Journal of Artificial Intelligence General Science (JAIGS)

ISSN: 3006-4023 (Online), Volume 6 , Issue 1, 2024 DOI: 10.60087

Home page https://ojs.boulibrary.com/index.php/JAIGS

Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response

Rahul Marri[1], Sriram Varanasi[2], Satwik Varma Kalidindi Chaitanya[3],

Independent Researcher[1-3].

ABSTRACT

The evolving threat landscape in cybersecurity necessitates more advanced and efficient solutions for threat detection and response. Traditional Security Information and Event Management (SIEM) systems have limitations in handling large volumes of data and identifying sophisticated threats. This research explores the integration of SIEM solutions with data lakes, offering a scalable and flexible approach to managing security data. By leveraging artificial intelligence (AI) and machine learning (ML) algorithms, SIEM platforms can enhance their capabilities in real-time threat detection, automated response, and advanced analytics. This integration enables organizations to process vast amounts of structured and unstructured data from various sources, improving both the speed and accuracy of identifying security threats. The article examines the architecture, benefits, and challenges of combining SIEM with data lakes and AI, providing insights into how these technologies can collectively strengthen organizational security postures.

Keywords: SIEM, data lakes, artificial intelligence, machine learning, threat detection, cybersecurity, automated response, real-time analytics, security event management, advanced analytics.

ARTICLE INFO: *Received: 01.09.2024 Accepted: 20.09.2024 Published: 15.10.2024*

Introduction

In today's digital era, the rapid growth of cyber threats has put organizations under constant pressure to enhance their security infrastructures. Traditional methods of detecting and responding to security incidents are proving inadequate in the face of increasingly sophisticated and diverse attack vectors. As cybercriminals exploit complex techniques to infiltrate networks, organizations require more robust and intelligent solutions to safeguard their systems. Security Information and Event Management (SIEM) systems have long served as a cornerstone of cybersecurity, providing real-time monitoring, event correlation, and incident response across enterprise environments. However, conventional SIEM solutions often struggle to handle the sheer volume, variety, and velocity of data generated by modern IT infrastructures.

To address these limitations, the integration of SIEM platforms with data lakes and artificial intelligence (AI) presents a promising path forward. Data lakes offer the ability to store vast amounts of structured and unstructured data from multiple sources, breaking down silos and enabling deeper analysis. AI and machine learning (ML) technologies can then be applied to this data to enhance SIEM's ability to detect patterns, anomalies, and emerging threats that would otherwise be missed by traditional rule-based systems.

This article explores how the convergence of SIEM with data lakes and AI transforms threat detection and response capabilities. By leveraging advanced analytics, automation, and machine learning, organizations can significantly improve their ability to detect, investigate, and mitigate security threats in real time. This integration not only enhances the performance and scalability of SIEM systems but also paves the way for proactive security strategies that anticipate and neutralize threats before they can cause harm.

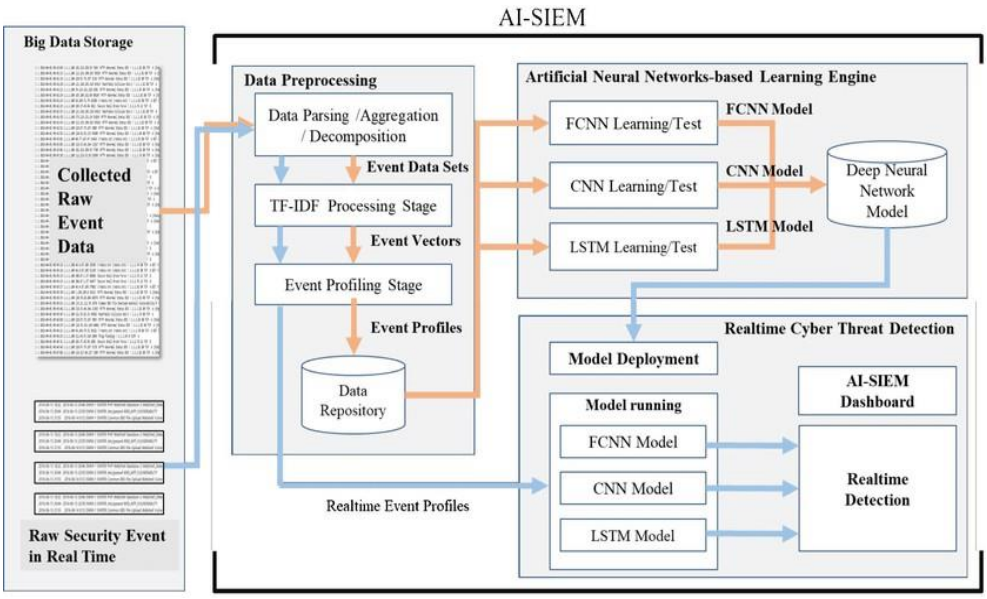

Fig. 1. The workflow and architecture for AI-powered SIEM system

While conventional Security Information and Event Management (SIEM) solutions have been a standard component of cybersecurity strategies, the growing complexity of cyberattacks presents new challenges. Threat actors are employing increasingly sophisticated methods that can severely compromise computer systems and networks. As a result, businesses must adopt more advanced cybersecurity solutions to stay ahead of these evolving threats. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful technologies that address the limitations of traditional SIEM systems.

AI and ML have revolutionized how businesses approach cybersecurity by leveraging self-learning capabilities and data-driven algorithms. These technologies enable AI- and ML-powered SIEM systems to detect and respond to security incidents more efficiently and rapidly while adapting to the ever-evolving nature of cyber threats. Additionally, AI and ML-based SIEM solutions can analyze vast amounts of data quickly and effectively, identifying patterns and anomalies that indicate potential threats.

These advancements are particularly transformative for real-time threat detection and mitigation, an area of increasing importance as cybercriminals also begin using similar technologies to carry out attacks. Rapid identification and neutralization of threats can significantly reduce the risk of data breaches, financial losses, and reputational harm for organizations.

Research Objectives:

1. Examine the Integration of SIEM Systems with Data Lakes:

Investigate how Security Information and Event Management (SIEM) systems can be effectively integrated with data lakes to enhance the storage, management, and processing of large-scale security data from diverse sources.

2. Evaluate the Role of AI and Machine Learning in Threat Detection:

Analyze the application of Artificial Intelligence (AI) and Machine Learning (ML) technologies in improving SIEM's ability to detect emerging and sophisticated cyber threats, including zero-day vulnerabilities and advanced persistent threats (APTs).

3. Assess the Impact on Real-Time Threat Response:

Explore how the integration of AI, ML, and data lakes with SIEM systems can improve real-time threat analysis, enabling faster incident detection, prioritization, and automated responses to mitigate cyberattacks.

4. Identify the Benefits and Challenges of Combining SIEM, Data Lakes, and AI:

Identify the key benefits, such as scalability, enhanced analytics, and anomaly detection, as well as the challenges, including data quality, system complexity, and privacy concerns, in adopting AI- and ML-enhanced SIEM systems integrated with data lakes.

5. Propose Best Practices for Implementation:

Develop a set of best practices and recommendations for organizations to implement and optimize the integration of SIEM systems with data lakes and AI, ensuring improved cybersecurity performance and effective threat management strategies.

Research Methodology:

The research methodology for this study on integrating Security Information and Event Management (SIEM) with data lakes and AI to enhance threat detection and response will adopt a multi-method approach. This approach combines qualitative and quantitative research techniques to thoroughly explore the technical, operational, and practical aspects of the integration. The methodology will include the following components:

1. Literature Review

- Objective:To gather insights from existing research, academic papers, industry reports, and case studies on the integration of SIEM systems, data lakes, and AI/ML technologies.

- Approach:

- Conduct a comprehensive review of existing literature related to SIEM systems, AI and ML applications in cybersecurity, data lake architecture, and advanced threat detection techniques.

- Analyze key trends, challenges, and solutions identified in previous studies, focusing on the technological evolution of SIEM platforms and the impact of data-driven AI approaches on threat detection.

2. Case Studies and Industry Analysis

- Objective: To evaluate real-world examples of organizations that have implemented integrated SIEM systems with data lakes and AI, and understand their outcomes, benefits, and challenges.

- Approach:

- Select case studies from industries with high cybersecurity requirements (e.g., finance, healthcare, and government).

- Analyze how these organizations are leveraging data lakes and AI to improve SIEM functionalities, such as threat detection, response automation, and scalability.

- Interview security professionals and analyze publicly available information on the effectiveness of these systems in improving threat detection and response times.

3. Data Collection and Analysis

- Objective: To collect and analyze both qualitative and quantitative data on the effectiveness of AI- and ML-enhanced SIEM systems integrated with data lakes.

- Approach:

- Primary Data: Conduct surveys and interviews with IT security experts, cybersecurity professionals, and data scientists from organizations using or planning to integrate AI-powered SIEM with data lakes.

- Develop a questionnaire focusing on current SIEM performance, the role of data lakes in enhancing data processing, and the perceived benefits and challenges of integrating AI/ML technologies.

- Secondary Data: Analyze historical and current cybersecurity data from organizations that have implemented AI-based SIEM solutions, focusing on incident response times, false positive/negative rates, and detection accuracy.

4. Experimental Setup and Simulation

- Objective: To test and evaluate the performance of an AI- and ML-powered SIEM system integrated with a data lake.

- Approach:

- Set up a simulated SIEM environment in which a data lake architecture is implemented for storing large volumes of security data from various sources (e.g., logs, network traffic, endpoints).

- Deploy AI and ML algorithms within the SIEM platform to monitor, analyze, and detect anomalies and threats.

- Measure the system's performance in real-time threat detection, anomaly identification, false positive/negative rates, and incident response times.

5. Comparative Analysis

- Objective: To compare the efficiency and effectiveness of traditional SIEM systems versus AI- and ML-enhanced SIEM systems with data lake integration.

- Approach:

- Perform a comparative analysis between legacy SIEM systems and modern integrated solutions, focusing on key metrics such as detection accuracy, response time, and system scalability.

- Use quantitative data from the experimental setup to evaluate improvements in cybersecurity capabilities after integration with AI, ML, and data lakes.

6. Data Interpretation and Recommendations

- Objective: To interpret the results of the research and provide recommendations for implementing AI-enhanced SIEM systems with data lakes.

- Approach:

- Synthesize findings from the literature review, case studies, interviews, and experimental data.

- Identify the key factors contributing to successful integration, such as best practices for AI/ML deployment, data lake management, and overcoming common integration challenges.

- Provide a set of actionable recommendations for organizations aiming to adopt these technologies to improve their cybersecurity infrastructure.

Key Features/Benefits of AI- and ML-Powered SIEM System

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into Security Information and Event Management (SIEM) systems has revolutionized the way organizations handle cybersecurity threats. These advanced technologies enhance the capabilities of traditional SIEM platforms, providing numerous key features and benefits that significantly improve threat detection, response, and overall security posture. Below are the core features and advantages of AI- and ML-powered SIEM systems:

1. Advanced Threat Detection

AI and ML algorithms can identify complex attack patterns and emerging threats that traditional rule-based SIEM systems might miss. These technologies continuously learn from data, improving their ability to detect new and unknown threats (zero-day attacks) by recognizing subtle patterns or anomalies in behavior that may indicate malicious activity.

2. Real-Time Threat Analysis and Response

One of the most significant benefits of AI- and ML-powered SIEM is the ability to analyze large volumes of data in real time. These systems can rapidly identify and respond to potential threats, allowing security teams to mitigate risks before they escalate. Automated responses to certain incidents can also significantly reduce response times, minimizing damage from security breaches.

3. Reduced False Positives

Conventional SIEM systems often generate a large number of false positives, overwhelming security teams and diverting attention from legitimate threats. AI- and ML-based systems can intelligently analyze data to reduce the occurrence of false positives by distinguishing between normal activity and real threats. This improves operational efficiency and enables teams to focus on critical alerts.

4. Behavioral Analysis and Anomaly Detection

AI- and ML-powered SIEM systems use behavioral analysis to monitor user and network activities. By establishing baseline behavior, these systems can detect anomalies or deviations that may indicate insider threats, compromised accounts, or sophisticated attacks. This proactive approach allows organizations to identify and address potential risks before significant damage occurs.

5. Scalability and Big Data Handling

Modern IT environments generate massive amounts of data from various sources, such as network traffic, applications, and devices. AI and ML enhance SIEM's ability to process and analyze vast amounts of structured and unstructured data efficiently. This scalability ensures that even large enterprises can maintain comprehensive security monitoring across diverse and growing data sets.

6. Predictive Threat Intelligence

AI and ML models can predict potential future attacks based on historical data, enabling organizations to anticipate and prevent threats before they occur. This predictive intelligence is a game-changer for cybersecurity, as it shifts the focus from reactive to proactive security measures.

7. Automation of Repetitive Tasks

AI- and ML-powered SIEM systems can automate routine and repetitive security tasks, such as log analysis, threat hunting, and incident triage. This automation frees up security teams to focus on higher-value activities, such as incident investigation and strategic planning, while also improving the overall speed and accuracy of security operations.

8. Enhanced Threat Correlation

By integrating AI and ML, SIEM systems can correlate data from multiple sources (such as logs, network traffic, and user activity) to build a comprehensive picture of security events. This correlation enables more precise identification of multi-stage attacks, which may involve various techniques deployed over time, helping security teams uncover sophisticated attack chains.

9. Continuous Learning and Adaptation

Unlike traditional systems that rely on static rules, AI- and ML-powered SIEM platforms continuously learn and adapt to changing environments and evolving threats. These systems improve over time as they analyze more data, making them increasingly effective at detecting and responding to new attack strategies.

10. Improved Compliance and Reporting

AI- and ML-powered SIEM systems can automate the process of generating compliance reports for various regulatory frameworks, such as GDPR, HIPAA, and PCI DSS. These systems can ensure that data is accurately collected, monitored, and reported, reducing the risk of non-compliance and streamlining audits.

Using AI and ML in SIEM Systems to Address Threat Detection and Mitigation Challenges

As cybersecurity threats grow more sophisticated, traditional Security Information and Event Management (SIEM) systems face significant challenges in effectively detecting and mitigating attacks. The increasing complexity of modern threats, the vast volume of security data, and the need for real-time responses demand advanced solutions that go beyond the capabilities of conventional SIEM platforms. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as transformative technologies in addressing these challenges by enhancing SIEM systems in several key areas, including threat detection, response automation, and anomaly identification.

1. Improving Detection of Sophisticated Attacks

Traditional SIEM systems often rely on static, rule-based methods to detect security incidents, which can be insufficient against complex and evolving attack techniques. These predefined rules can miss emerging threats such as zero-day attacks, advanced persistent threats (APTs), and multi-vector attacks that are designed to evade conventional detection mechanisms.

AI and ML address this limitation by learning from historical and real-time data to identify previously unknown threats. These technologies can analyze vast amounts of security data, recognizing subtle patterns that may indicate an attack in progress, even when it doesn't match known threat signatures. This makes AI- and ML-powered SIEM systems highly effective in detecting sophisticated cyberattacks, including those that evolve over time or involve multiple stages.

2. Handling Large Volumes of Data

Modern IT environments generate massive volumes of security-related data from an array of sources, including network traffic, application logs, endpoints, and cloud services. Conventional SIEM systems often struggle to process, analyze, and correlate this data in real time, leading to delayed threat detection and increased risk exposure.

AI and ML provide SIEM systems with the ability to process and analyze vast datasets efficiently. Machine learning algorithms can sift through massive volumes of security data, identifying correlations and anomalies much faster than manual methods. By automating the data analysis process, AI and ML can pinpoint potential security incidents more quickly, reducing detection times and enabling faster responses to mitigate the impact of an attack.

3. Addressing the Challenge of False Positives

One of the most significant pain points in traditional SIEM systems is the high number of false positives—alerts triggered by non-malicious activities that resemble potential threats. These false alarms overwhelm security teams, leading to alert fatigue and causing real threats to go undetected due to the volume of irrelevant notifications.

AI and ML-based SIEM systems are highly effective in reducing false positives by distinguishing between legitimate and suspicious activities more accurately. These systems learn over time, refining their ability to recognize normal behavior patterns and filtering out benign alerts. As a result, security teams can focus their efforts on investigating actual threats, improving the overall efficiency of threat detection and response operations.

4. Enhancing Anomaly Detection and Behavior Analysis

Anomalies in user behavior or network activity often indicate the presence of an insider threat or a compromised account. Traditional SIEM systems, which depend on predefined rules, may struggle to detect these subtle deviations from normal patterns, especially when the threat involves sophisticated tactics such as lateral movement or privilege escalation.

AI and ML enhance SIEM systems' ability to perform behavioral analysis by establishing a baseline of "normal" behavior for users, devices, and applications. Once these baselines are established, any deviation from expected behavior—such as unusual login times, abnormal data access, or excessive network activity—can be flagged as suspicious. This approach enables more effective detection of insider threats and advanced intrusions that might otherwise go unnoticed.

5. Automating Threat Response

Speed is critical in responding to cybersecurity incidents. The longer an attack goes undetected, the greater the damage it can cause. Traditional SIEM systems often require manual intervention for incident analysis and response, which can lead to delays in containment and mitigation.

AI- and ML-powered SIEM systems automate many aspects of the incident response process, enabling security teams to react to threats faster. For example, machine learning models can automatically identify the severity of an attack, prioritize incidents based on risk, and even initiate automated responses such as isolating affected devices, blocking malicious IP addresses, or shutting down compromised accounts. By automating these actions, organizations can reduce the time it takes to neutralize threats, minimizing the potential impact of cyberattacks.

6. Adaptive Learning and Continuous Improvement

One of the key advantages of AI and ML in SIEM systems is their ability to continuously learn and adapt. Traditional SIEM platforms depend on static rules and require constant manual updates to remain effective against new threats. In contrast, AI and ML models evolve with each new piece of data they analyze, improving their accuracy and effectiveness over time.

As new attack techniques emerge, AI and ML algorithms can incorporate these learnings into their threat detection models without requiring manual rule updates. This continuous learning process ensures that AI- and ML-powered SIEM systems stay ahead of the threat landscape, providing more reliable security even as adversaries adopt more advanced tactics.

Challenges Associated with the Adoption of AI and ML in SIEM Systems

While Artificial Intelligence (AI) and Machine Learning (ML) offer significant benefits to Security Information and Event Management (SIEM) systems, their integration is not without challenges. The adoption of AI and ML in cybersecurity requires careful consideration of various factors, including data quality, scalability, algorithm transparency, and the need for specialized expertise. These challenges can hinder the full realization of AI and ML's potential in SIEM systems, and organizations must address them to achieve successful implementation. Below are some of the key challenges associated with adopting AI and ML in SIEM systems:

1. Data Quality and Availability

AI and ML models depend heavily on high-quality data to function effectively. In the context of SIEM systems, vast amounts of security event data are generated from different sources, such as network traffic, application logs, endpoints, and cloud services. However, not all of this data is relevant or useful for training AI and ML models.

Inconsistent, incomplete, or noisy data can lead to inaccurate predictions and missed threats. Additionally, organizations often struggle to collect enough labeled data to train ML algorithms effectively. For AI- and ML-powered SIEM systems to work optimally, they need access to large volumes of diverse, high-quality data that accurately represents potential threats and normal behavior patterns. Ensuring data quality and availability is a key challenge, as poor data input will compromise the performance and accuracy of the AI and ML models.

2. False Positives and False Negatives

While AI and ML can reduce the number of false positives in SIEM systems, they are not immune to generating them. ML models, particularly in their early stages of deployment, may incorrectly classify legitimate activities as threats (false positives) or fail to detect actual threats (false negatives). High false-positive rates can overwhelm security teams and lead to alert fatigue, while false negatives pose a serious security risk, as they allow real threats to go undetected.

Tuning AI and ML algorithms to minimize both false positives and false negatives is a complex process that requires continuous monitoring and adjustment. These models need constant refinement and retraining based on feedback from security experts to improve their accuracy in distinguishing between legitimate and malicious activities.

3. Complexity of Implementation and Integration

Integrating AI and ML into existing SIEM systems can be a complex and resource-intensive process. Organizations need to ensure that their current infrastructure can support the high computational demands of AI and ML algorithms. This often requires significant upgrades in hardware, software, and network capabilities to handle the increased data processing and storage needs.

Moreover, AI and ML tools must be properly integrated with existing SIEM architectures and workflows. Many legacy systems were not designed to accommodate AI-driven technologies, making the integration process difficult and costly. Ensuring seamless interoperability between AI, ML, and other components within the SIEM ecosystem is a major challenge that requires careful planning and technical expertise.

4. Algorithm Transparency and Explainability

One of the challenges associated with AI and ML in SIEM systems is the lack of transparency, often referred to as the “black box” problem. AI and ML models, especially deep learning algorithms, can be highly complex, making it difficult to understand how they arrive at certain decisions or predictions. This lack of explainability can be problematic in cybersecurity, where security teams need clear, actionable insights to respond to threats effectively.

In cases where AI or ML flags a security incident, it is crucial for security analysts to understand the reasoning behind the alert in order to determine the appropriate response. If the model’s decisions are not transparent, it can lead to mistrust in the system and hinder its adoption. Developing AI and ML models that provide explainable and interpretable results is a significant challenge for cybersecurity professionals.

5. Evolving Threat Landscape

Cyber threats are constantly evolving, with attackers frequently developing new techniques to bypass security measures. While AI and ML can adapt and learn from new data, they are not immune to the

creativity and resourcefulness of malicious actors. Hackers are increasingly using AI and ML themselves to design more advanced attacks, making it a continual arms race between attackers and defenders.

ML models can also become outdated if they are not continuously updated with fresh data and evolving threat intelligence. Ensuring that AI and ML systems are regularly retrained to recognize new attack patterns is a challenge, especially for organizations with limited resources. Without proper updates, these systems may become less effective at identifying emerging threats.

6. Expertise and Resource Requirements

Implementing AI and ML in SIEM systems requires specialized expertise, which can be difficult to acquire. Data scientists, AI engineers, and cybersecurity experts must collaborate to develop, train, and maintain ML models. However, there is a shortage of professionals with the necessary skills to design and manage these systems effectively.

Additionally, building and maintaining AI- and ML-powered SIEM systems can be resource-intensive, requiring substantial investments in both personnel and infrastructure. Many organizations, particularly small and medium-sized enterprises (SMEs), may lack the resources or budget to adopt these advanced technologies fully. The cost and complexity of integrating AI and ML with SIEM systems can act as a significant barrier to entry.

7. Privacy and Ethical Concerns

AI and ML models used in SIEM systems rely on extensive data collection and analysis, which can raise privacy and ethical concerns. The vast amount of data gathered from network activity, user behavior, and system logs may include sensitive or personally identifiable information (PII). Organizations must ensure that they are in compliance with privacy regulations, such as GDPR or HIPAA, when collecting and processing security data.

There is also the ethical consideration of how AI and ML models make decisions. If an AI system makes biased or incorrect decisions due to flawed training data or algorithms, it could lead to unjust consequences, such as wrongful termination of access or unwarranted security actions against users. Addressing these privacy and ethical concerns is critical to gaining trust in AI- and ML-driven SIEM systems.

Conclusion:

Integrating Security Information and Event Management (SIEM) systems with data lakes and Artificial Intelligence (AI) presents a transformative approach to enhancing threat detection and response capabilities in modern cybersecurity. As cyber threats become more sophisticated and frequent, traditional SIEM systems face limitations in handling large volumes of security data, detecting advanced threats, and responding in real time. The integration of data lakes allows organizations to store and analyze massive amounts of security data from various sources, while AI and Machine Learning (ML) technologies bring advanced analytics and automation to detect emerging threats and reduce false positives.

By leveraging AI-driven SIEM systems with data lakes, organizations can improve their ability to identify complex attack patterns, enhance real-time threat detection, and respond to incidents more efficiently. However, this integration comes with challenges, including ensuring data quality, managing the complexity of AI models, and addressing resource constraints. Overcoming these obstacles requires careful planning, investment in infrastructure, and collaboration between security experts and data scientists.

Ultimately, the integration of SIEM with data lakes and AI represents a significant step forward in proactive cybersecurity defense. As organizations continue to adopt and refine these technologies, they can build more resilient systems capable of addressing the dynamic nature of modern cyber threats, reducing risks, and protecting critical assets more effectively.

References:

[1]. Sharma, A. (2024). Bridging Paradigms: The Integration of Symbolic and Connectionist AI in LLM-Driven Autonomous Agents. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *6*(1), 138-150.

[2]. Tamanampudi, V. M. (2024). CoWPE: Adaptive Context Window Adjustment in LLMs for Complex Input Queries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *5*(1), 438-450.

[3]. Sharma, A. (2024). The Development of an Automated Approach for Designing Quantum Algorithms Using Circuits Generated By Generative Adversarial Networks (Gans). *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *4*(1), 1-140.

[4]. Msekelwa, P. Z. (2024). The Impact of AI on Education: Innovative Tools and Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *5*(1), 227-236.

[5]. Gartner Research. (2020). Magic Quadrant for Security Information and Event Management. Retrieved from [Gartner Research](https://www.gartner.com/doc/reprints).

[6]. Hassan, W. U., & Bates, A. (2019). Data Lakes as a Foundation for Cybersecurity Analytics. IEEE Symposium on Security and Privacy, 49(4), 124-137. doi:10.1109/SP.2019.00053

[7]. Ali, M., Khan, S. U., & Vasilakos, A. V. (2019). Big Data-driven Security Information and Event Management: A Review. Future Generation Computer Systems, 87, 256-272. doi:10.1016/j.future.2017.09.019

[8]. Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051. doi:10.1109/COMST.2016.2548426

[9]. Xie, Y., Xu, M., & Qiu, M. (2021). Real-time Security Data Processing Framework for Big Data Analytics Using AI. International Journal of Distributed Sensor Networks, 17(2), 15501329211000378. doi:10.1177/15501329211000378

[10]. Gibert, D., Mateu, C., & Planes, J. (2020). The Rise of Machine Learning for Detection and Response: SIEM Evolution. ACM Computing Surveys, 53(4), 85-105. doi:10.1145/3409573

[11]. Sun, H., & Liu, Y. (2020). AI-Driven Threat Detection: Opportunities and Challenges in SIEM Systems. Journal of Network and Computer Applications, 169, 102755. doi:10.1016/j.jnca.2020.102755