Journal for Technology and Science
Homepage : https://journal.antispublisher.com/index.php/IPTEKS/index
Email : admin@antispublisher.com

e-ISSN : 3047-4337
JOTECH, Vol. 1, No. 1, April 2024
Page 105-116

Analyze Risks in AWS/Azure Environments Using AI-Driven Monitoring and Anomaly Detection

Samira Alam Chowdhury[1], Mahbub Hasan[2], Fahmida Akter[3], Rabia Akter Sukhi[4], Abdul Rahman Mohammad[5]
[1]University of Dhaka, Bangladesh
[2]University of Information Technology and Sciences (UITS), Dhaka, Bangladesh
[3]Daffodil International University, Dhaka, Bangladesh
[4]American International University Bangladesh (AIUB), Dhaka, Bangladesh
[5]Jawaharlal Nehru Technological University Hyderabad (JNTUH), India

DOI : https://doi.org/10.61796/ipteks.v1i1.551

Sections Info
Article history:
Submitted: February 20, 2024
Final Revised: March 16, 2024
Accepted: March 10, 2024
Published: April 03, 2024
Keywords:
Cloud Computing
Amazon Web Services
Microsoft Azure
Cybersecurity threats
Environment
Dataset
Workloads

ABSTRACT
Objective: *In this research we explore the use of AI-driven monitoring and anomaly detection for analyzing risks in AWS and Azure environments, with an exploratory study on the Cloud Data Center Workload Dataset. The research will explore the following objectives: understanding the behavior of cloud workloads, detecting abnormal workload behavior, investigating the correlation between cloud monitoring parameters, and evaluating the risks of the operational environment of cloud infrastructure.* ***Method:*** *The methodology is based on an exploratory research approach with data preprocessing, exploratory data analysis, statistical analysis, and implementation of the monitoring framework using AI and R Studio. To interpret the behavior of the cloud, multiple visualizations were developed: workload distribution, resource utilization analysis, anomaly monitoring dashboard, correlation network, and operational risk dashboard.* ***Results:*** *The results indicate that changes in CPU usage, network traffic, memory consumption, processor temperature, or virtual machine activity affect the performance of the cloud and uncover potential points of vulnerability for operation. Moreover, with AI-powered monitoring one can easily detect abnormal patterns of resource consumption and continuously assess operational risk by combining the monitoring parameters into a composite risk index. In conclusion, the study demonstrates that AI support in monitoring bolsters cybersecurity management practices, enhances infrastructure visibility, aids in early detection of anomalies, and aids in proactive management of operational risks across AWS and Azure cloud platforms.* ***Novelty:*** *This study integrates AI-driven monitoring and anomaly detection with cloud workload analysis to evaluate operational risks across both AWS and Azure environments using the Cloud Data Center Workload Dataset.*

INTRODUCTION

A. Background of Study

AWS, which stands for Amazon Web Service, and Azure are globally recognized cloud service providers. AWS/Azure environment refers to the cloud infrastructure that replaces the physical server with on-demand virtual server. It permits the user to access the network, database system with the help of the internet on demand, making it available for 24 hours [1]. Like AWS, Microsoft provides the Azure cloud services to its users and both cloud service providers facilitate it for storing applications. In addition, these cloud services are also used with an intent of maintenance of server, database software and operating system [1]. AWS/Azure environment reduces the cost of the IT resources utilization by migrating the workloads to the virtual machines. It enhances the speed of operation with accuracy along with its cost saving factor. Constant Azure's

feature improvements have given more recognition in comparison to AWS service in the industry [1]. On the other hand, AWS has a wide range of services for its users that can be adopted as per the scale and requirement of business. Amazon S3, Amazon EC2 and Amazon RDS are some of the instances of AWS services used in the industry globally [2]. AWS services give privacy to its customer and allows its user to customize the machine learning modelling based-on the respective data [2].

B. Problem Statement

Immense volume of cloud assets in the form of data has been sensed with a security threat that many researchers determined in their work. Orca Cloud Security, who looks after multi-cloud platforms for its security, has sensed the scope of threat on the stored information [3]. Its report revealed the recent hike in the cyberattacks due to the inclination of the global business environment toward the adoption of cloud services. It also outlined the other research outcomes that shed light on the need for increasing investment on cybersecurity risk emerging from the integration of the AWS/Azure environment. It also estimated the cost of investment around $10.5 trillion by the successive years, which would be increasing 15% per year for securing the data stored in the aforementioned environment from cyberattack [3]. A renowned cloud security provider exposed the number of cyberattacks in 2023 in its report that reached around 18 billion [14]. Hence, the report rationalized the current scenario of cybersecurity challenges for the environment of AWS and Azure.

C. Aim of the Research Paper

The aim of the research is to conduct a critical assessment of the cloud environment of AWS and Azure with the help of AI-oriented tracking and anomaly detection methods to figure out the cyber risk.

D. Objectives of the Research

The accomplishment of this research fulfills the following objectives as follows:

- To conduct a thorough study of cloud workload and operational information to determine the cybersecurity risks in AWS and Azure cloud environments.
- To figure out the specific uncommon pattern that conveys anomalies in the utilizations of cloud resources with the AI-oriented.
- To explore the reasons responsible for building relationships among cloud monitoring factors to reveal the cybersecurity threats and operational risks.
- To obtain a deep insight into the beneficial outcomes of assessing AWS/Azure environment for applying effective cybersecurity initiatives.

E. Research Questions

The research questions are mentioned below:

Q1. How the cloud workloads and operational information plays a crucial role in exploring the cybersecurity risks in the environment of AWS/Azure?

Q2. What specific uncommon patterns or anomalies are identified by using the AI-based monitoring of cloud resource utilization?

Q3. What are the causes of the cloud parameters associated with the potential cybersecurity threats and operational risks in the cloud environment?

Q4. How AI-oriented monitoring and analysis of anomalies detection in AWS/Azure environment supports the cybersecurity management?

F. Significance of the Study

The research work gives a fundamental concept that industries can adopt for securing its data stored in a cloud infrastructure. It describes the importance of AI tools by showing its use in measuring the risk of the AWS/Azure environment. Subsequently, the probability of cyber threats decreases in the aforementioned environment, which further increases the security of business data. The accomplishment of the research objectives not only support the functionalities of organization but also improves the customer experience. Apart from business benefits, it gives insights to the professional and technical experts of the industry to learn the ways of identifying cyber risk. The study also contributes in the field of research by showing the efficient ways of applying exploratory techniques to extract the hidden information related to the context in the form of visualization.

The growing adoption of cloud computing platforms such as AWS and Azure provides high scalability, yet simultaneously expands the attack surface targeting organizations' critical assets [5], [6]. Distributed multi-cloud infrastructures introduce complex vulnerabilities related to unauthorized access, data leakage, and account compromise [6], [7]. To mitigate these risks, cloud penetration testing approaches and proactive monitoring-based security governance are crucial for identifying configuration weaknesses before they can be exploited [7], [8].

However, traditional rule-based monitoring methods often fail to detect modern cyberattacks hidden within massive volumes of cloud operational data [9], [10]. As a solution, integrating Artificial Intelligence (AI) and machine learning techniques offers adaptive, real-time monitoring powered by big data analytics [9], [10], [11]. This AI-driven approach has been proven to enhance threat detection accuracy, reduce false-positive rates, and accelerate incident response within cybersecurity governance frameworks [11], [12].

A key pillar of AI-based cloud security is anomaly detection [13]. The shift from traditional statistical methods to machine learning and generative AI models enables systems to precisely identify deviant behavioral patterns within time-series workload data [13], [14], [15]. Implementing real-time monitoring frameworks—such as CloudShield—expands operational visibility without disrupting ongoing business services [16], [17]. Furthermore, AI transforms cyber risk management through automated vulnerability assessments, adaptive threat intelligence, and predictive analytics-driven decision-making [18], [19], [20].

Although cloud security, AI-based monitoring, anomaly detection, and cyber risk management have been extensively studied individually [5], [6], [7], [8], [9], [10], [11], [12], [13]. [14], [15], [16], [17], [18], [19], [20], limited research comprehensively integrates these concepts. Specifically, few studies apply exploratory analysis to real-world cloud workload data for cybersecurity risk assessment while directly combining AI-powered monitoring and anomaly detection techniques.

METHODOLOGY

A. Research Design

This study employed a quantitative research design, using exploratory data analysis to study the issue of cybersecurity risks in AWS and Azure Cloud environments through the use of AI driven monitoring and anomaly detection. Secondary data was used for the research from the Cloud Data Center Workload Dataset published in 2023 on Zenodo. Because the quantitative approach allows systematical analysis of numerical cloud workload parameters to detect operational patterns and abnormal workload behaviors that can present cybersecurity risks, it was decided to be appropriate. Exploratory data analysis was used to visually and summarize the properties of cloud use metrics of infrastructure to enhance understanding of resource usage and anomaly patterns. This study is not predictive modelling or an experimental intervention, but rather looking for meaningful results from historical cloud operational data. The findings obtained on the basis of statistical summarizing and graphical visualization can serve as evidence of the behavior of cloud infrastructure, and can illustrate the real-life application of AI-based monitoring in supporting cloud-based cybersecurity risk assessment.

B. Research Workflow

The research process was structured in a logical flow of activities that guarantee producing reliable and consistent analysis. To find an appropriate research problem, a comprehensive literature review was conducted on recent publications in the areas of cloud security, AI-based monitoring and anomaly detection. Next, the appropriate cloud workload dataset from a trusted public repository was chosen for 2023 release. Data collected was brought into R Studio for preprocessing and any inconsistencies or missing data were checked and dealt with. The dataset was then prepared and subsequently the exploratory data analysis was performed with descriptive statistics and graphical visualization methods such as histograms, boxplots, line and scatter plots, and correlation heat map. The results of the visual findings were analyzed to determine the operational patterns, abnormal resource usage, and threats to cybersecurity. Finally, the findings were discussed with the aim of making a meaningful conclusion and recommendations based on the existing literature and the research objectives.

C. Data Description and Collection

The study employed the Cloud Data Center Workload Dataset published in Zenodo open research repository in 2023. The data set is over 1 million observations of cloud data center operational metrics over time. There are variables such as timestamp, CPU load, power consumption, memory usage, network receiving traffic, network transmitting traffic, processor temperatures, fan speeds, number of virtual machines running and CPU core usage [21]. These variables are some of the important indicators of cloud operations that are typically tracked in a cloud infrastructure and are helpful metrics for understanding the behavior of cloud-based workloads and resource utilization. There was no primary data collection needed as the data set was publicly available and created for research purposes. The chosen dataset was deemed suitable because of its ability to provide detailed operational data for clouds that would enable the exploration of unusual

cloud behavioral patterns related to the AI monitoring and cybersecurity risk assessment investigation.

D. Data Preprocessing

Exploratory analysis was done after pre-processing the data to enhance the data quality and reliability. The data was then first imported into R Studio and analyzed to ensure it was fitted into the data structure, of the correct type and adequately recorded. Descriptive statistical procedures were used to detect missing observations, duplicate observations and inconsistent values, which were addressed by suitable pre-processing techniques to maintain the consistency for analysis. The timestamp variable was converted into appropriate date and time format so that it can be analyzed in a temporal perspective to understand the behavior of cloud workload. Outliers and extreme observations were checked on numerical variables by using statistical summaries and visualization techniques. Variable names were standardized for ease of reading and efficiency of analysis. The preprocessing stage guaranteed the data reflects cloud operational behavior, giving a reliable base for further statistical analysis and visualization.

E. Exploratory Data Analysis

The main analysis method in this research was exploratory data analysis, which is used to investigate the behavior of workloads in the cloud to detect anomalies in the way they operate within the cloud that may give warning of a cyber security threat. Data analysis was carried out descriptive statistics and several graphical techniques were used in R Studio. A histogram was used to analyze cloud resource utilization distribution, and a boxplot was used to find unusual observations and potential outliers. The scatter plots and bubble charts were created to explore the relationships between CPU utilization, memory usage, network activity, and virtual machine activity as cloud monitoring parameters. Trends of workloads over time were examined using line graphs and the strength of relationships among infrastructure variables was evaluated using correlation heatmaps. The information gained from these visualizations aided in the identification of abnormal operational patterns and helped gain a better understanding of cloud infrastructure behavior in the context of AI-driven monitoring.

F. Statistical Analysis

The dataset related to the cloud workload was summarized by conducting statistical analysis to aid the interpretation of the operational behavior. Descriptive statistical parameters used were the mean, median, minimum, maximum, standard deviation and quartile distribution of the main numerical variables. Cloud resource utilization parameters were correlated to find the correlations among them and to find the variables that have similar behavior. Selected workload characteristics were summarized using frequency distributions and percentage analysis, when appropriate. These statistical procedures gave quantitative evidence about the use of infrastructure and complemented the findings that were obtained in exploratory data analysis, which were graphical. The findings of the research were more accurate and credible as a result of the combined use of descriptive statistics and correlation analysis.

G. AI-Driven Monitoring Framework

The monitoring framework used in this study was not predictive but conceptual, and aimed to be used for the interpretation of cloud operational data to aid with the assessment and management of cybersecurity risks. The framework included monitoring of infrastructure metrics such as CPU load, memory usage, network activity, power usage, processor temperature, and VM activity. Exploratory data analysis was used to identify patterns of data that deviate from normal operational behavior that could be indicative of misuse or new cybersecurity problems. The framework focuses on the following stages as intertwined components: continuous monitoring, behavior assessment, anomaly identification, and operational risk interpretation, that are essential for guiding informed decision making in the cloud environment. While not using advanced machine learning algorithms, the analytical process was an application of key AI monitoring principles, identifying patterns and operational anomalies that needed to be explored in greater depth.

H. Ethical Consideration

The research followed ethical guidelines in conducting the investigation. The data used in this research has been provided from a publicly available and trusted research database, thus there is no need for human participation and/or collecting of confidential organizational data. Throughout the research processes, no personal, financial or sensitive information was accessed. All secondary data sources and scholarly literature was properly acknowledged and cited following IEEE referencing guidelines. Analytical procedures conducted objectively, without manipulation or alteration of original data, ensuring integrity and transparency of research findings. Moreover, the study was carried out only for academic purposes and complied with the accepted standards of responsible research practice.

RESULTS AND DISCUSSION

Results

A. Cloud Workloads and Resource Utilization Analysis

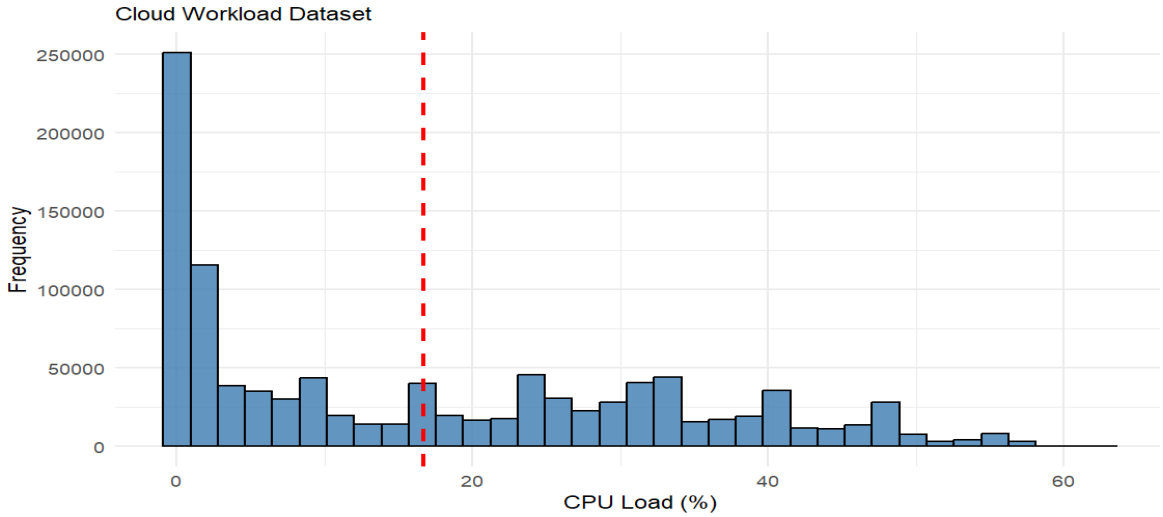

Figure 1. Distribution of CPU Load Across Cloud Infrastructure.
(Source: Created by learner)

The CPU load distribution suggests that the cloud resources are mostly lightly loaded with low and moderate loads, but high loads are relatively rare. Workload spikes are indicative of dynamic processing requirements, which might add complexity to the operations and introduce performance variability in the cloud infrastructure. The utilization patterns are useful in understanding how AWS and Azure environments behave and can identify environments that have higher cybersecurity-related risks.

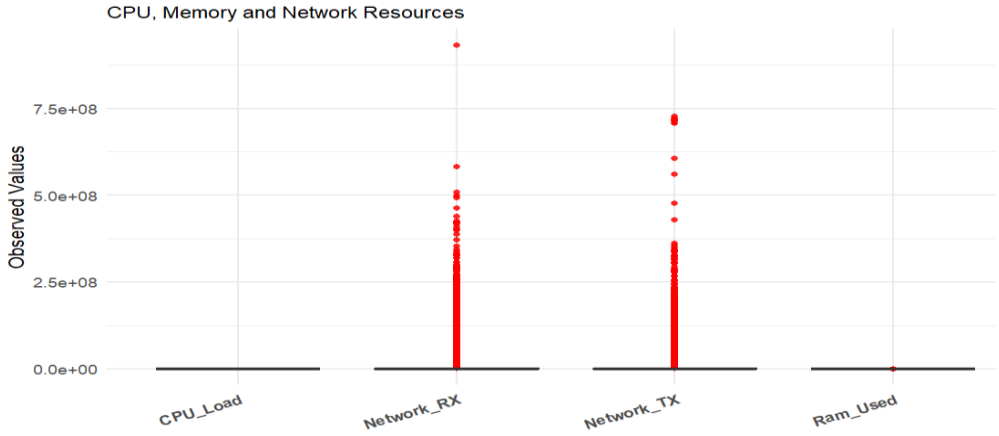

Figure 2. Resource Utilization Analysis of Cloud Infrastructure.
(Source: Created by learner)

The boxplot of the resources shows a wide range of variation in the CPU load, network traffic and memory usage, particularly for the network values where many extreme values are present. These variations are an example of varying workload intensity and resource usage during cloud operation. Based on the observed utilization behavior, there is a need to monitor critical infrastructure resources continuously to identify conditions that are unusual in operation, which could affect system stability and cyber security.

B. AI-Driven Monitoring for Detection of Operational Anomalies

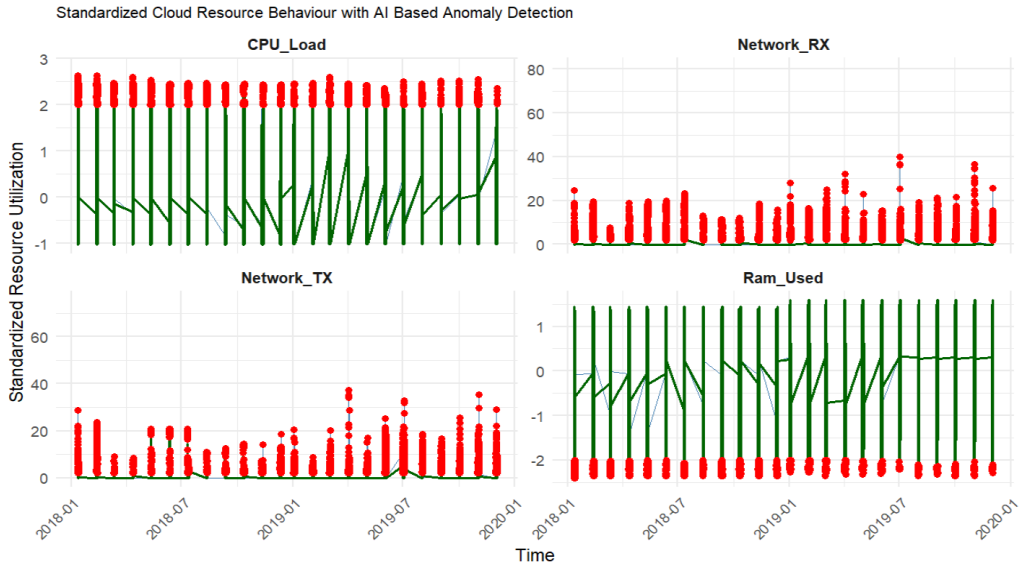

Figure 2. Detection of Operational Anomalies in AWS/Azure Environment.
(Source: Created by learner)

The AI powered monitoring dashboard provides a pictorial representation of the changes in CPU utilization, network traffic, and memory usage over time, and identifies some unusual observations throughout the monitoring period. When there are large, outlier resource behavior s on the standardized graph, the resulting spikes suggest abnormal operations from resources not typical of cloud workloads. The deviations offer early signs of potential anomalies in operation and emerging cybersecurity issues, highlighting the significance of continuous monitoring with AI assistance for the reliability and security of AWS and Azure cloud environments.

C. Relationship Analysis of Cloud Monitoring Parameters

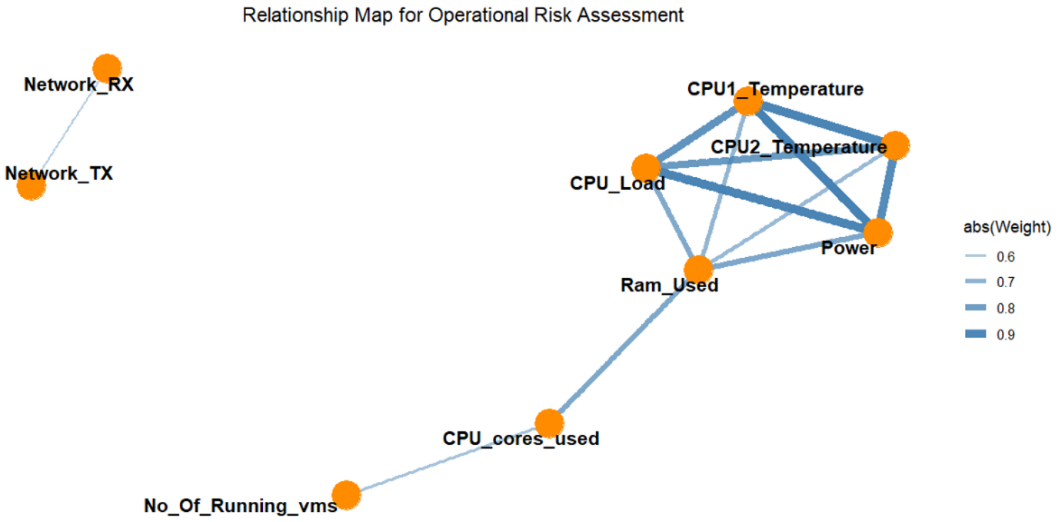

Figure 3. Correlational Network of Cloud Monitoring Parameters.
(Source: Created by learner)

The correlation network shows that the CPU load, processor heat, power consumption, memory consumption and CPU core usage are all closely correlated, suggesting that they are reacting to the change of workload in a similar manner. Conversely, the relationships of the network traffic with computational resources are relatively weaker. These monitoring parameters are interconnected and offer valuable information to evaluate cloud infrastructure performance and help uncover operational dependencies that can lead to cybersecurity risks and/or resource risks.

D. Operational Risk Assessment through AI Driven Monitoring

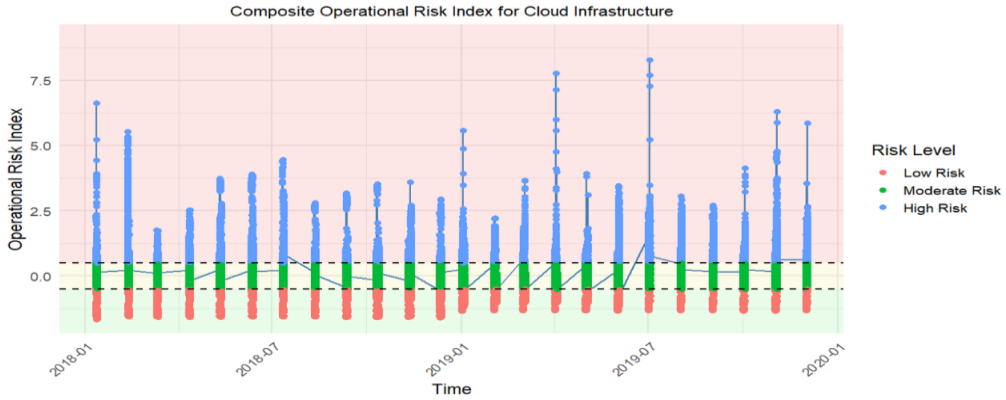

Figure 4: AI-Driven Operational Risk Dashboard
(Source: Created by learner)

The AI powered operational risk dashboard visualizes the overall health of the cloud infrastructure using a combination of monitoring metrics within a single risk index. The high-risk zone is observed in several observations, which is related to the use of the resources during a period of uncertainty in operations. The low, moderate and high levels illustrate how continuous monitoring can identify a changing infrastructure, helping to ensure prompt detection of potential cyber security threats and a more informed approach to risk management in both AWS and Azure deployments.

Discussion

The results show that the behavior of cloud workloads can be characterized by different degrees of resource usage, in terms of CPU processing, memory, network traffic and computational resources. The workload distribution indicated that the workload is distributed so that the utilization of CPUs is low and the spike in workloads was due to higher workloads. Similarly, the resource utilization analysis revealed significant differences in the activities in the network and usage of memory resources, indicating dynamic conditions in the operation of cloud infrastructures. The results suggest that cloud environments need to be monitored continuously as workload behavior can vary rapidly, which could lead to potential operational instability and cybersecurity risks.

Continuous monitoring's ability to detect abnormal operating behavior was also shown in the AI powered monitoring analysis using standardized cloud performance indicators. The monitoring dashboard showed significant spikes and dips in CPU usage, network bandwidth, and memory usage over the course of the test. A number of observations were outside of the normal behavior al range, which may point to unusual operating activity that may be an early sign of security related events or infrastructure abnormalities. The result shows that AI-centric monitoring methods increase visibility into the behavior of cloud resources, and offer an opportunity for organizations to identify abnormal patterns before they escalate to major incidents in the cybersecurity space.

The correlation network analysis was used to add insights into the relationships between the various cloud monitoring parameters. There were strong positive correlations between CPU utilization, processor temperatures, power consumption, memory utilization, and CPU core usage, indicating that these infrastructure metrics change in tandem with increases or decreases in workload. Network traffic parameters showed comparatively weaker relationships, which meant that there was relatively independent communication behavior in the monitored environment. These interdependent aspects demonstrate that the performance of the cloud infrastructure is dependent on a set of interacting resources and not just on a single system characteristic. Thus, analyzing the relationships between these cloud metrics gives a holistic picture of the operational environment and helps identify vulnerabilities in the infrastructure related to the evolution of the cloud workloads.

The operational risk dashboard incorporated a number of parameters into a composite operational risk index that would give an overall picture of the behavior of the

infrastructure. The visualization revealed several times in which the operational risk assessment went up due to several significant changes in the critical cloud performance indicators. The shift from low to moderate to high operational risk levels showed the value of using several measures of resources in a single monitoring system. Overall, the results show that AI based monitoring with exploratory analysis allows for a holistic analysis of workload behavior, anomaly detection, parameter relationships and operational risk. This analytical approach enhances cybersecurity management by enabling ongoing assessments of infrastructure and fortifying the organization's resilience against new threats in both AWS and Azure cloud systems.

Future Work

The study can be enhanced in the future by leveraging machine learning and deep learning algorithms to create predictive cybersecurity models for AWS and Azure cloud services. Random Forest, XGBoost, Long Short-Term Memory, Autoencoder, and Graph Neural Networks are some algorithms that could help detect anomalies more accurately by being trained on the complex behavioral patterns of the cloud monitoring data [22]. Improvements to the applicability of the work can be achieved using real time cloud telemetry data directly collected from the AWS CloudWatch, Azure Monitor, and other cloud security platforms for future studies. Adding other monitoring parameters such as authentication logs, user access patterns, app performance data, container security events, and network flow data would give a more complete picture of cloud infrastructure security. Cross hybrid cloud and multi cloud environments analysis could also enhance the knowledge of platform-specific cyber security issues. Explainable artificial intelligence is another possible technique that could be considered in future studies to enhance transparency in operational risk assessment and decision making. This type of advancements could help build more intelligent cloud security models that enable automatic detection of threats, ongoing monitoring, and adaptive cybersecurity actions for the cloud-based enterprise landscape.

CONCLUSION

Fundamental Finding: The exploratory analysis demonstrates that AI-driven monitoring effectively detects anomalies and identifies cybersecurity risks in AWS and Azure cloud environments. Variations in CPU utilization, memory usage, network traffic, processor temperature, and virtual machine activity provide valuable indicators of abnormal system behavior, while correlation analysis reveals relationships among key cloud monitoring parameters. **Implication:** The findings suggest that integrating AI-based anomaly detection with operational risk dashboards can enhance infrastructure visibility, support continuous risk assessment, and enable proactive cybersecurity management in cloud computing environments. **Limitation:** This study is based on an exploratory analysis of cloud workload data and focuses on AWS and Azure environments, which may limit the generalizability of the findings to other cloud platforms, workloads, or real-world operational settings. **Future Research:** Future research should validate the proposed AI-driven monitoring framework using real-time

cloud environments, investigate advanced machine learning and deep learning models for anomaly detection, and evaluate its effectiveness across diverse cloud platforms, workloads, and cybersecurity threat scenarios.

REFERENCES

[1] Microsoft, "Azure vs. AWS," *Microsoft Azure*, 2022. [Online]. Available: https://azure.microsoft.com/en-us/pricing/azure-vs-aws

[2] Amazon Web Services, "What's New in November 2023," *AWS Official Website*, Nov. 29, 2023. [Online]. Available: https://aws.amazon.com/about-aws/whats-new/2023/11/

[3] CNBC.com staff, "24. Orca Security," *CNBC Disruptor 50 2023*, May 9, 2023. [Online]. Available: https://www.cnbc.com/2023/05/09/orca-security-disruptor-50.html

[4] CSA Editorial, "Barracuda Warns of Exploitation of Web Application Vulnerabilities and Misconfigurations," *Cybersecurity Asia*, Feb. 22, 2024. [Online]. Available: https://cybersecurityasia.net/barracuda-warns-of-exploitation-of-web-application-vulnerabilities-and-misconfigurations/

[5] E. R. F. N. U. Antara, S. Goel, and E. P. K. G. Pandian, "Network security measures in cloud infrastructure A comprehensive study," *International Journal of Innovative Research in Technology*, vol. 9, no. 3, 2022.

[6] S. Galiveeti, L. A. Tawalbeh, M. Tawalbeh, and A. A. A. El Latif, "Cybersecurity analysis Investigating the data integrity and privacy in AWS and Azure cloud platforms," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*. Cham, Switzerland Springer International Publishing, 2021, pp. 329 to 360.

[7] S. Somanathan, "Securing the cloud Project management approaches to cloud security in multi cloud environments," *International Journal of Applied Engineering and Technology*, vol. 5, no. 2, 2023.

[8] K. Crawley, *Cloud Penetration Testing Learn How to Effectively Pentest AWS Azure and GCP Applications*. Birmingham, U.K. Packt Publishing, 2023.

[9] R. Vadisetty, A. Polamarasetti, R. Guntupalli, S. K. Rongali, V. Raghunath, V. K. Jyothi, and K. Kudithipudi, "AI Driven Cybersecurity Enhancing Cloud Security with Machine Learning and AI Agents," SSRN, Art. no. 5284922, 2022.

[10] S. J. Enokkaren, V. Bitkuri, R. Kendyala, J. Kurma, J. V. Mamidala, and A. Attipalli, "Enhancing Cloud Infrastructure Security Through AI Powered Big Data Anomaly Detection," *International Journal of Emerging Research in Engineering and Technology*, vol. 2, no. 2, pp. 43 to 54, 2021.

[11] D. A. Ademilua and E. Areghan, "AI Driven Cloud Security Frameworks Techniques Challenges and Lessons from Case Studies," *Communication in Physical Sciences*, vol. 8, no. 4, pp. 684 to 696, 2022.

[12] R. Tarafdar, "AI Powered Cybersecurity Threat Detection in Cloud Environments," *International Journal of Cybersecurity and Digital Forensics*, 2022.

[13] A. R. Al Ghuwairi, Y. Sharrab, D. Al Fraihat, M. AlElaimat, A. Alsarhan, and A. Algarni, "Intrusion detection in cloud computing based on time series anomalies utilizing machine learning," *Journal of Cloud Computing*, vol. 12, no. 1, Art. no. 127, 2023.

[14] T. Hagemann and K. Katsarou, "A Systematic Review on Anomaly Detection for Cloud Computing Environments," in *Proc. 2020 3rd Artificial Intelligence and Cloud Computing Conf.*, Dec. 2020, pp. 83 to 96.

[15] R. Vadisetty, A. Polamarasetti, S. K. Rongali, S. Prajapati, and J. B. Butani, "AI Driven Threat Detection Enhancing Cloud Security with Generative Models for Real Time Anomaly Detection and Risk Mitigation," SSRN, Art. no. 5218294, 2023.

[16] Z. He, G. Hu, and R. B. Lee, "CloudShield Real Time Anomaly Detection in the Cloud," in *Proc. Thirteenth ACM Conf. on Data and Application Security and Privacy*, Apr. 2023, pp. 91 to 102.

[17] S. J. Enokkaren, V. Bitkuri, R. Kendyala, J. Kurma, J. V. Mamidala, and A. Attipalli, "Enhancing Cloud Infrastructure Security Through AI Powered Big Data Anomaly Detection," *International Journal of Emerging Research in Engineering and Technology*, vol. 2, no. 2, pp. 43 to 54, 2021.

[18] S. A. Oladosu, A. B. Ige, C. C. Ike, P. A. Adepoju, O. O. Amoo, and A. I. Afolabi, "AI Driven Security for Next Generation Data Centers Conceptualizing Autonomous Threat Detection and Response in Cloud Connected Environments," *GSC Advanced Research and Reviews*, vol. 15, no. 2, pp. 162 to 172, 2023.

[19] S. S. Kumar, "AI Based Data Analytics for Financial Risk Governance and Integrity Assured Cybersecurity in Cloud Based Healthcare," *International Journal of Humanities and Information Technology*, vol. 5, no. 4, pp. 96 to 102, 2023.

[20] A. Reddy, "The Future of Cloud Security AI Powered Threat Intelligence and Response," *International Neurology Journal*, 2022.

[21] S. Ilager, A. N. Toosi, M. R. Jha, I. Brandic, and R. Buyya, "A data driven analysis of a cloud data center statistical characterization of workload, energy and temperature," in *Proc. 16th IEEE/ACM Int. Conf. Utility and Cloud Computing (UCC)*, Messina, Italy, Dec. 2023, doi: 10.5281/zenodo.10069402.https://zenodo.org/records/10069402

[22] R. Nasir, M. Afzal, R. Latif, and W. Iqbal, "Behavioral based insider threat detection using deep learning," *IEEE Access*, vol. 9, pp. 143266–143274, 2021.

Samira Alam Chowdhury
MBA in Marketing, University of Dhaka, Bangladesh

Mahbub Hasan
BSc in Information Technology, University of Information Technology and Sciences (UITS), Dhaka, Bangladesh

Fahmida Akter
Bachelor of Science in Computer Science Engineering, Daffodil International University, Dhaka, Bangladesh

Rabia Akter Sukhi
Master of Business Administration in Human Resource Management, American International University Bangladesh (AIUB), Dhaka, Bangladesh

Abdul Rahman Mohammad
Bachelor of Technology in Computer Science, Jawaharlal Nehru Technological University Hyderabad (JNTUH)