4th IEEE International Conference on AI in Cybersecurity (ICAIC), 5-7 February 2025, University of Houston, Texas, USA

Generative AI for Automated Security Operations in Cloud Computing

Author 1: Advait Patel
Affiliation: Broadcom
Email: advaitpa93@gmail.com

Author 2: Pravin Pandey
Affiliation: Tiffany & Co
Email: pravin.pandey@outlook.com

Author 3: Hariharan Ragothaman
Affiliation: Athenahealth
Email:hariharanragothaman@ieee.org

Author 4:Ramasankar Molleti
Affiliation:Options Clearing Corporation
Email: sankar276@gmail.com

Author 5:Diwakar Reddy Peddinti
Affiliation: Independent Researcher
Email:ms.diwakar.reddy@gmail.com

2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC) | 979-8-3315-1888-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICAIC63015.2025.10849302

Abstract—**New opportunities in cloud computing have brought many new risks that require effective protection of dynamic distributed environments. Introducing a new formative technology, generative AI, to cloud security has far-reaching benefits for automating threat detection, real-time incident addressing, and vulnerability management. This paper focuses on extending generative AI with cloud security tools like AWS GuardDuty and Google Cloud Security Command Center; the contemplation of accuracy enhancement and response efficiency highlights its aim. Concerning actual applications such as SOAR systems, the study demonstrates how media industry giants, such as Netflix and JPMorgan Chase, have used AI to minimize risk factors while increasing operational efficiency. The paper also discusses the significant increase in response time, enhanced detection accuracy, and the shift to proactive security strategies brought by generative AI. Drawing attention to AI systems' opportunities, the study examines the subsequent issues connected with AI applications, including over-dependence on AI tools, adversarial risk to models, and the complex nature of decision-making in the context of AI systems. The present study also highlights the importance of generative AI in strengthening the defense of the cloud environment, but, at the same time, it recognizes the significance of preventive efforts and planned action plans to manage these technologies efficiently.**

Keywords—cloud security, generative AI, incident response, soar systems

I. INTRODUCTION

Cloud computing has done much for organizations by providing a scalable and cheap way of storing and processing data. But this has opened a new front of security problems. Threats inherent in cloud environments include unauthorized access, data compromise, and very complex attacks aimed at specific settings [1]. Because cloud systems are distributed and can process staggering amounts of data, monitoring and securing such environments is becoming more and more challenging. Conventional security methods fail to detect threats and provide responses as fast as threats appear and evolve, which means threats can go unnoticed in the organization. The challenges have become more manageable with the help of a new development called generative AI. In particular, generative AI deploys machine learning algorithms to look for patterns, outliers, and new types of threats within the mountains of incoming data. Because of its capacity to build sample situations and produce authentic data, the security team can work ahead of time or anticipate a threat and swiftly respond to it [2]. Specifically, generative AI generates the following benefits for security professionals: 1) automating demanding routine tasks, such as log analysis, threat hunting, and vulnerability scanning, thereby lightening the workload by many folds; 2) increasing the throughput and accuracy of threat prediction and response. More specifically, this study concerns the implementation of generative AI in automated security management on virtualized computing platforms. Namely, it enhances understanding of how generative AI can improve threat intelligence, incident handling, and vulnerability management. The various anti-cloud-native security tools, such as AWS GuardDuty and Google Cloud Security Command Center, as well as real-world systems, such as Security Orchestration, Automation, and Response (SOAR), are also discussed in the study. The aim is to examine how generative AI could evolve cloud security operations, what problems it can solve, and the potential directions for further improvement of the cloud cybersecurity environment. Hence, this research seeks to fill existing gaps in the existing literature by providing much-needed insight into the growth of AI-based cloud security.

II. LITERATURE REVIEW

A. Current Advancement in AI for Cybesecurity

AI has greatly influenced cybersecurity since it has offered more tactical approaches to early identification of threats and response to them. Structured security measures are rules where most security policies are predefined, with little flexibility to address emerging threats in cyberspace. On the other hand, AI systems employ machine learning (ML) techniques that can parse significant volumes of big data and continually learn about new threats [3]. Approaches like supervised, unsupervised, and reinforcement learning techniques have boosted the ability to detect threats. AI uses in cybersecurity are intrusion detection systems (IDS), user behavior analytics (UBA), and endpoint protection. For instance, sophisticated statistical models can assess the variability of traffic that shows the signs of attack [4]. Natural language processing has been applied for security log analysis, and thanks to it, the speed of vulnerability detection has increased.

B. Integration of AI with Cloud Security Tools

Security risks in cloud computing solutions differ from those of more traditional solutions because of their distributed architecture, multi-tenant/multi-dimensional framework, and ability to scale resources. AI has been found very useful, especially when interfaced with cloud-native security tools to mitigate the challenges. AWS GuardDuty, Microsoft Defender for Cloud, and Google Cloud Security Command Center use

979-8-3315-1888-2/25/$31.00 ©2025 IEEE

artificial intelligence in real-time threat detection to protect organizations.

AWS GuardDuty: This service employs ML to identify network traffic, access logs, and feeds from other sources for the AWS environment. That is how it defines various unwanted actions, including attempts to gain unauthorized access or to transfer data outside the protected network or the presence of viruses and other malware [5].

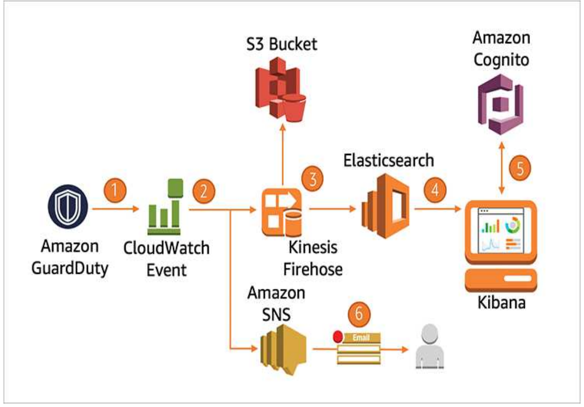

Figure 1. Amazon GuardDuty Architecture [5]

Figure 1 above describes how Amazon GuardDuty operates. It integrates Amazon GuardDuty, CloudWatch Events, Kinesis Firehose, and SNS. This solution helps observe and neutralize security threats much faster. GuardDuty processes CloudTrail records, VPC flow logs, and DNS queries and shares the results with CloudWatch Events. Results are computed within 5 minutes and sent further by implementing custom event patterns [5]. Two CloudWatch Event Rule targets are defined: Kinesis Firehose and SNS. It provides the result directly to two locations: an Elasticsearch domain for dashboarding using Kibana and an S3 bucket for historical storage. S3 data can also extend a data lake and permit analysis using Amazon Athena. SNS sends the alert immediately with an email or SMS to the operations teams. With Kibana, one can investigate, and published results are viewable using the Elasticsearch query language. IP whitelisting is replaced with a more convenient method—Amazon Cognito User Pools—to secure overall authentication. Such a setup allows for real-time oversight, access to the findings, and efficient utilization of the GuardDuty results.

Google Cloud Security Command Center: This platform uses AI to manage and provide a unified view of the security environment in Google Cloud projects [6]. Using predictive analysis, it categorizes threats by severity and provides an action plan for addressing them (refer to Figures 2 and 3 below).

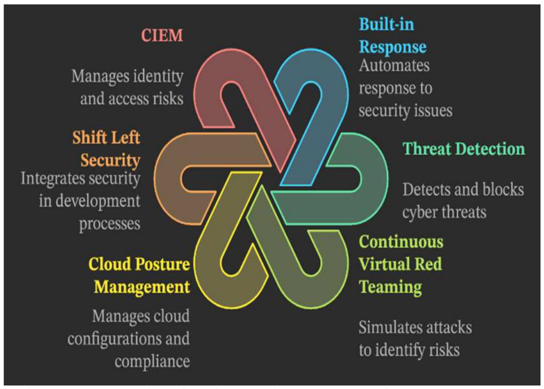
CIEM
Manages identity and access risks
Built-in Response
Automates response to security issues
Shift Left Security
Integrates security in development processes
Threat Detection
Detects and blocks cyber threats
Cloud Posture Management
Manages cloud configurations and compliance
Continuous Virtual Red Teaming
Simulates attacks to identify risks

Figure 2: Google Cloud Security Command Center Features

Google Cloud SCC uses modern threat identification mechanisms using machine learning techniques and best-in-class security intelligence. It automates detecting risks, including malware, forbidden access tries, and many suspicious things, before they become a big problem. The timely detection of threats on the platform is instrumental in conceiving and developing new strategies to combat emergent threats, improving the robustness of the whole protective structure [6].

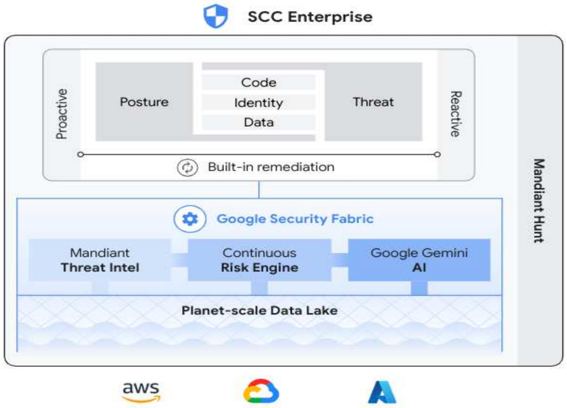

Figure 3: Google Cloud Security Command Center [7]

The figure above presents the structure of Google Security Command Center SCC Enterprise, a flexible multi-cloud risk management solution. It combines advanced SecOps that applies artificial intelligence with cloud protection and then offers preventive and responsive security for clouds situated in AWS, Google, and Microsoft Azure [7]. To achieve the best security in the cloud, SCC concentrates on five areas: posture, code, identity, data, and threat.

At its core, SCC leverages the Google Security Fabric, which combines three critical elements:

- Mandiant Threat Intelligence is a service that permits clients to stay informed on current threats and their adversaries.
- The Continuous Risk Engine identifies risks, configuration mistakes, and threats in continuous operation.
- Implementing an intelligent product, Google Gemini AI, to handle top-tier features, including threat detection, risk scoring, and response optimization.

This architecture employs a planet-scale data lake to analyze and integrate security operations for multi-cloud environments. By design, SCC has inherent remediation; thus, the auto-response capability addresses vulnerabilities and threats. Further, the company runs Mandiant Hunt with SCC, which is expert-led and always-on threat identification and analysis [7]. The proactive measures include main issues like misconfiguration and compliance violations, while the reactive capabilities recognize and coordinate with active dangers. Thus, CCT's data-driven approach to automation increases cloud security and overall performance by integrating threat intelligence.

Microsoft Defender for Cloud: This tool uses AI and analytics targeting workload visibility across multi-cloud and hybrid infrastructures. These integrations demonstrate how useful AI is for handling the massive amount of security data produced by cloud platforms. By lowering false positives, AI-powered solutions free up security personnel to concentrate on real threats. Additionally, AI's predictive powers improve the proactive detection of vulnerabilities, strengthening the security posture of the cloud as a whole.

However, there are gaps in the use of AI, incredibly generative AI, for challenging security tasks in cloud computing. Currently, generative AI, which comprises models that can create prosaic and creative solutions, is applied in cloud security operations less frequently than other AI methods.

1. Limited Exploration of Generative AI for Security Automation

Other generative AI models, such as GANs and transformer models, have had some success in different domains, but their applicability in automating security duties has been understudied. For example, generative AI could fake frequent assault patterns or produce fake data to ground other security algorithms. Such applications can significantly enhance the stability of cybersecurity systems, although research in this field is scarce.

2. Optimizing SOAR Workflows

First, Cyber Security Orchestration, Automation, and Response (SOAR) platforms are crucial tools in modern security operations, but the saturation of generative AI across these platforms is limited. SOAR workflows connect multiple tools and various data sources to automate threat-related activities. Whereas AI improves some features, generative AI can further develop other features, like providing response pattern generation based on specific threat types [8]. However, limited resources about the technologies that underpin these creative and adaptable generative AI workflows are available compared to the more common predictive or prescriptive analytics-type approaches.

3. Scalability and Real-Time Processing

Cloud domains produce big data, which demands elastic and near-real-time processing techniques. Recent literature on generative AI in security is primarily premised on conceptual models rather than design and implementation solutions that are scalable to cloud services.

III. Methodology

The potential of generative AI to improve automated security operations in cloud computing systems is being studied using a variety of methodologies and frameworks. Three main areas are examined: incorporating cloud-native security technologies, enhancing threat management's accuracy and response time, and analyzing practical applications such as AI-enabled Security Orchestration, Automation, and Response (SOAR) systems.

A. Integration with Cloud-Native Security Tools

Cloud-native security tools are required to target cloud environments' flexible and dispersed structures. Incorporating generative AI in these tools adds value to its advanced features of discovering outliers, real-time data analysis, and distinctive patterns.

a. Use Cases of Generative AI in Tools like AWS GuardDuty

AWS GuardDuty is an ML-powered security offering for AWS purposes that works with a continuous flow of logs to identify security events, including unauthorized attempts to access an AWS resource or indications of malware activity. The generative AI can also help GuardDuty by generating fake data that may mimic an upcoming actual attack so that the system can be trained to detect such attacks or more complex or new types of attacks [9]. For instance, a generative adversarial network (GAN) can generate attack traffic that emulates the true nature of the threat. Training GuardDuty on this enriched dataset makes it more capable of detecting these anomalies, which conventional models might oversee (refer to Figure 1). Similarly, information derived from context-heavy sources such as the users' activity log or similarity in patterns of API calls can be fed to transformer-based models to detect abnormal behaviors that point towards insider threat or privilege misuse.

b. *Real-Time Data Processing and Pattern Recognition*

One of the most significant advantages of generative AI is its ability to process and analyze large volumes of real-time data provided by cloud computing systems. That is why all these tools, including Google Cloud Security Command Center, can have use cases for AI models to identify intricate patterns in streaming data (refer to Figures 2 and 3). For example, a variational autoencoder (VAE) could take the input of live network traffic and then highlight behavior that deviated from norms for immediate action to be taken [10].

The analogy is invaluable in identifying multi-vector attacks where the strange signs may seem unrelated. Analytically generative AI models can associate these irregularities and expose the ongoing attack plan. This capability enhances detection accuracy and enables one to distinguish actual threats from less important ones, thus easing the job of the security teams.

a. Techniques to Optimize AI-Driven Threat Hunting and Incident Response

Generative AI can apply enhanced threat modeling to automate threat hunters' tasks of creating adaptive threat models to use during the hunt. For instance, finding past attack information and generating other possible current or future attacks is possible. These scenarios assist security teams in preempting and uncovering some vulnerability situations. Another technique is the application of transformer models, which will be used for contextual threats. Transformer models like BERT or GPT can decipher raw and unstructured data from logs, alerts, and user reports when solving an incident. By putting this information into context, they can provide the best remediation actions [11, 12].

TABLE I. DIFFERENCES AND SIMILARITIES BETWEEN BERT (BIDIRECTIONAL ENCODER REPRESENTATIONS FROM TRANSFORMERS) AND GPT (GENERATIVE PRE-TRAINED TRANSFORMER)

Aspect	BERT	GPT	Similarities
Primary Architecture	Encoder-only transformer.	Decoder-only transformer.	Both are based on the transformer architecture.
Training Objective	Masked language modeling (MLM) and next sentence prediction (NSP).	Causal language modeling (predicting the next word sequentially).	Both use unsupervised pre-training on large text corpora.
Directionality	Bidirectional: learns context from both left and right of a word	Unidirectional: learns context sequentially from left to right.	Both analyze and model contextual information from raw text data.
Application Focus	Focused on understanding and classification tasks (e.g., sentiment analysis, Q&A).	Focused on generative tasks (e.g., text completion, summarization).	Both can be fine-tuned for specialized tasks.
Output	Outputs contextual embeddings for tokens, not full sentences.	Outputs coherent sentences or paragraphs.	Both generate embeddings for input text, useful for NLP tasks.
Pre-training Dataset	Typically trained on Wikipedia and BooksCorpus.	Typically trained on diverse, large-scale datasets (e.g., web text).	Both require extensive datasets to capture diverse language representations.
Computational Cost	Lower due to its focus on token embeddings and bidirectional context.	Higher due to its autoregressive decoding for generation.	Both are resource-intensive but scalable with distributed systems.
Remediation Context	Excels at analyzing logs, alerts, and structured problem-solving.	Excels at generating human-like remediation instructions.	Both can process incident data and recommend remediation strategies based on their contextual understanding.

For incident response, generative AI helps automate the creation of a playbook. In the SOAR environment, AI means that further response workflows can be created based on the identified threat type. For instance, an attack such as ransomware may initiate the following process: they might initiate a flowchart that disconnects the compromised devices, perform a backup data recovery, and send an alert based on the attack.

b. *Metrics for Measuring Performance Improvements*

Robust performance measures are necessary to assess generative AI's efficacy in security operations. Important metrics consist of (the metrics are summarized in Figure 4):

Detection Accuracy: Based on the rate of the number of threats identified by the AI system out of all the actual threats [13].

False Positive Rate: To solve the problem of producing too many unnecessary alerts, generative AI could limit this problem by ensuring security is not disrupted through excessive notifications.

Response Time: Time needed to identify, assess, and address a threat. By automating crucial procedures, generative AI seeks to dramatically lower this statistic.

Resource Utilization: Savings when using AI to analyze CPU time, memory utilization, and bandwidth.

User Feedback: Weekly reports from security teams on the usefulness and applicability of content identified by AI algorithms after events.

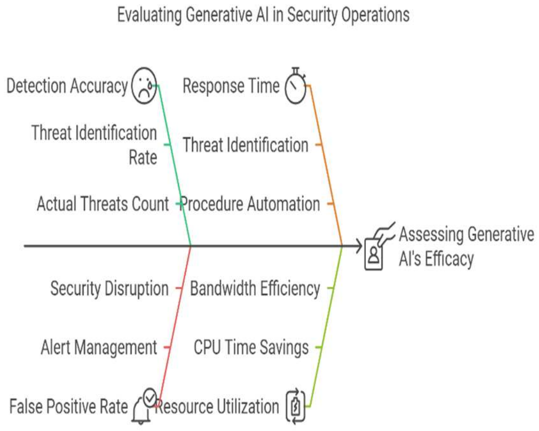

Figure 4: Evaluating Generative AI in Security

B. *Real-World Implementations*

SOAR technologies aggregate many security solutions and process the tasks of identification and response to threats. Generative AI advances these systems through the additional feature of adaptive and intelligent orchestration.

For instance, Splunk Phantom and Palo Alto Networks' Cortex XSOAR are SOAR platforms that involve machine learning for flow automation. Generative AI needs to be improved: build a live playbook based on the mentioned threat types. In a Distributed Denial of Service (DDoS) attack, generative AI could respond by assigning more resources to handle the handle while simultaneously banning the IPs involved [13]. Another implementation deals with the application of generative AI in layers of Security Information and Event Management (SIEM) systems that feed into SOAR systems. These AI models provide sound recommendations since they parse the log data, map events, and diagnose the causes of a mishap. This integration guarantees faster and more accurate rectification than rectifications in isolation.

Validating generative AI in security work calls for various rich data sources for training and demonstration. Common sources include:

- Cloud Activity Logs: Logs from Google Cloud Logging, Azure Monitor, or AWS CloudTrail include information about resource access patterns, API calls, and user activities [14].

- Threat Intelligence Feeds: Use threat intelligence feeds such as VirusTotal, Aberdeen Research, AlienVault, or IBM X-Force feeds as generic training data for AI about known attack patterns.
- Synthetic Datasets: The other advantage of generative AI is that it can generate artificial datasets to model and include the specific types of attacks that are hard to emulate.
- Incident Reports: AI systems can learn from real-world situations using historical data from previous instances.
- Live Traffic Analysis: It is possible to validate AI performance in real time by monitoring actual network traffic.

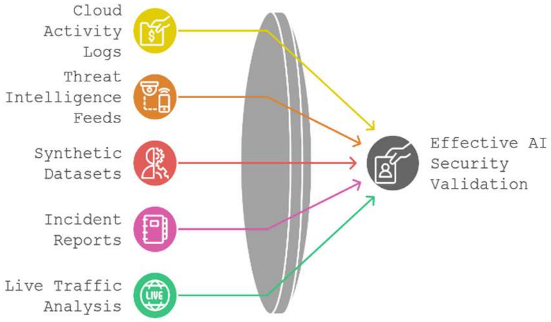

Figure 6: Data-Driven AI Security Insights

The situations expected in testing should be as varied as possible, including specific phishing attacks, internal threats, and mass campaigns. Information from such tests is employed to adjust the AI models and check their efficiency in identifying threats and reacting.

IV. Results and Discussion

A. *Integrating AI with Cloud-Native Security Tools*

Software solutions such as AWS GuardDuty and Google Cloud Security Command Center have been developed to address the security challenges of cloudy architectures. Combined with generative AI, these tools can strengthen organizational security by providing additional layers of data analysis, quicker identification of strange behavior, and predictive threat mapping ability [15].

Organizations using AWS GuardDuty include Netflix, which shows how the firm has incorporated the feature into its security management strategies. Netflix has adopted the GuardDuty AI service to watch millions of log entries for potential suspicious activities [16]. This proactive approach helps Netflix keep the environment safe for streaming services while providing a smooth customer experience.

Besides, Shopify uses Google Cloud Security Command Center to safeguard its Shopify e-commerce platform. Shopify, which incorporates the AI models into the Command Center, will effectively attain the capability to analyze the security telemetry data and correlate and prioritize the events. This capability quickly responds to threats to protect customer data and thus enhances trust. These systems increase capabilities manifold, particularly in pattern recognition, anomaly detection, and context-aware threat detection. For example, AI can process a considerable amount of log data in real time and, for instance, define nuance discrepancies, revealing a possible security threat [17]. Generative AI also generates fake datasets to create various attack vectors; the systems develop the ability to identify and counter all types of attacks.

This integration has several advantages for organizations and companies. First, it allows for threat identification at a higher level and earlier, significantly extending protection against breaches or reducing the impact of violations at different levels—financial and others. Besides, AI automation removes additional burdens from security teams and makes traffic more efficient for strategic decisions [18]. The flexibility of acknowledged cloud-native tools integrated with artificial intelligence guarantees organizations' security, including startups

B. *Enhancing Response Time and Accuracy in Cloud Security Operations*

Security data from multiple sources can then be fed to generative AI, which can process and analyze the data in real time, making it easier for organizations to be alert for the most dangerous threats. For instance, AI systems may contain and prioritize alerts by separating the dangerous ones from the simple noise. This saves time and effort that security teams spend analyzing the events and guarantees that severe threats will be identified and solved rapidly.

This also means that using generative AI increases the effectiveness of threat identification and countering [19]. Traditional systems can be problematic, with high false positive results that overwhelm security teams with alerts. Using generative AI to distinguish events from noise, for instance, relating different incidents to determine synchronized acts of terror, lowers the rate of false positives. Further, AI-integrated models can recommend appropriate response actions that match the incident's properties, thereby improving the impacts of the protective measures [20].

Individual companies using artificial intelligence report outstanding gains in managing security and safety. For example, Capital One is employing AI in banking, a financial firm that uses the technology in security to lower response time and increase precision. These risks have, therefore, been mitigated at Capital One through the adoption of AI that can monitor millions of daily instances and guarantee proximity to financial regulations. Similarly, global healthcare centers like the Mayo Clinic use artificial intelligence security measures to safeguard patients' vital information [21]. These systems immediately identify unauthorized entry attempts and legal requirements, such as HIPAA, in healthcare facilities.

C. *Security Orchestration, Automation, and Response (SOAR) Systems*

SOAR systems are critical in contemporary security operations because they can centrally coordinate and automate security processes. When integrated with generative AI, SOAR systems work synergistically, providing the tools to help organizations effectively manage and defeat threats. Generative AI improves SOAR systems by generating real-time playbooks that allow an organization to respond to an incident. The AI-created checklists are based on the details of each scenario and describe the proper course of action for security teams. Also, AI systems can rehearse scenarios, enabling organizations to assess the validity of the designed workflows for mitigating new threats. AI is also prominent in SIEM tools, threat intelligence feeds, and cloud-native security platforms, where SOAR systems can correlate multiple sources of information. The proposed approach offers security teams a unified picture of the security environment, which enhances the decision-making process. Banks like JPMorgan Chase already use AI-boosted SOAR systems to manage their security affairs. These systems automate the investigation process of alerts, lowering the period it takes to neutralize threats. JPMorgan Chase has improved operation efficiency and implemented more robust security measures using generative AI [22]. The retail sector also uses AI-supported SOAR systems. For instance, Walmart uses SOAR platforms to protect its facilities worldwide from cyber threats. The application of generative AI in Walmart's environment improves methods of identification and response to incidents and protection of supply chain and customer data [23]. However, there is always the possibility of overdependence on artificial intelligence systems. Organizations can regard AI as an infallible system that automatically addresses all security concerns, ignoring human supervision issues. Nevertheless, as with any system used in practice, even generative AI is never perfect; it is outstanding at automating routine operations and identifying outliers. False positives and false negatives are inherent in any artificial intelligence system and can cause missed threats or unnecessary disturbances.

V. Conclusion

Generative AI has become an innovative technology in cloud security because it can power a broad range of security use cases for organizations. Generative AI is connected to cloud-native tools such as AWS GuardDuty and the Google Cloud Security Command Center to enhance real-time data processing and increase the accuracy of threats while decreasing the time necessary for their detection. Its additional contribution to enhancing Security Orchestration, Automation, and Response (SOAR) systems indicates its ability to solve sophisticated security issues based on successful use cases in Netflix, Shopify, and JPMorgan Chase's firms. However, this generative AI has its drawbacks. Sometimes, it may bring information the user does not require or need. Overloading the AI systems presents overconfidence in manual monitoring, and adversarial attacks are always a potential threat to AI models. This means that decisions made by AI are not easily explained to others, which poses a significant challenge regarding the level of trust and compliance.

However, there is good potential for further development of generative AI in cloud security. Progressive innovation of its detection accuracy, adaptability, and multi-cloud will also enhance its strength in the future. Overcoming its drawbacks and integrating AI with human support, generative AI can be an essential building block in protecting ever-more intricate cloud environments from today's and upcoming cyber threats.

References

[1] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and Security of Cloud Computing: A Complete Guideline," *Symmetry*, vol. 15, no. 11, pp. 1–33, Nov. 2023, doi: https://doi.org/10.3390/sym15111981.

[2] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," *Information Fusion*, vol. 97, no. 101804, p. 101804, 2023, doi: https://doi.org/10.1016/j.inffus.2023.101804.

[3] N. Mohamed, "Current Trends in AI and ML for cybersecurity: a state-of-the-art Survey," *Cogent Engineering*, vol. 10, no. 2, Oct. 2023, doi: https://doi.org/10.1080/23311916.2023.2272358.

[4] S. Islam, M. A. Hayat, and M. F. Hossain, "ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: IMPACT, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS," Dec. 27, 2023. https://www.researchgate.net/publication/377019141_ARTIFICIAL_INTELLIGENCE_FOR_CYBERSECURITY_IMPACT_LIMITATIONS_AND_FUTURE_RESEARCH_DIRECTIONS

[5] M. Fortuna and R. Sakaria, "Visualizing Amazon GuardDuty findings," *Amazon Web Services*, Sep. 06, 2018. https://aws.amazon.com/blogs/security/visualizing-amazon-guardduty-findings/

[6] "Security Command Center," *Google Cloud*. https://cloud.google.com/security/products/security-command-center

[7] S. Potti, "Introducing Security Command Center Enterprise: The first multicloud risk management solution fusing AI-powered SecOps with cloud security," *Google.com*, 2024. https://cloud.google.com/blog/products/identity-security/introducing-security-command-center-enterprise (accessed Nov. 28, 2024).

[8] S. Shea, "What is SOAR (Security Orchestration, Automation and Response)? A definition from WhatIs.com," *SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/SOAR

[9] R. Nowrozy, "GPTs or Grim Position Threats? The Potential Impacts of Large Language Models on Non-Managerial Jobs and Certifications in Cybersecurity," *Informatics*, vol. 11, no. 3, p. 45, Jul. 2024, doi: https://doi.org/10.3390/informatics11030045.

[10] J. Liu *et al.*, "Multi-Channel Multi-Scale Convolution Attention Variational Autoencoder (MCA-VAE): An Interpretable Anomaly Detection Algorithm Based on Variational Autoencoder," *Sensors*, vol. 24, no. 16, pp. 5316–5316, Aug. 2024, doi: https://doi.org/10.3390/s24165316.

[11] V. Bertalan and D. Aloise, "Using Transformer Models and Textual Analysis for Log Parsing," *2023 IEEE 34th International Symposium on Software Reliability Engineering (ISSRE)*, pp. 367–378, Oct. 2023, doi: https://doi.org/10.1109/ISSRE59848.2023.00037.

[12] I. Jahan, T. Rahman, C. Peng, and J. X. Huang, "A comprehensive evaluation of large Language models on benchmark biomedical text processing tasks," *Computers in Biology and Medicine*, pp. 108189–108189, Feb. 2024, doi: https://doi.org/10.1016/j.compbiomed.2024.108189.

[13] Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain, and T. A. Al-Amiedy, "Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy," *Applied Sciences*, vol. 12, no. 23, p. 12441, Jan. 2022, doi: https://doi.org/10.3390/app122312441.

[14] C. Hall, "Key Log Sources in the 3 Main Cloud Providers," *Cadosecurity.com*, Aug. 09, 2024. https://www.cadosecurity.com/blog/key-log-sources-in-the-3-main-cloud-providers (accessed Nov. 28, 2024).

[15] S. Sai, U. Yashvardhan, V. Chamola, and B. Sikdar, "Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E and Other Models for Enhancing the Security Space," *IEEE access*, vol. 12, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3385107.

[16] S. M. Kerner, "How Netflix Secures AWS Cloud Credentials | eSecurity Planet," *eSecurityPlanet*, Aug. 10, 2018. https://www.esecurityplanet.com/cloud/how-netflix-secures-aws-cloud-credentials/

[17] T. Adewale, "Artificial Intelligence in Cloud Security: Use Cases and Benefits," Nov. 01, 2024. https://www.researchgate.net/publication/385509493_Artificial_Intelligence_in_Cloud_Security_Use_Cases_and_Benefits

[18] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data and Information Management*, vol. 8, no. 2, pp. 100063–100063, Dec. 2023, doi: https://doi.org/10.1016/j.dim.2023.100063.

[19] S. S. Thakur, “Generative AI Use Cases in Cloud Operations,” *RTInsights*, Oct. 25, 2024. https://www.rtinsights.com/the-role-of-generative-ai-in-enhancing-cloud-operations-real-use-cases/ (accessed Nov. 28, 2024).

[20] A. Takyar, “AI in Incident Response: Exploring Use cases, Solutions and Benefits,” *LeewayHertz - AI Development Company*, May 28, 2024. https://www.leewayhertz.com/ai-in-incident-response/

[21] “The Convergence of AI and Healthcare: Safeguarding Security and Compliance Amidst this Rapid Transformation,” *www.datadynamicsinc.com*, Aug. 25, 2023. https://www.datadynamicsinc.com/blog-the-convergence-of-ai-and-healthcare-safeguarding-security-and-compliance-amidst-this-rapid-transformation/

[22] J.P. Morgan, “AI Boosting Payments Efficiency & Cutting Fraud | J.P. Morgan,” *www.jpmorgan.com*, Nov. 20, 2023. https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction

[23] J. Geisler, “How Walmart protects against cyber threats,” *How Walmart protects against cyber threats*, Mar. 13, 2022. https://tech.walmart.com/content/walmart-global-tech/en_us/blog/post/how-walmart-protects-against-cyber-threats.html