e.g. NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) v1.1 [1], can be essential to maintaining secure and compliant environments. This dives into the importance of cloud security posture management. It emphasizes the need for more specific CSF-based cloud security posture management tools that leverage Big Data and AI, and are designed to protect assets - for instance with providers such as AWS (Amazon Web Services).

As organizations increase their cloud services (e.g. AWS) for primary operations, the need for CPSM grows further. Cloud security posture management helps identify, assess, and mitigate security risks in cloud environments. It is significant for data protection along with maintaining compliance with regulatory requirements. An organization that is well-managed with cloud security posture will considerably decrease its risk of data breaches, unauthorized access, and any other security incident. A CPSM tool can allow organizations to be aware of security threats. This can be highly useful to provide customer satisfaction, increase the clientele, and more fundamentally, to secure the data per se.

National Institute of Standards and Technology (NIST) much values academic research; its Technology Innovations Program (TIP) has white papers, e.g. [2] about sustainability. NIST created a Cybersecurity Framework (CSF) [1], a set of best practices to guide organizations with security posture. It helps reduce cybersecurity risks. It allows organizations to change the framework for their unique needs, risks, and regulatory requirements. The NIST CSF v1.1 framework has five main functions: Identify, Protect, Detect, Respond, and Recover. This provides good guidance while assessing and improving organizational security posture.

A CSF-based cloud security posture management tool, enhanced with big data and AI capabilities, can significantly help organizations using cloud services via continuous monitoring for threats, misconfiguration alerting, threat intelligence capabilities and more. Leveraging technologies for the management of big data, such a tool can effectively control and analyze massive volumes of security data, identifying patterns and trends that might show potential security risks. This can allow for a more proactive approach to cloud security for organizations. The integration of AI within the tool can accelerate the process of risk identification and remediation, adding autonomy in decision-making. This can also reduce the potential for human error and ensure a faster response to security incidents. Following the NIST CSF v1.1 guidance, the tool can enable organizations to identify and address any security risks, heading towards a more safe and secure cloud environment. Adapting such a tool can make organizations adhere to best practices and regulatory compliance. Leveraging Big Data and AI in conjunction with the CSPM tool can provide a powerful mechanism to enhance cloud security. It can navigate the complexity of cloud data with greater confidence and agility.

Hence, with this motivation, we propose to build a CSPM tool that aims to develop a new method to enhance the security posture of cloud-based assets, more specifically in the AWS environment. The tool, built around the NIST CSF v1.1 framework, can significantly contribute to cybersecurity research. The main contributions of our work are as follows.
1. Design a CSPM tool to conduct advanced threat detection, proactive monitoring, and misconfiguration alerting
2. Leverage the integration of AI & big data management in the CSPM, displaying how it impacts cloud security posture
3. Exemplify the design in AWS to evaluate applicability and practical use of the CSPM tool for ubiquitous data access

II. Related Work

Cloud Security Posture Management and related areas have been the subject of interest for many studies, given that there has been an increase in organizations utilizing cloud services, thus leading to potential security threats. One of the earliest research projects in 2010 by Johnson et al. [3] investigated weaknesses in cloud security as per commercial security tools. Their work resulted in proposing new methods and tools to augment cloud security strategies. This research contributed one of the earliest insights on the shortcomings of cloud security for commercial based security tools.

Dong et al. [4] proposed a system DeepIDEA to leverage deep learning methods and attain high accuracy in intrusion detection on imbalanced data. They propounded an attack-sharing loss function to reduce the decision boundary attack classes, hence removing biases on majority / benign classes, thus enhancing classification. This can be useful in the cloud.

Another piece of work was created by Enriquez et al. [5] whose research highlighted the security vulnerabilities in cloud computing due to misconfigurations and inadequate change control. This work promoted a CSPM as a solution to improve the overall cloud configuration, security posture, and monitoring of an organization. The study looked into security flaws in areas such as Azure Defender, Azure DDoS (Distributed Denial of Service) protection, and Access and Permissions. It suggested re-evaluating internal protocols to fix these issues without disrupting any workflows or cost management. It also advised best practices for managing the Azure cloud. This research had limitations due to a lack of data collection from a company interviewed.

Researchers An et al. [6] focused on security issues in cloud computing, regarding susceptibility to unique threats. This study looked at existing graphical security models, such as Attack Graphs and Attack Trees, limited in scope and lack automation. In order to address these concerns, it proposed "CloudSafe" as a system to integrate various tools and frameworks for automating cloud security assessments. The system was demonstrated through testing on AWS, where it could gather security data and generate comprehensive security reports. These reports were able to supply valuable information for users and cloud service providers about the security posture of cloud environments.

Research by Chandra et al. [7] focused on the need for a scalable infrastructure to manage and analyze big data. It discussed the crucial role of cloud computing and compared SQL and Hive, two popular data management technologies. The study analyzed both Hive and SQL for cloud data management and mining. It dived into multiple approaches for processing queries on the cloud. It had recommendations for cloud data analytics in multiple real-world scenarios.

Pawlish et al. presented a survey paper [8] on increasing usage of the DevOps paradigm and its relation with cloud-based data management and analytics. It mentioned creating more sustainable or "green" businesses. It used a Geographic Information System (GIS) as an illustrative example and explained that the findings can be applied to other situations. The paper highlighted a shift in IT to cloud and hybrid models for data analytics to reduce negative environmental impacts. It highlighted privacy and security challenges of the cloud. Earlier work by this author [9] focused on using cloud services for greening data centers, using data mining for addressing issues including security, privacy and accessibility.

Our work in this paper goes a step beyond such related work in terms of designing an actual CPSM tool. Earlier work differs from our research because we aim to use cloud data for security concerns and purposes and provide enhanced security posture. We aim to utilize big data information an integrate AI capabilities to help cloud security posture in organizations.

III. Scope of our CSPM Tool

As organizations move into multi-cloud and hybrid-cloud environments, managing a security posture across all environments is highly challenging. The volumes of data being managed by these cloud services are absurd. Current data volumes are of the highest order of Yottabytes, i.e., 10^{24} bytes. The upcoming data unit is the Brontobyte, which equals 10^{27} bytes and is expected to be next in line. This rapid increase in big data increases the complexity of managing security configurations and policies. Hence, the scope of our CSPM tool entails big data and AI capabilities. The tool equipped with these capabilities can offer a centralized system for monitoring and managing security across multiple platforms. It can incorporate autonomy in decision-making based on data analytics in order to be more effective in providing a secure platform. More specifically, a CSPM tool powered by AI can automate identifying misconfigurations across cloud services, reducing human error, and enhancing security. It can further be enhanced as cloud computing evolves into edge computing with edge AI technologies.

Attackers today have an extensive range of capabilities that are becoming increasingly sophisticated. Since there have been technological advances and an increase in cloud environments, attackers have been able to broaden their attack strategies. Attackers often leverage cloud-specific vulnerabilities such as weak access controls, misconfigured cloud resources, and insecure APIs. One of the most significant capabilities of modern attackers is the ability to automate attacks. They can launch large-scale attacks on many targets using automated scripts and tools. They exploit machine learning and AI to improve their attacks, making them harder to detect and prevent. However, attackers face limitations. One of the key limitations is the increasing complexity of security measures. This fits the scope of our CSPM tool. AI and machine learning can be used to detect and respond to threats in real time. This can make it much harder for attackers, thereby helping to increase security.

TABLE I: ATTACK TYPES AND METHODS

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

Additionally, cloud service providers such as AWS have invested heavily in their security infrastructure. AWS environments come with built-in security measures [10], and when these are implemented correctly with security tools, they can make attacks much harder. Our CPSM tool extends to this scope by harnessing AWS technologies within its framework. The complexity of cyber threats is changing daily. With many organizations migrating towards cloud environments, it has become one of the prime targets for attackers. Our CSPM tool can allow organizations to stay ahead of these threats through advanced threat & intelligence monitoring, allowing security teams to detect and respond to security incidents quickly. There are many common attacks that are seen for cloud computing as mentioned in Table I.

As privacy regulations become stricter, maintaining compliance is a concern for many organizations. Our CSPM tool can help demonstrate compliance with government frameworks, such as NIST CSF v1.1. It can provide comprehensive visibility. Misconfigurations are a common cause of security breaches in cloud environments. They can be caused by simple mistakes, lack of security controls, or not keeping up with the changes in cloud environments [11]. Our CSPM tool aims to identify and remediate these misconfigurations, which can reduce the attack surface. If left undetected, misconfigurations can lead to security incidents, e.g. data breaches or unauthorized access. Organizations would also no longer be compliant with regulatory standards like NIST CSF v1.1. Hence, our CSPM tool can play a critical role here, helping organizations to maintain compliance.

AI and big data propel changing industries which include cybersecurity. While big data provides raw data that will be analyzed, AI can learn from data that can enhance threat detection and remediation. This AI-based learning can thus help to reduce human error in threat detection and accelerate remediation. Algorithms used to analyze data can pinpoint patterns indicating potential risks. This is vital in our CSPM tool that aims to continuously conduct threat monitoring. As organizations increase their data volume, big data analytics has become essential for threat detection. An organization can improve its security posture by identifying security risks through trend analysis. For instance, in a recent workshop on AI for Education at the AAAI conference on Artificial Intelligence, Kalvakurthi et al. presented a system demo of “Hey, Dona!” an AI-driven personal agent for virtual voice assistance in student course registration [12]. “Hey, Dona!” processes large amounts of sensitive data, which might lead to security issues. Using AI and big data in a CSPM tool, we can work with such systems to offer more protection in academic environments. Our CSPM tool can monitor various potential threats and misconfigurations, in order to secure sensitive student data and maintain user trust. CSPM tools with these capabilities are necessary for proactive cloud security management in this era of AI and big data.

The complexity of cloud environments, evolving threat landscapes, common types of attacks, and the potential impact of misconfigurations all define the scope of our CSPM tool. By offering advanced monitoring features, identifying and remediating misconfigurations, and helping organizations to maintain compliance, this CSPM tool can play a massive role in managing organizational cloud security posture.

IV. Features and Capabilities of the CSPM Tool

Any security-related tool must provide an in-depth set of features and capabilities to effectively manage the data. Incorporating advanced threat and intelligence monitoring and misconfiguration alerting, our proposed CSF-based CSPM tool can help organizations identify and remediate potential security risks while maintaining compliance with cybersecurity frameworks such as NIST CSF v1.1.

This CSPM tool aims to continuously monitor the entire AWS infrastructure of an organization. This continuous monitoring applies to instances, storage, databases, and network configurations by analyzing AWS logs and other intelligence information. The monitoring aims to include real-time detection of threats and vulnerabilities, allowing organizations to be actively aware of security incidents and risks. This can allow the organization to maintain a healthy cloud security posture. The CSPM tool aims to use advanced analytics and monitoring techniques to analyze data from AWS sources. As explained, it can review all AWS services, logs, and third-party threat intelligence information.

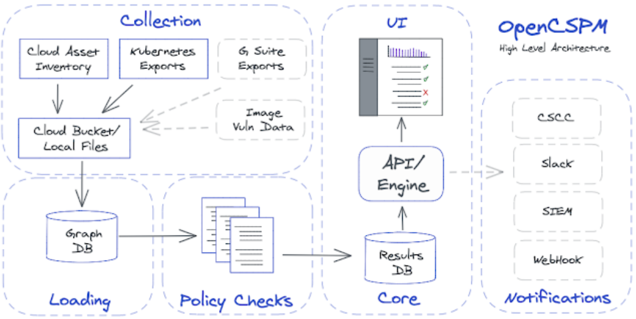


Fig. 1. Architecture of our CPSM tool

We present the architecture of our proposed CPSM tool in Fig. 1 thriving upon pertinent literature in *OpenCPSM* [13]. We can observe multiple stages of our CSPM tool design here. *OpenCSPM* has created this architecture that explains working with cloud logs and buckets. Using these buckets and logs containing big data can allow the tool to use AI technology to identify any abnormal behaviors from an asset. It can execute machine learning techniques such as multiple classifiers to identify patterns from existing data. Explainable AI techniques such as decision trees can help in additional comprehensibility while deep learning methods can deploy various neural network models for accurate predictions of threats, attacks etc. Our CPSM tool can thus detect potential security threats and even help identify potential breaches or attacks in the early stages analogous to some literature [14]. Our tool can offer warnings / alerts, allowing organizations to act immediately and mitigate risks. AWS offers services to work in conjunction with the CSPM tool. These include Amazon GuardDuty, AWS Security Hub, and AWS Inspector, and can all enhance the performance of the tool. These AWS technologies can allow consolidation of big data security findings and can ensure that the CSPM tool has the latest information. They can also help the CSPM in providing a view of the security posture of the concerned organization.

Misconfigurations in cloud environments occur more often than we imagine. Misconfigurations can cause high security risks. In AWS cloud environments, there are many misconfigurations that can occur, as exemplified in Table II.

Using AI, our CSPM tool can automatically detect misconfigurations in AWS assets. By doing so, it can notify the organization immediately to take quick action before there are any potential security risks. This tool would map the detected misconfigurations to the best practices and controls of the NIST CSF v1.1 framework. This can allow for a clear understanding of the data affected from security domains, and the remediation of the concerned issues. Mapping this can therefore allow the given organization to understand their overall compliance with the NIST CSF v1.1 framework. Since there can be many alerts, the CSPM tool must introduce a priority system. This system aims to allow for the misconfiguration alerts based on the level of risk posed to the organization. The CSPM tool can analyze the potential risk to the organization. This can allow for security teams to focus on the most critical vulnerabilities. The CSPM tool also aims to provide recommendations for the misconfigurations that are found. It would reference the AWS knowledge center to provide a more solid background about configurations. These recommendations can help security teams address issues that allow the organizational cloud security posture management to remain compliant with the NIST CSF v1.1 framework.

TABLE II. MISCONIFURATION EXAMPLES

AWS Misconfigurations	Description
IAM	Can lead to unauthorized access to critical services, creating a significant security risk that may expose sensitive information or allow for malicious actions within an environment.
S3	May expose sensitive data to the public, enabling unauthorized users to access, modify, or delete critical files.
Access Key Misuse	Can enable malicious actors to gain control of user's AWS services, turning a powerful security feature into a potential attack vector.
Cognito	Can result in unauthorized user authentication and identity issues, potentially granting access to users who should not have specific permissions.
EBS Encryption	Can leave sensitive data inadequately protected, exposing organizations to possible data breaches and compliance violations.
Security Group	Can open network access, making the entire infrastructure susceptible to potential breaches and cyberattacks.

The features and capabilities discussed in this section show the value of an advanced CSF-based CSPM tool to secure AWS environments. Our proposed CSPM tool can thus empower organizations in order to actively identify and address security risks posed by cloud services.

V. Implementation Details

As regards the design for implementation, we explain the important methods of configuring and customizing our CSPM tool, which allow it to fit with the organizational needs. Our CPSM tool incorporates the aspect of third-party integration from threat intelligence providers. Fig. 2 here illustrates our overall implementation outline.

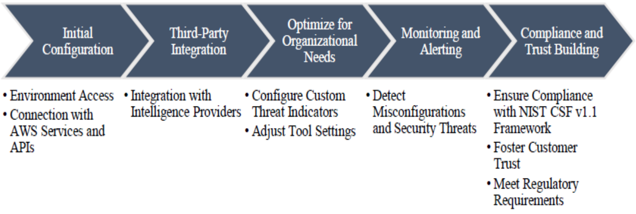

Initial Configuration
Third-Party Integration
Optimize for Organizational Needs
Monitoring and Alerting
Compliance and Trust Building
• Environment Access
• Connection with AWS Services and APIs
• Integration with Intelligence Providers
• Configure Custom Threat Indicators
• Adjust Tool Settings
• Detect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

Fig. 2. Implementation steps of our CPSM tool

By implementing the measures as mentioned in the steps here, organizations can have the advantage of the full potential of a CSPM tool, which will help secure their AWS assets and proactively address security risks.

To ensure that the CSPM tool has the necessary access to monitor and analyze AWS assets, it needs to be set up with the appropriate Identity and Access Management (IAM) role and permissions. The integration role of the CSPM tool includes permissions for read-only access to AWS services and resources. It can allow the tool to retrieve configuration data and security findings without changing the infrastructure. Needless to state, we aim to acquire the least privileges to prevent any possible security incidents in line with good practices [15]. Our CSPM tool can be configured to connect with AWS APIs and services such as Amazon EC2, Amazon S3, AWS Lambda, and AWS Security Hub. These connections can allow the tool to get any information needed to perform the proper scans. It can allow for visibility into the cloud security posture of the organizational environment.

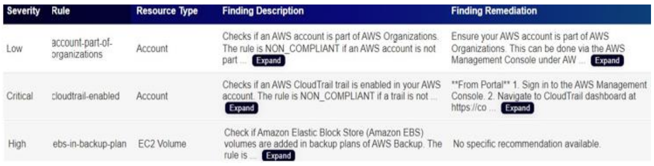
Since it is desirable to get the maximum performance for the CSPM tool, its implementation aims to enable it for integration with third-party threat intelligence providers. These integrations can allow the tool to be updated with data on the latest threats and related issues. It can foster a more comprehensive view of threat landscapes, making the tool enhance its detection features. Since each organization is different, the CSPM tool can offer the capability to configure custom threat indicators. This can facilitate security teams to focus on specific threats to their industry, region, or infrastructure. Security teams can thus tailor our CSPM tool to their needs for their unique security requirements.

Since we aim to make the tool as flexible as possible for organizations, security teams can adjust the settings, i.e. alert thresholds, monitoring frequency, and data retention policies to fit their unique security requirements. An organization can thus find a balance between security measures and operational efficiency to enable alignment between the organizational cloud posture security and risk management. Not only would the CSPM tool detect misconfigurations and security threats, but it would also give recommendations for remediation plans. These remediation plans can be from AWS' knowledge center for each triggered alert.

Implementing and optimizing the CSPM tool is vital in enhancing cloud security posture and complying with the NIST CSF v1.1 framework. Configuring access management, customizing threat intelligence feeds, and aligning the tool with organization security policies, can help security teams get maximum performance from the CSPM tool to reduce security incidents / threats. Successfully implementing and optimizing the CSPM tool can empower organizations to protect their own cloud environments, build customer trust, and meet regulatory requirements.

VI. Monitoring and Reporting

Our Cloud Security Posture Management (CPSM) tool has a design with a dashboard to display key information, alerts, and security findings related to organizational AWS assets. It can offer real-time visibility into the cloud security posture, assisting security teams to assess their infrastructure, identify potential risks, and prioritize remediation efforts. This CSPM tool can help security teams to generate customizable reports aligning with their specific reporting needs. These reports can aid organizations in complying with the NIST CSF v1.1 framework. Moreover, stakeholders can be informed about organizational security posture. In order to enhance the value of our CSPM tool for reporting, seamless integration must be offered as per organizational Security Information and Event Management (SIEM) system etc. Fig. 3 is a brief excerpt from an initial demo of our CPSM tool, highlighting its monitoring. As seen here, *severity* of the non-compliance is categorized (low, high, critical), the concerned *rule* and *resource type* are identified (e.g. EC2 volume), a short *description* is offered (with *expand* options for elaboration), and a *remediation* is offered if available (based on big data analytics from existing AWS vast resources). AI-based implementation provides the much-needed autonomy for making decisions while reporting, e.g. automatically assessing the severity level in monitoring.



Severity	Rule	Resource Type	Finding Description	Finding Remediation
Low	account-part-of-organizations	Account	Checks if an AWS account is part of AWS Organizations. The rule is NON_COMPLIANT if an AWS account is not part ... Expand	Ensure your AWS account is part of AWS Organizations. This can be done via the AWS Management Console under AW ... Expand
Critical	cloudtrail-enabled	Account	Checks if an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not ... Expand	**From Portal** 1. Sign in to the AWS Management Console. 2. Navigate to CloudTrail dashboard at https://co ... Expand
High	ebs-in-backup-plan	EC2 Volume	Check if Amazon Elastic Block Store (Amazon EBS) volumes are added in backup plans of AWS Backup. The rule is ... Expand	No specific recommendation available.

Fig. 3: Preliminary excerpt of demo: AWS config non-compliant resources

In order to ensure that our CSPM tool is effective, organizations should review / update their configurations and settings. In this process, they must adjust alert thresholds, update custom threat indicators, and refine IAM permissions & roles via security needs as well as infrastructure changes. Organizations should conduct regular audits to evaluate their compliance with NIST CSF v1.1 framework as outlined in some studies [16, 17, 18]. Some of these can be helpful for edge computing, next in line with cloud computing. They can also be helpful as we have more use of AI and robots online.

VII. Conclusions and Roadmap

The design of our CSPM tool presented in this paper paves the way for organizations to protect their environments and maintain their security posture actively. We list the following major takeaways from this paper.

- Big data analytics in the cloud can help organizations to take a more proactive and data-driven approach to security.
- AI-based methods help learn efficiently and accurately for detection & remediation of threats with more autonomy.
- Our CPSM design is a good benchmark to combat cyber-threats/vulnerabilities, needed for ubiquitous data access.
- It paves the way for next-generation cybersecurity tools as more robots & AI systems are online; hence emphasizing AI-based analytics for protection in ubiquitous AI tools.

Our roadmap includes polishing implementation, followed by conducting detailed experimental evaluation of our CPSM tool. This includes user surveys, comparative studies, and a general assessment for overall effectiveness prior to release. We aim to make our CPSM tool available on a site such as GitHub, so that open access can be provided for free to some interested users upon request. This paper presents our work in progress, establishing a clear motivation, surveying related work, presenting the scope of our CPSM tool, outlining its features & capabilities, stating implementation details, and discussing the monitoring & reporting aspects of the tool with an initial demo excerpt. While directly making an impact on ubiquitous computing, cybersecurity, and cloud services, our work on the CPSM tool design, makes a broader impact on AI-based digital connectivity. This is analogous to other works by our research team [12], [19-22]. It can be vital for smart mobility / smart living in smart cities & smart nations.

Acknowledgments

Aparna Varde has NSF grant 2018575 “MRI: Acquisition of a High-Performance GPU Cluster for Research and Education”. She is an Associate Director of CESAC (Clean Energy & Sustainability Analytics Center), Montclair. Jiacheng Shang has NSF grant 2153397 “CRII: SaTC: Towards Secure and Privacy-preserving Input on Augmented Reality Systems”.

References

[1] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[2] A. Varde, S. Robila, M. Weinstein, *Energy: Green Data Centers for Sustainability,* White Paper by NIST-TIP: National Institute of Standards and Technology - Technology Innovations Program, 2011, https://www.researchgate.net/publication/268208144

[3] R. E. Johnson, “Cloud computing security challenges and methods to remotely augment a cloud's security posture”, *International Conference on Information Society*, London, UK, 2010, pp. 179-181.

[4] B. Dong, A. Varde, D. Li, B. Samanthula, W. Sun, W., L. Zhao, “Cyber Intrusion Detection by Using Deep Neural Networks with Attack-sharing Loss”. *IEEE DataCom*, 2019, arXiv preprint arXiv:2103.09713.

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

[6] S. An, T. Eom, J. Park, J. Hong, A. Nhlabatsi, N. Fetais, K. Khan, D Kim, “Cloudsafe: A tool for an automated security analysis for cloud computing”, *IEEE TrustCom/BigDataSE),* 2019, pp. 602-609.

[7] S. Chandra, A. S. Varde, J. Wang, “A Hive and SQL Case Study in Cloud Data Analytics”, IEEE UEMCON, pp. 112-0118.

[8] M. J. Pawlish, A. S. Varde. “The DevOps Paradigm with Cloud Data Analytics for Green Business Applications”. *ACM SIGKDD Explorations*, 2018, 20(1): 51–59. doi.org/10.1145/3229329.3229334

[9] M. J. Pawlish, A. S. Varde, S. A. Robila, “The greening of data centers with cloud technology”, *Intl. J. of Cloud Applications and Computing (IJCAC),* 2015, 5(4), 1-23, DOI: 10.4018/IJCAC.2015100101

[10] A. Behl, “Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation”, *World Congress on Information and Communication Technologies*, 2011, pp. 217-222.

[11] N. A. Khasuntsev, “Automatic detection of misconfigurations of AWS Identity and Access Management Policies”, 2022, Univ. of Twente, NL.

[12] V. Kalvakurthi, A. Varde, J. Jenq, “Hey Dona! Can you help me with student course registration?”, AAAI 2023 Conf., Workshop on AI for Education, https://doi.org/10.48550/arXiv.2303.13548

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

[14] A. Sari, “A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications”. *J. of Info. Security*, 2015. DOI: 10.4236/jis.2015.62015

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

[16] X. Zhang, N. Wuwong, H. Li, X. Zhang, “Information Security Risk Management Framework for the Cloud Computing Environments”, *IEEE Intl. Conf. on Comp. and Info Technology*, 2010, pp. 1328-1334.

[17] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, W. Lv, *“*Edge Computing Security: tate of the Art and Challenges*”, Proc. of IEEE*, 107(8):1608-1631, Aug. 2019, doi: 10.1109/JPROC.2019.2918437

[18] J. Guffey, Y. Li, “Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches & Solutions”, *IEEE CCWC 2023*, 806-812.

[19] D. Radakovic, A. Singh, A. Varde, P. Lal, “Enriching Smart Cities by Optimizing Electric Vehicle Ride-Sharing through Game Theory” *IEEE ICTAI* pp. 755-759, DOI: 10.1109/ICTAI56018.2022.00116

[20] C. Varghese, D. Pathak, A. S. Varde, “SeVa: a food donation app for smart living”, *IEEE CCWC conf.,* pp. 408-413.

[21] K. Hammond, A. Varde, “Cloud Based Predictive Analytics”, *IEEE ICDM workshops*, 2013, pp. 607-612, 10.1109/ICDMW.2013.95

[22] J. Tancer, A. Varde, “The Deployment of MML for Data Analytics over the Cloud” *IEEE ICDM workshops,* 2011, pp. 188-195.