Leveraging LLM for Zero-Day Exploit Detection in Cloud Networks

Kapil Patil*1, Bhavin Desai*2

*1Principal Technical Program Manager, Oracle, Seattle, Washington, USA

*2Product Manager, Google, Sunnyvale, California USA

ABSTRACT

Cloud network security faces challenges due to the increasing complexity and evolving nature of cyber threats, rendering traditional rule-based monitoring systems inadequate. This paper explores the potential of Large Language Models (LLMs) to revolutionize cloud security by addressing the limitations of rule-based approaches. We investigate how LLMs can enhance anomaly detection, generate actionable threat intelligence, and automate incident response processes. Through real-world examples and case studies, we demonstrate the practical applications of LLMs in fortifying cloud network security. However, we also acknowledge the challenges and ethical considerations associated with LLM deployment, such as hallucinations, bias, and privacy concerns. We propose strategies to mitigate these risks and emphasize the importance of human oversight in LLM-driven security systems. This comprehensive review underscores the significance of LLMs in shaping the future of cloud network security and provides valuable insights for researchers, practitioners, and decision-makers in this rapidly evolving field.

Keywords: Cloud Security, Large Language Models, Artificial Intelligence, Natural Language Processing, Cybersecurity, Machine Learning.

I. INTRODUCTION

The rapid adoption of cloud computing has revolutionized how organizations operate, offering scalability, flexibility, and cost-efficiency. However, this shift has also introduced a new set of security challenges. The dynamic and distributed nature of cloud environments, coupled with the constantly evolving threat landscape, demands sophisticated security measures that surpass the capabilities of traditional rule-based systems. These traditional systems, while valuable, often struggle to keep pace with the complexity and scale of cloud networks. They are prone to alert fatigue due to the sheer volume of events, can be difficult to scale effectively, and may fail to detect novel or sophisticated attacks that fall outside of predefined rules.

Large Language Models (LLMs), powered by advancements in artificial intelligence and natural language processing, present a promising avenue for addressing these challenges. Large Language Models (LLMs) have showcased an impressive ability to comprehend and create text that closely resembles human language. This makes them ideal for automating tasks like identifying anomalies, producing threat intelligence reports, and responding to incidents. LLMs possess the capacity to revolutionize cloud network security by harnessing their ability to analyze large datasets and uncover complex patterns.

This paper explores the potential of LLMs to revolutionize cloud security by addressing the limitations of rule-based approaches. We examine into the capabilities of LLMs, their advantages over traditional methods, and their application in real-world scenarios. Specifically, we investigate the following research questions:

1. How can LLMs be effectively employed to enhance anomaly detection in cloud networks, enabling the identification of previously unknown threats and reducing false positives?
2. In what ways can LLMs contribute to the generation of actionable threat intelligence, providing security teams with valuable insights to proactively mitigate risks?
3. How can LLMs be leveraged to automate incident response processes, accelerating threat mitigation and minimizing the impact of security breaches?

Additionally, we acknowledge the challenges and ethical considerations associated with LLM deployment in security contexts, including issues related to hallucinations, bias, and privacy. We propose strategies to mitigate these risks and emphasize the importance of human oversight in LLM-driven security systems. Through a comprehensive review of existing research and case studies, this paper aims to provide a deeper understanding of the role LLMs can play in shaping the future of cloud network security.

II. METHODOLOGY

This paper explores the potential of Large Language Models (LLMs) to revolutionize cloud security by addressing the limitations of traditional rule-based approaches. It investigates how LLMs can enhance anomaly detection, generate actionable threat intelligence, and automate incident response processes in cloud networks. The paper delves into the capabilities of LLMs, their advantages over traditional methods, and their application in real-world scenarios, drawing on research and case studies from companies like Microsoft, Intuit, and Walmart. It also examines the challenges and ethical considerations associated with LLM deployment, emphasizing the importance of responsible AI use in cybersecurity.

A. Limitations of traditional rule-based security monitoring systems

The strength of the traditional rule-based monitoring system lies in its simplicity and system administrators can set up specific parameters and receive notifications. However, rules-based security monitoring systems are host to several limitations including limited scalability, rule design complexities, rule disconnections and their overly deterministic nature. Other limitations include poor graphics, tendency towards increased false positives and poor documentation

1. **Difficulties in scaling**: Traditional rule-based monitoring struggles to scale effectively, hindering its applicability in complex cloud environments with escalating threats. This method prioritizes predefined rules, potentially overlooking other crucial security factors. Maintaining and updating rule libraries demands substantial time and human intervention, further limiting their effectiveness amidst expanding cloud security requirements.

2. **Complexities in rule design**: Traditional rule-based monitoring systems are complex to design and often struggle with unstructured data, requiring additional rules that further complicate the process. This impacts cloud data availability and monitoring effectiveness. Siloed rule design by business units, focused on specific objectives without dependencies, exacerbates these challenges

3. **Deterministic monitoring:** Traditional rule-based monitoring systems are limited by their deterministic nature. Their output, predetermined by initial conditions and security perimeter, lacks the dynamism needed to address evolving threats. This static approach stifles innovation, as it relies solely on predefined rules, leaving no room for the system to adapt or learn.

4. **Alert fatigue and false positives:** Traditional rule-based cloud security monitoring systems often overwhelm administrators with alerts, causing critical issues to be overlooked. These systems lack predictive capabilities, struggling to adapt to dynamic environments. Their complexity demands manual intervention for maintenance and configuration. Additionally, their rudimentary graphs fail to provide the insightful visualizations crucial for effective cloud security management.

B. Key Principles for Effective AI Implementation in Cybersecurity:

Successfully implementing artificial intelligence (AI) in security environments requires a strategic approach that goes beyond simply adopting the latest technology. To ensure AI initiatives deliver tangible value and mitigate risks, organizations must adhere to key principles throughout the development and deployment process. These principles are:

1. **Focus on the Problem**: Prioritize the specific security challenge to be addressed over general AI hype or the mere availability of data. Ensure the selected AI capabilities directly align with the unique complexities and accuracy requirements of the problem.
2. **Criticality Awareness**: Thoroughly assess the potential impact of AI errors. Begin with low-risk applications where mistakes are less consequential, and gradually expand AI implementation as expertise and confidence grow.
3. **Align with Business Goals**: Define and meticulously track AI performance metrics (accuracy, efficiency, cost reduction, etc.) that directly contribute to overarching business objectives, ensuring alignment and measurable value.
4. **Prioritize Deployability**: Early in the project, thoroughly investigate the feasibility of AI deployment, considering dependencies, integration requirements, and potential obstacles to prevent the development of unused or impractical solutions.

5. **Data-Centric Approach**: Only after clearly defining the problem, gather relevant, high-quality data that specifically addresses the identified security challenge. Maintain rigorous data quality and relevance throughout the AI lifecycle.
6. **Account for Data Drift**: Implement mechanisms to monitor and adapt to changes in data patterns over time. Retrain AI models as needed to maintain their accuracy and effectiveness in evolving security environments.
7. **Embrace Simplicity**: Opt for the simplest AI solution that fulfills the project's requirements. Avoid unnecessary complexity, which can hinder development, deployment, and maintenance efforts.
8. **Early Deployment**: Deploy a minimum viable AI product as early as possible. This approach allows for the identification and resolution of challenges within the real-world production environment before full-scale implementation.
9. **Flexible Response**: Maintain flexibility and adaptability throughout the AI project. Be prepared to adjust deployment strategies and response mechanisms based on the observed performance and outcomes of the AI system.
10. **Cost Management:** From the outset, diligently estimate and optimize processing and computational costs associated with the AI solution. Proactively identify and implement cost-saving measures to ensure long-term sustainability.
11. **Foster Cross-Competence**: Encourage and facilitate collaboration between data scientists and cybersecurity experts. Promote knowledge sharing and cross-training initiatives to bridge skill gaps and enhance collective expertise.
12. **Develop Reusable Tools**: Invest in the creation of reusable tools and standardized processes for common tasks in AI project development. This approach streamlines future initiatives, promotes efficiency, and ensures consistency across AI implementations.

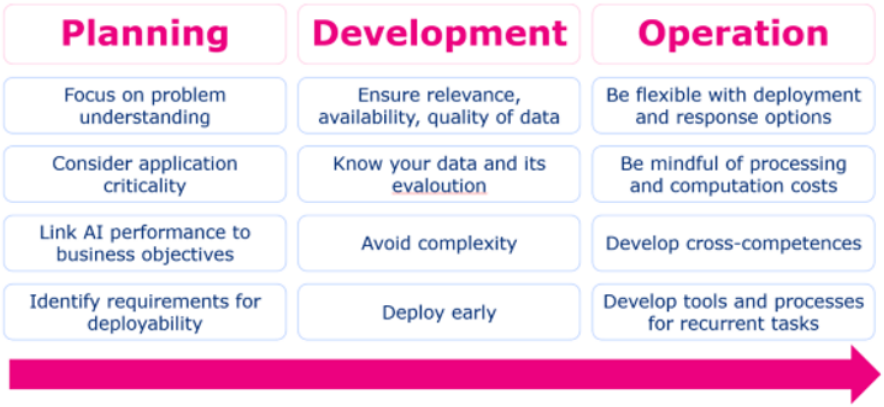


Figure 1: Keys for Successful AI applications in cybersecurity, organized by project stages

Figure 1 outlines key considerations for successful AI applications in cybersecurity, categorized by project stage. In the planning phase, focus on understanding the problem, assessing application criticality, and linking AI performance to business goals. Development emphasizes data quality, model knowledge, and simplicity. During operation, maintain flexibility in deployment and response, optimize costs, foster cross-competence between teams, and create reusable tools.

C. LLM Capabilities and Advantages in Cloud Network Security:

A Large Language Model (LLM) is a state-of-the-art Artificial Intelligence (AI) system that is capable of understanding and generating human-like text for use in security monitoring. ChatGPT and Gemini are typical examples of LLMs. LLMs employ deep learning and typically require expensive training on the applicable text data to be able to perform crucial functions such as security monitoring content creation and responding to user security questions. The application of LLM can resolve most of the security challenges involved in the use of traditional rule-bases security monitoring systems. With LLMs, it is possible to manage the complexity involved in cloud environments thus creating a holistic security view of the overall cloud security posture. The organization will be able to leverage AI and ML to automate and improve cloud security monitoring processes. Even though LLMs are still in their infancy, they are increasingly being adopted in cloud security environments and related disciplines of cybersecurity.

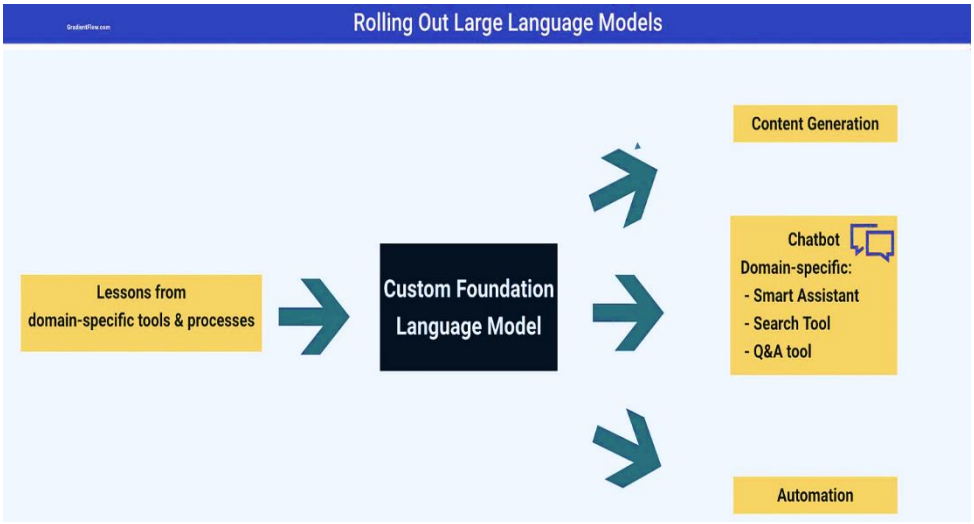


Figure 2: Framework for rolling out LLMs [35]

Figure 2 illustrates a framework for rolling out large language models. Utilizing lessons learned from domain-specific tools and processes, a custom foundation language model is developed. This model can be used for various applications such as content generation, automation, and domain-specific tools like chatbots, smart assistants, search tools, and Q&A tools.

LLMs differ from traditional rule-based network monitoring systems in many respects including their ability to learn and adapt to the changing cloud security landscape. By leveraging ML algorithms, LLMs can assess huge data volumes in real-time and detect patterns that may show potential security problems in the cloud environment. They can also identify security issues before they occur which allows organizations to take pre-emptive actions to reduce the impact of the security threats as well as downtime.

Yet another difference is that LLMs can be trained on a variety of data sets of network patterns, security logs and threat intelligence and integrated into security systems such as the Security Information and Event Management (SIEM) systems to significantly enhance their capabilities. Tuyishime *et al* (2023), studies the integration of LLMs and proves how they transform SIEMs from traditional security monitoring tools into advanced, intelligent platforms that can provide deeper insights, automating complex processes, and improving the overall efficiency of security operations [15].

LLMs offer many advantages over traditional rule-based monitoring which include the following;

1) **Detection of novel and zero-day exploits:** LLMs can detect novel and zero-day exploits in the cloud network environment, a capability that traditional rule-based monitoring systems are unable to accomplish. However, it is important to manage the use of LLMs in threat detection due to complications associated with security and privacy in the cloud. Therefore, ideally, expert security professionals should validate the LLMs' AI recommendations.

    a) **Identification of complex correlations**: LLMs can also be used to identify complex correlations between unrelated events within cloud environments as well as a holistic view of all the security events happening therein. They can also power chatbots that provide 24/7 assistance to security teams in their day-to-day duties, offering quick access to information and targeted guidance on incident resolution. The use of chatbots can improve operational efficiency and sparing security analysts to focus on more strategic cloud security activities.
    b) **Generation of alerts**: LLMs can also be applied in various security aspects due to their proficiency in Natural Language Processing (NLP). They can generate natural language alerts and detailed security. They can summarize key security findings and data points that can be used for further security analyses. This enhanced reporting and documentation capabilities assists in the performance of various audits and meeting compliance requirements.
    c) **Generation of quality reports**: They generate reports that are clear, concise yet comprehensive, and easily understandable therefore actionable for security teams. Therefore, the adoption of LLMs in cloud security can result in considerable time savings significantly reducing the time taken in investigating and responding to security threats and improved productivity among cloud security teams.

2) **Anomaly Detection with LLMs**: Anomaly detection is the major form of AI application in cybersecurity[14]. In anomaly detection, LLMs are proving to be critical in shaping the attributes of datasets that are required in most detection models thereby improving their efficacy and reliability. However, there is caution against the uncritical use of existing datasets for training large language models (LLMs) in cybersecurity applications[3]. Anomaly detection in cloud environments depends on the ability of the detection tools to correctly identify deviations from normal patterns. In this regard, LLMs can be put into learning modes and trained to detect such deviations thereby improving the anomaly detection processes in cloud networks. It is also stated that LLMs can also assist in User and Entity Behavior Analysis (UEBA) features[8]. These features can be incorporated in SIEMs to improve the detection of anomalies, suspicious activities, insider threats, compromised accounts, lateral movement within cloud networks and other cloud security threats. They can also analyze behavior patterns to distinguish between legitimate organizational activities and those activities that can be associated with potential security threats. Put simply, LLMs enhance the precision of behavioral analytics.

3) **Threat Intelligence Generation**: LLMs can be deployed to automatically analyze vast volumes of logs to identify network traffic patterns, anomalies, or signs of cyber threats that may not be detected using traditional methods. By understanding the context within security logs, LLMs can reduce false positives significantly and highlight genuine security incidents, thereby improving the accuracy of threat detection processes in the organization. Ferrag *et al* (2024), proposed the application of LLMs is revolutionizing threat detection in cybersecurity [2]. Through the thorough analysis of both current and historical security data, LLMs can generate actionable threat intelligence, offering insights into potential vulnerabilities, attack patterns, and recommended countermeasures. This capability by LLMs can assist organizations in proactively addressing security vulnerabilities before they are exploited by attackers.

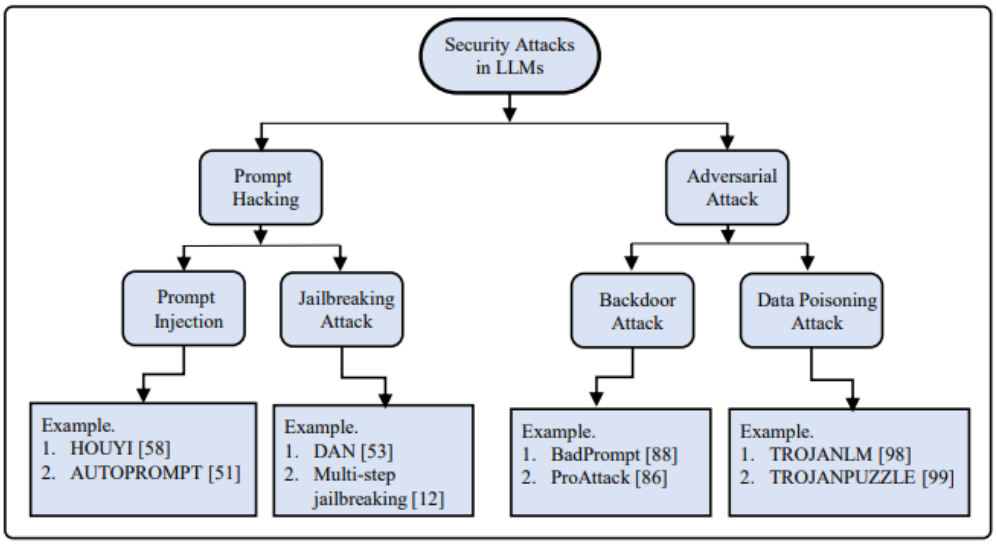


Figure 3: Security Attacks in LLM

Figure 3 illustrates a taxonomy of successful attacks on Machine Learning (ML) systems. These attacks are categorized into two primary types: poisoning attacks, which manipulate training data, and adversarial attacks, which exploit vulnerabilities during system operation. Poisoning attacks include both direct injection of malicious data and indirect influence through strategic actions. Adversarial attacks encompass backdoor attacks that trigger specific model behaviors and data poisoning attacks that corrupt operational data. Examples of each attack type are provided.

4) **Initial Incident Response Automation:** LLMs can be used in the automation of the initial analysis of cloud security events. They can understand large volumes of events data and reason over that data. The cloud incident management environment is so complex that the use of LLMs becomes very imperative. Wang (2023) states that LLM can analyze the root cause of the events and provide guidance in the generation of subsequent steps in the cloud incident response process. Diagram below refers;

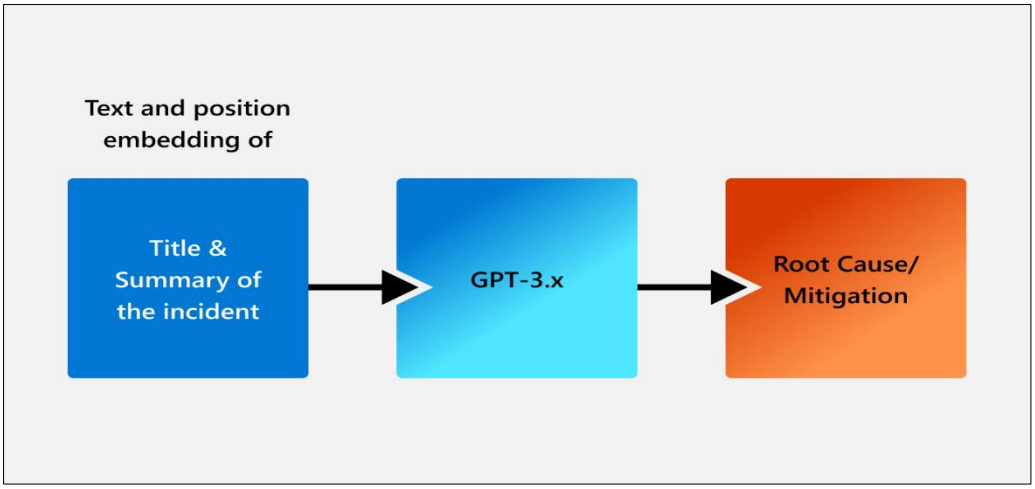


Figure 4: Cloud Incident Analysis and Mitigation Using LLM [36]

Figure 4 illustrates a process where the title and summary of an incident are embedded and input into GPT-3.x, which then generates an analysis of the root cause and suggests mitigation strategies. A recent study (Wang, 2023) suggests that large language models (LLMs) have the potential to analyze the root cause of events and guide subsequent steps in the cloud incident response process[11]. According to Ahmed (2023), once the root cause is known, steps should be taken to fix it[12] .The use of LLMs in this process are various including providing decision support for the response to events, generating the necessary scripts and enabling the automation of communication systems within the SOAR framework. LLMs can also automate parts of the incident response process by generating scripts or workflows. For example, a LLM can automatically draft communication affected users, advising them of s specific event and suggesting mitigatory measures.

Large language models (LLMs) offer significant potential for streamlining incident response processes in cloud environments. Phillips (2024) suggests integrating LLMs into Security Operations Centers (SOCs) to automate tasks such as initiating scripts and performing scans in response to anomalies[6]. This can reduce response times by up to 25% compared to traditional methods, leading to faster threat mitigation. Automation also minimizes human error and ensures consistency in initial response actions. Beyond cybersecurity, LLMs can enhance data correlation in fields like Human Resources, improving the efficiency of data loss prevention efforts.

III. REAL-WORLD APPLICATIONS AND CASE STUDIES: LEADING THE AI TRANSFORMATION

Large language models (LLMs) are revolutionizing cybersecurity and enhancing customer service in various industries. Microsoft's Copilot for Security utilizes LLMs to analyze security signals and provide real-time guidance to security professionals, significantly improving threat detection and response. Intuit's Institute Assist, an AI-powered virtual assistant, leverages LLMs to understand complex tax queries and provide accurate answers based on the latest tax laws. Walmart, in partnership with IBM, is utilizing AI in various aspects of its operations, including inventory management and customer service, to improve efficiency, reduce costs, and enhance the overall customer experience.

A. Microsoft Copilot for Security: Microsoft is pioneering the use of AI in cybersecurity with its Copilot (Fig. 5) for Security. This tool employs large language models (LLMs) to analyze security signals and offer real-time guidance to security professionals. By automating repetitive tasks and providing contextual insights, Copilot significantly enhances threat detection and response capabilities, making it a valuable asset in the fight against cyberattacks. Yao Y (2023) posits that LLMs offer promising solutions to cloud security practices by enhancing organization's threat and malware detection capabilities due to their capabilities to process large data sets [10]. As a result, they can spot attack patterns entity-wide and generate alerts. Farzad *et al* (2024) provides an overview of the use of LLMs threat detection to achieve compliance with the NIST Cybersecurity Framework (NIST CSF)[9]. Various vendors among them Sentinel and Microsoft have begun releasing LLM-driven threat detection technologies and provide automated responses and reports. Diagram below shows the application of LLMs in Microsoft Copilot for Security.

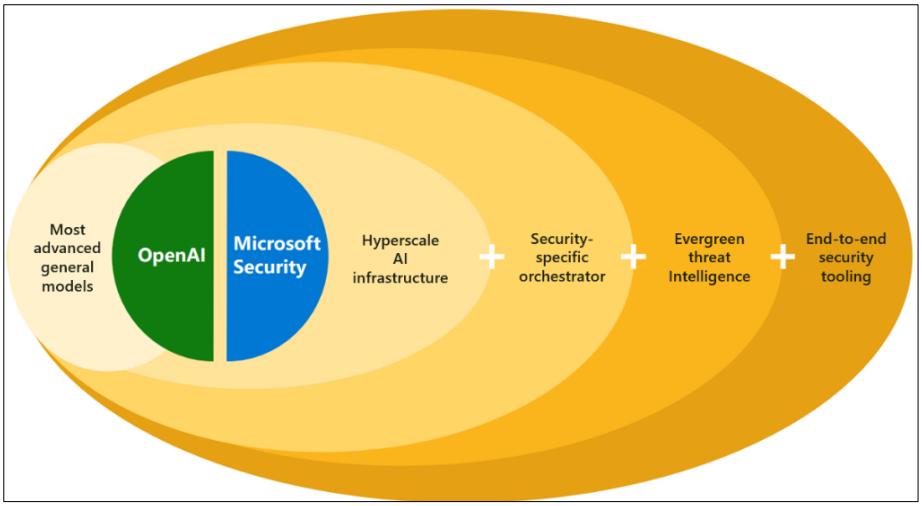


Figure 5: Microsoft Security Copilot's Layered Approach to Cybersecurity [16]

Microsoft Copilot for Security combines powerful LLMs with security-specific resources provisioned by Microsoft which are informed by Microsoft's threat intelligence as well as open-source intelligent feeds. Just to show how powerful it is, it leverages over 65 trillion daily signals, and includes information from various security solutions using plug-ins and other connections to knowledge bases.

Microsoft Copilot for Security has proven to be more relevant, powerful, and customized for the user and is supported by its learning capabilities to speed up the identification and responses to emerging threats. Its early adopters such as the three Australian companies namely Australian Super, Powerlink Queensland, and TAL, has reported significant improvements in their threat detection efforts. For example, Australian Super intends to boost productivity by 5% within a year through the adoption and implementation of AI technologies in cybersecurity, including Microsoft Copilot for Security. The adoption of Microsoft Copilot for Security at Powerlink Queensland has also led to an increase in the level of accuracy to in the work of its security team. The accuracy level started at around 50% and rose to within the range of 75-95% thus confirming the power of LLMs in enhancing cloud security.

B. Intuit's Institute Assist: Intuit, Intuit, has developed an AI-powered virtual assistant called Institute Assist[32]. Designed for accounting professionals, this tool leverages natural language processing (NLP) to understand complex tax queries and provide accurate answers based on the latest tax laws. Institute Assist streamlines research processes and enables accountants to deliver faster, more informed advice to their clients. Additionally, Intuit is also a leading provider of accounting software such as QuickBooks and have taken the lead in building their own LLMs by leveraging open-source models and training its own data. The company has developed its own Institute Assist feature that assists users in customer support incorporating security -related support.

C. Walmart and IBM's AI Applications: Walmart, in partnership with IBM, is utilizing AI in various aspects of its operations. For example, the company has deployed AI-powered robots to automate inventory management tasks, such as scanning shelves and identifying out-of-stock items.

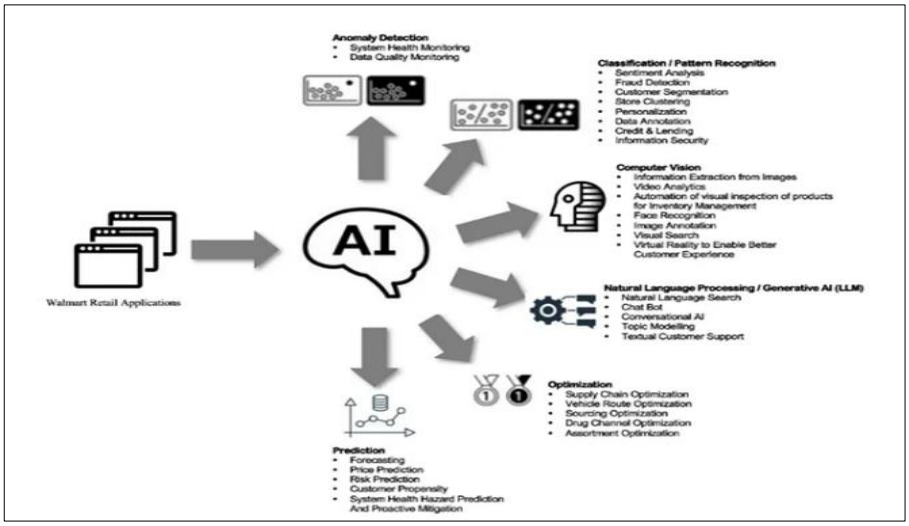


Figure 6: Applications of Artificial Intelligence (AI) in Walmart Retail [33]

Additionally, Walmart is exploring the use of AI in customer service, with chatbots assisting shoppers with their inquiries. These AI applications aim to improve efficiency, reduce costs, and enhance the overall customer experience.

When compared with other AI/ML tools, LLMs have fared well. For example, Generative AI is focused on the creation of models to produce original content rather than performed other functions performed by LLMs such as data and security analysis. While content may be required in cloud security, it is not as useful as security analysis carried out by LLMs. LLMS can deal with more parameters beyond mere content creation. Foundational models can be adapted to provide a base for cloud security but are not as focused as LLMs as they can be trained on specific security domains. When compared with Short Language Models (SLMs) which are based on short data sequences, LLMs are effective and versatile to deal with various sophisticated cloud security threats. However, it should be noted that all AI/ML tools are not designed to be mutually-exclusive but complement each ither in enhancing the organization's cloud security posture.

IV. CHALLENGES AND ETHICAL CONSIDERATIONS IN LARGE LANGUAGE MODEL (LLM) DEPLOYMENT

The deployment of large language models (LLMs) has ushered in a new era of possibilities across numerous domains. However, their integration into real-world applications is not without significant challenges and ethical considerations. These concerns encompass technical limitations, societal impacts, and the potential for misuse, all of which necessitate careful attention from researchers, developers, and policymakers alike.

A. Hallucinations and Bias: LLMs, despite their impressive capabilities, are prone to generating outputs that may be factually incorrect or biased, a phenomenon known as "hallucination." This arises from the models' reliance on statistical patterns in training data, which can perpetuate existing biases and inaccuracies. Mitigating hallucinations and biases requires ongoing research into robust evaluation metrics, debiasing techniques, and transparency in model training data [25][26]

B. Transparency and Accountability: The opacity of LLM decision-making processes raises concerns about transparency and accountability. Understanding how these models arrive at specific outputs is crucial for building trust and ensuring responsible use. Explainable AI (XAI) techniques, model documentation, and auditing mechanisms are essential tools for addressing these challenges [27][28]

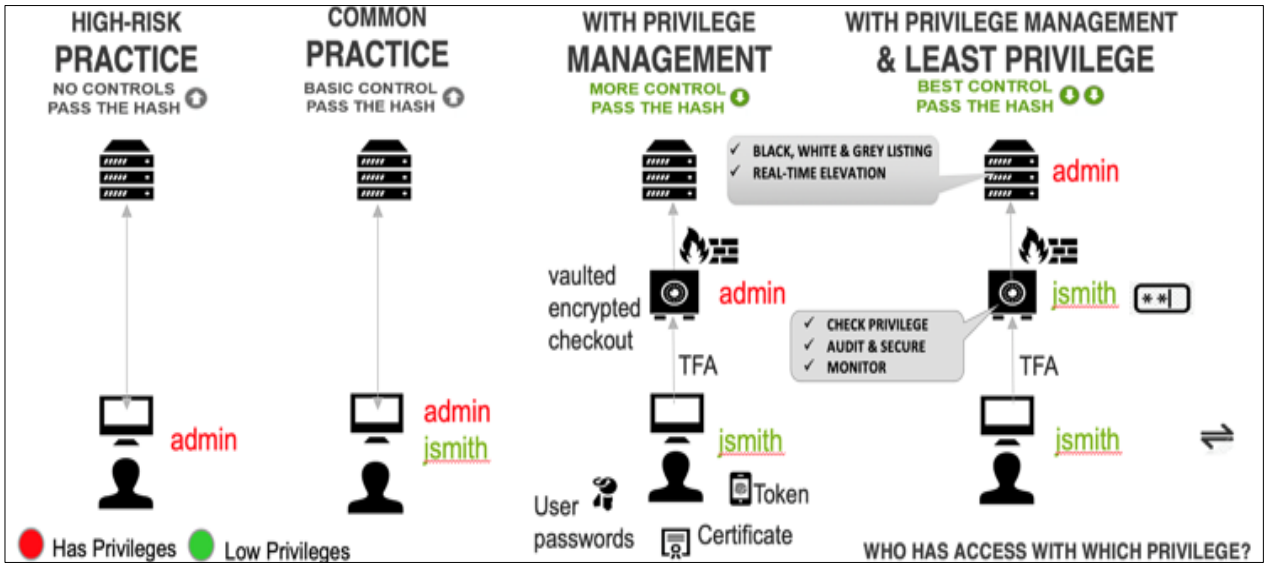
C. Privacy and Data Integrity: LLMs often require vast amounts of data for training, raising concerns about privacy and data integrity. Protecting sensitive information, anonymizing data, and obtaining informed consent are critical aspects of responsible LLM development. Additionally, ensuring the provenance and integrity of training data is essential for mitigating the risk of model manipulation or misuse [29][30]

D. Vulnerability to Cyberattacks: LLMs are susceptible to adversarial attacks, where malicious actors manipulate input data to trigger unintended or harmful behavior. These attacks can exploit vulnerabilities in model architecture, training data, or deployment environments. Robustness testing, adversarial training, and secure deployment practices are crucial for safeguarding LLMs against such threats [32]

V. MITIGATIG RISKS AND ENSURING RESPONSIBLE LLM USE

Large language models (LLMs) offer immense potential but also pose significant risks, including the generation of harmful content, the perpetuation of biases, and the potential for misuse. To mitigate these risks and ensure responsible LLM use, several key principles must be adhered to.

A. The Principle of Least Privilege (PoLP): The PoLP dictates that LLMs should only be granted the minimum level of access and capabilities necessary to perform their intended functions. By restricting LLM access to sensitive data and limiting their ability to execute potentially harmful actions, the risk of misuse and unintended consequences



can be significantly reduced. This principle aligns with security best practices outlined in works like Saltzer and Schroeder's seminal paper on protection systems [22]

Figure 6: Evolution of Privilege Management Towards Least Privilege

The diagram above illustrates the progression of privilege management strategies in cybersecurity. It begins with high-risk practices like no access controls and then moves to common practices with basic controls. It further shows how organizations can adopt privilege management solutions for enhanced security and finally achieve the best control through least privilege, where users have minimal necessary access, reducing the risk of unauthorized access and potential threats.

B. Rigorous Testing and Validation: Thorough testing and validation are crucial to identify and rectify any potential flaws or biases within LLMs. This process should involve a diverse range of inputs and scenarios to ensure that the model performs reliably and safely under various conditions. The field of software testing provides established methodologies, such as those described in Myers' "The Art of Software Testing," that can be adapted for LLM evaluation [23]

C. Human Oversight and Decision-Making: While LLMs can automate various tasks, it is essential to maintain human oversight and decision-making, particularly in high-stakes situations. Human judgment remains crucial for interpreting complex outputs, resolving ambiguities, and ensuring ethical considerations are taken into account. This approach echoes the principles of human-in-the-loop AI systems, as explored in research by Amershi et al. [24]

VI. EVALUATION AND FUTURE DIRECTIONS

However, despite their many benefits in cloud security, there is a need to guard against generalizing the effectiveness of LLMs due to the challenges encountered in their application. Su (2004) notes that LLMs often struggle to apply their learned patterns across diverse and complicated environments, contexts and in novel scenarios leading to a condition known as hallucination [36]. Yamin (2004) asserts that's hallucination may lead bias causing LLMs generating misleading outputs for the users [5]. LLMs are also not transparent in how they operate as they operate in a form of a 'black box' leading to issues around accountability for compliance purposes especially in regulated industries such as healthcare and finance. While challenges like hallucinations can be mitigated by implementing a variety of strategies including using quality training data and refining data sets and related prompting techniques, the knowledge possessed by LLMs depends on the quality of the input data and the training involved. Hence, they are not able to generate security insights beyond their information horizon.

During the deployment and integration of LLMs, organization face many practical challenges. Granting a LLM too much access to that organization's existing systems can heighten the risk of data privacy as the models may access and read sensitive files. There is also as risk of as the models interact with propriety data and code. The integrity of data may also be compromised as LLMs can lead to data alterations, corruption, or loss and in the process contravening various compliance requirements and raising the risk of fines, penalties, or loss of reputation. According to Das and Amin (2024), another challenge faced is the possibility of the LLMs falling prey to cyber-attacks such as adversarial attacks from threat actors [1]. Kanamugire and Faiq (2024) further state that such adversarial attacks can be targeted and untargeted based on the preferences of the attacker [4]. These challenges can be reduced by several measures such as adhering to the principle of least privilege when implementing LLMs and undertaking rigorous testing and validation of LLM AI models to align with security expectations. Human experts may also be involved to provide oversight and make critical security decisions during the implementation of LLMs in cloud security.

Because of the inherent limitations of the LLMs in their application in cloud security monitoring systems, this paper proposes certain measures to improve their operational effectiveness. Firstly, the paper proposes LLMs to be assisted by some form of self-management capabilities in the form of autonomic architecture and management to enhance their scalability. LLM-driven security monitoring systems can be automatically adjusted by several measures including increasing frequency or expanding monitoring perimeter. The system should be able to automatically redirect and recalibrate monitoring efforts to concentrate on security issues posing the greatest risk. Additionally in settings where transparency is mandated by laws and regulations, LLMs can be tuned to align with the principles of transparency in their operations. Future research on the use of LLMs to enhance cloud security should focus on various aspects such as integrating LLMs with other cloud security tools and platforms such as CSPM. Other areas of focus include developing explainable AI models to be incorporated in security applications.

VII. CONCLUSION

As this discussion shows the adoption of LLMs is crucial in improving threat detection, providing security insights and providing faster incident response in cloud security. In anomaly detection LLMs are critical in forecasting thus shaping the current cloud security technologies landscape. They enable the organization to increase the levels of security data availability and quality while reducing model bias in anomaly detection when compared to traditional rule-based network monitoring systems. The provision of actionable holistic insights is also an important benefit of LLM including the importation of rich graphics. LLMs also improve incident response processes by providing timely and information security alerts for the security teams.

This paper explores the critical role LLMs play within the context of cloud network monitoring systems. It started by providing a general overview of the limitations of the traditional network monitoring systems and then discussed the adoption of LLMs as a way of addressing the limitations of traditional rule-based monitoring systems and improving the security cloud environments. As can be discerned, LLMs bring sophisticated capabilities in the security cloud networks. However, the adoption of LLMs is also fraught with challenges which should be addressed if this technology is to be effective. Despite these challenges, cloud security has witnessed unprecedented through the use of LLMs in cloud security. This review therefore underscores the crucial importance of LLM in enhancing cloud network security. LLMs have immense potential to revolutionize the entire cloud network security architecture and the industry continues to look forward to the possibility of LLMS playing a pivotal role in addressing the various complexities involved in enhancing security in cloud environments.

VIII. REFERENCES

[1] Das B C and Amini M H (2024), *Security and Privacy Challenges of Large Language Models*, Arxiv

[2] Ferrag, Mohamed Amine *et al* (2024), *Revolutionizing Cyber Threat Detection with Large Language Models*`, Technology Innovation Institute, Abu Dhabi

[3] Genarri J (2024), *Considerations for Evaluating Large Language Models for Cybersecurity Tasks*, Carnegie Mellon University

[4] Kanamugire J and Faiq A.S (2024), *Security Issues in Large Language Models Such as ChatGPT*, St Cloud State University

[5] Yamin M. (2024), *Applications of LLMs for Generating Cyber Security Exercise Scenarios*, Norwegian University of Science and Technology

[6] Philip C (2024) *Automating Security Workflows with LLMs*, Medium

[7] Gruschka, Nils & Jensen, Meiko. (2010). *Attack Surfaces: A Taxonomy for Attacks on Cloud Services*.
[8] Marchal S et al (2024), *Applying Artificial Intelligence in Cybersecurity*, Finish Transport and Communications Agency
[9] Nourmohammadzadeh Motlagh, Farzad et al (2024), Large *Language Models in Cybersecurity: State-of-the-Art*
[10] Yao Y (2023), *A Survey on Large Language Model (LLM) Security and Privacy: The Good, The Bad, and The Ugly*
[11] Wang R (2023), *Large-language models for automatic cloud incident management*, ICSE
[12] Ahmed T (2023), *Recommending Root-Cause and Mitigation Steps for Cloud Incidents using Large Language Models,* ICSE
[13] Su J et al (2024), *Large Language Models for Forecasting and Anomaly Detection: A Systematic Literature Review*,
[14] Khabanda V (2023), *Application of Artificial Intelligence in Cybersecurity*,
[15] Tuyishime E et al (2023), *Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach,* MDPI
[16] *Describe Security Copilot* [Documentation]. Microsoft Learn. Retrieved May 25, 2024. https://learn.microsoft.com/en-us/training/modules/security-copilot-getting-started/2-describe-security-copilot
[17] Burt, Dan. *AI, Cybersecurity and Large Language Models* [Blog post]. Palo Alto Networks Blog. April 12, 2024. https://www.paloaltonetworks.com/blog/2024/04/ai-cybersecurity-and-large-language-models/
[18] *Exploring the Security Risks of Using Large Language Models* [White paper]. BrightSec. March 2024. https://brightsec.com/whitepapers/exploring-the-security-risks-of-using-large-language-models/
[19] Apruzzese, G. et al. "The role of machine learning in cybersecurity." Digital Threats: Research and Practice. 2023
[20] Dasgupta, D. et al. "Machine learning in cybersecurity: a comprehensive survey." The Journal of Defense Modeling and Simulation. 2022
[21] Sarker, I.H. et al. "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions." SN Computer Science. 2021
[22] Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278-1308.
[23] Myers, G. J., Sandler, C., & Badgett, T. (2011). The art of software testing. John Wiley & Sons.
[24] Amershi, S., Cakmak, M., Knox, W. B., & Kulesza, T. (2014). Power to the people: The role of humans in interactive machine learning. AI Magazine, 35(4), 105-120.
[25] Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610-623).
[26] Solaiman, I., & Dennison, C. (2021). Process for Adapting Language Models to Society (PALMS) with Values-Targeted Datasets. *arXiv preprint arXiv:2108.06183*.
[27] Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access*, 6, 52138-52160.
[28] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*.
[29] Carlini, N., Liu, C., Erlingsson, Ú., Kos, J., & Song, D. (2022). Extracting Training Data from Large Language Models. *arXiv preprint arXiv:2012.07805*.
[30] Jagielski, M., Carlini, N., Berthelot, D., Kurakin, A., Papernot, N., Goodfellow, I., ... & Abadi, M. (2020). High Accuracy and High Fidelity Extraction of Neural Networks. *arXiv preprint arXiv:2001.02597*.
[31] Alzantot, M., Sharma, Y., Elgohary, A., Ho, B. J., Srivastava, M., & Chang, K. W. (2018). Generating Natural Language Adversarial Examples. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing* (pp. 2890-2896).
[32] *Introducing Intuit Assist, the Generative AI-Powered Financial Assistant for Small Businesses and Consumers* [Press Release]. Intuit. May 25, 2023. https://www.intuit.com/company/press-room/press-releases/2023/introducing-intuit-assist-the-generative-ai-powered-financial-assistant-for-small-businesses-and-consumers/
[33] Sankaran, Karthik. *Machine Learning Platform at Walmart* [blog post]. Walmart Global Tech Blog. June 15, 2020. https://medium.com/walmartglobaltech/machine-learning-platform-at-walmart-b06819825ef7

[34] Smeyers, Jasper. *Unleashing LLMs in Cybersecurity: A Playbook for All Industries* [blog post]. Gradient Flow. May 17, 2023. https://gradientflow.substack.com/p/unleashing-llms-in-cybersecurity

[35] Goldstein, Ariel et al. *Large Language Models for Automatic Cloud Incident Management* [blog post]. Microsoft Research Blog. May 15, 2023. https://www.microsoft.com/en-us/research/blog/large-language-models-for-automatic-cloud-incident-management/

[36] Banerjee, Akanksha et al. *Language Models for Cloud Incident Response and Prevention*. arXiv preprint arXiv:2402.10350, 2023. https://arxiv.org/html/2402.10350v1