JOURNAL OF BASIC SCIENCE AND ENGINEERING

A COMPREHENSIVE FRAMEWORK FOR AI-BASED THREAT INTELLIGENCE IN CLOUD CYBER SECURITY

Anjan Kumar Reddy Ayyadapu

Abstract

In the realm of cloud cyber security, the evolution of AI-based threat intelligence has become pivotal in safeguarding digital assets against increasingly sophisticated threats. This paper proposes a comprehensive framework for leveraging artificial intelligence (AI) to enhance threat intelligence capabilities within cloud environments. The framework integrates various stages of threat intelligence, including data collection, preprocessing, and feature engineering, with advanced AI and machine learning techniques such as supervised and unsupervised learning, and deep learning models. Key components include the threat intelligence lifecycle of detection, analysis, and mitigation, supported by diverse data sources like network traffic, user activity logs, and external threat feeds. Integration with existing security systems, evaluation metrics, and real-world case studies highlight practical implementations and successes. Challenges such as data privacy, scalability, and model interpretability are discussed, with future directions focusing on AI advancements and collaborative efforts to address evolving threats.

1. **Keywords: Threat Intelligence, Cloud Cyber Security, artificial intelligence AI.**

INTRODUCTION

Cloud computing has revolutionized businesses by providing scalable, on-demand access to computing resources. However, it has also introduced new challenges in cyber security. Artificial intelligence (AI) has emerged as a powerful tool in threat intelligence, leveraging machine learning algorithms and data analytics to detect, analyze, and respond to potential security incidents in real-time.

Figure 1: AI in cloud cyber security

This paper proposes a comprehensive framework for AI-based threat intelligence, covering the entire lifecycle of threat intelligence, from data collection and preprocessing to advanced AI model

deployment. The framework addresses practical implementation within cloud architectures and evaluates AI-driven threat intelligence effectiveness.

2. LITERATURE REVIEW

Ahmed, S. A. H. (2019) In his study, Ahmed explores the profound influence of artificial intelligence (AI) on the field of cybersecurity. He delves into how AI technologies, including machine learning and deep learning, can enhance threat intelligence, automate response mechanisms, and improve the overall resilience of cyber defenses. Ahmed discusses various AI-driven approaches to identifying and mitigating cyber threats, such as anomaly detection, predictive analytics, and automated incident response. The paper highlights both the potential benefits and challenges associated with integrating AI into cybersecurity practices, such as the need for large datasets for training AI models and the risk of adversarial attacks.

Angelopoulos, A., et al. (2019) conduct a thorough survey on the application of machine learning (ML) in addressing faults within the industry 4.0 framework. They study various ML solutions designed to enhance fault detection, diagnosis, and prediction in industrial environments. The authors categorize and analyze different ML techniques, including supervised, unsupervised, and reinforcement learning, and their suitability for specific fault management tasks. The paper also discusses key aspects such as data acquisition, preprocessing, and the integration of ML algorithms with industrial control systems. Through numerous case studies and practical examples, the authors demonstrate the effectiveness of ML in improving system reliability and operational efficiency.

Bäck, A. (2019) research focuses on the implementation of data-driven decision-making processes within industrial control systems (ICS). He examines how big data analytics and real-time data processing can enhance decision-making accuracy and efficiency in ICS. The paper discusses various data-driven techniques, including predictive maintenance, process optimization, and anomaly detection, and their applications in industrial settings. Bäck emphasizes the importance of data quality, integration, and governance in achieving effective data-driven decision-making. The study also highlights the challenges associated with data-driven approaches, such as data privacy, security, and the need for skilled personnel.

Baryannis, G., et al. (2019) provide an extensive study of the role of artificial intelligence (AI) in supply chain risk management (SCRM). They explore the current state-of-the-art AI technologies and their applications in identifying, assessing, and mitigating risks within supply chains. The paper categorizes AI techniques into predictive analytics, optimization algorithms, and simulation models, and discusses their effectiveness in various SCRM tasks. The authors highlight key challenges, such as data availability, model interpretability, and integration with existing supply chain systems. They also propose future research directions, emphasizing the need for more robust, scalable, and adaptive AI models to handle the complexity and dynamism of modern supply chains.

Dhaliwal, N. (2019) his paper focuses on the automation of analysis workflows in clinical systems using artificial intelligence (AI). He discusses the development and implementation of AI tools that streamline data upload, processing, and study, thereby enhancing efficiency and accuracy in clinical data management. The paper studies various AI techniques, such as natural language processing (NLP), machine learning, and computer vision, and their applications in automating clinical workflows. Dhaliwal highlights the benefits of AI-driven automation, including reduced manual effort, minimized errors, and improved data quality.

3. AI-BASED THREAT INTELLIGENCE AND INCIDENT RESPONSE IN CLOUD CYBER SECURITY

The cloud is forcing organisations to move their data and apps, which increases the requirement for effective incident response and sophisticated threat intelligence. Addressing cyber risks can be aided by integrating AI into cloud cyber security operations. AI lessens the impact of security issues by enabling faster and more accurate incident response. Comprehending the strategic integration of AI operations and cloud cyber security reduces the impact of security events, making it imperative for organisations to provide efficient and focused security solutions.

3.1. How AI is used in threat intelligence

Maintaining a strong defence against cyber threats requires being able to recognise possible dangers in cloud cybersecurity. AI gives businesses access to sophisticated capabilities that go beyond conventional methods, enabling them to strengthen their security.

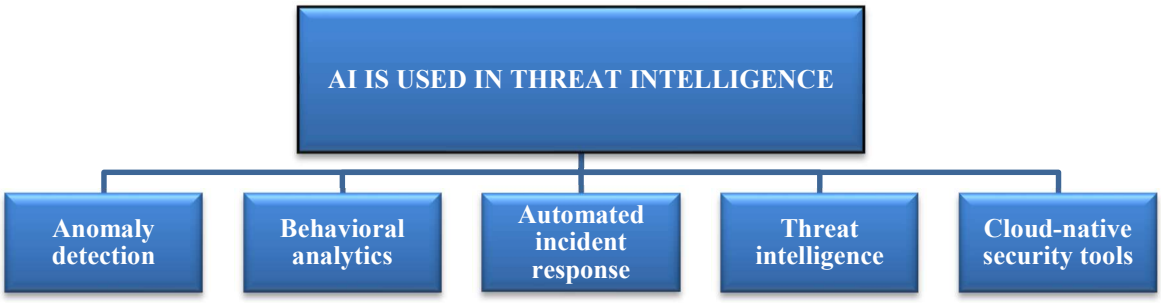

Figure 2: AI In Threat Intelligence

Here is how AI empowers proactive threat identification in Cloud Cyber Security;

3.1.1. Anomaly detection

Artificial intelligence (AI) systems are skilled at detecting anomalies, or departures from the usual, which helps defend against zero-day attacks. This is accomplished by creating baselines, which are dynamic procedures where AI continuously picks up new skills and keeps track of system and

user actions in a cloud environment. AI can swiftly discover possible security issues by identifying common interactions and patterns among individuals, systems, and apps through continuous observation and learning. For the purpose of spotting possible dangers like zero-day assaults, which conventional methods would not have been able to discover, AI-driven anomaly detection is essential.

3.1.2. Behavioral analytics

AI can strengthen defences against insider threats by monitoring users and using behavioural analytics. This strategy depends on AI's capacity to understand typical user behaviour and spot abnormalities. By using User and Entity Behaviour Analysis (UEBA) to identify anomalies in massive event streams, AI incorporates behavioural analytics into Cloud Cyber Security. UEBA uses user behaviour analysis—which looks at things like accessed resources, data download trends, geolocation, and login timing—to detect compromised accounts or insider threats. Additionally, AI uses natural language processing to examine communications for any threats.

3.1.3. Automated incident response

AI expedites recovery times and minimise damage by streamlining incident handling procedures. Without the need for human intervention, it can promptly detect and address attacks, improving the effectiveness of cloud cyber security. Artificial Intelligence can effectively respond by automatically quarantining infected devices or reversing alterations made by cybercriminals. Cyber security personnel can now concentrate on higher-value duties since it automates monotonous processes like setting up firewalls, running malware scans, reacting to alarms, patching vulnerabilities, and resetting passwords.

3.1.4. Threat intelligence

AI systems are able to deliver real-time updates on Cloud Cyber Security infrastructure by integrating with threat intelligence streams. With the most recent information at hand, this assists organisations in identifying and mitigating potential hazards. AI solutions are essential for implementing adaptive encryption models, automating key management, selectively encrypting high-risk data, and figuring out the best encryption tactics in complex cloud environments. AI also makes predictive analysis possible by using knowledge of existing risks to generate insights that can be used to bolster security measures.

3.1.5. Cloud-native security tools

By integrating AI for enhanced threat intelligence and incident response, cloud-native security platforms (CNSPs) improve security protocols in cloud environments. These platforms incorporate best practices for many parties, making compliance, disaster recovery, and monitoring tasks easier. Organisations can increase cloud-native monitoring and compliance, respond to developing cyber

threats, and streamline security measures across many clouds and providers by utilising AI's adaptable attribute.

3.2. The role of AI in modern security

Given that 80% of businesses experience cloud cyber security events and that 45% of breaches are cloud-based, artificial intelligence (AI) may be able to address today's security issues. Artificial intelligence (AI) can assess events, spot abnormalities, and link disparate data sets, which lessens the need for human expertise. This might remove the difficulty of finding, developing, and keeping qualified personnel, allowing cybersecurity specialists to concentrate on high-level evaluations and strategic initiatives.

4. BEST PRACTICES FOR AI- BASED CLOUD CYBER SECURITY

Following best practices is necessary to fully utilise AI in threat intelligence and cloud cyber security.

Figure 3: Best Practices for AI- Based Cloud Cyber Security

Organisations can enhance the efficacy of AI in Cloud Cyber Security and guarantee a strong defence against security threats by following these recommended procedures. This is what businesses should think about in order to improve their strategy.

4.1. Adopt a multi-layered security structure.

Incorporate AI within a thorough security architecture that includes stringent access rules, network segmentation, encryption for critical cloud data, and reliable key management procedures for safe storage methods.

4.2. Continuous Analysis

AI may be used to continuously analyse cloud environments, giving real-time insights and enhancing efficiency. Frequent penetration tests and vulnerability assessments can find possible vulnerabilities and measure defensive capabilities.

4.3. Integration with existing security tools

To create a cohesive security environment, integrate AI-enabled security tools with your current infrastructure. Recognise and abide by the security features offered by cloud service providers. For enhanced protection, make use of native Cloud Cyber protection services such as AWS Security Hub, Azure Centre, or Google Cloud Cyber Security Command Centre.

4.4. Deploy advanced security monitoring

Organisations should use AI-powered technology to improve real-time threat analysis, automated incident response, and continuous monitoring and intrusion detection systems for cloud cyber security.

4.5. Alert triage with AI

Using AI for alert triage helps Cloud Cyber Security incident response by classifying and ranking security alerts. Incoming alerts are analysed by AI systems, which use preset criteria to determine the alert's relevancy and severity. Security teams can concentrate on the most serious threats first because this simplifies the triage procedure. Artificial intelligence (AI) has the ability to distinguish between true threats and false positives, recognise minute indicators of possible occurrences, and interact with threat intelligence streams for in-the-moment threat analysis. AI is capable of learning from feedback and previous events, adjusting to changing threat environments and speeding up response times.

4.6. Automated containment measures

By putting infected devices in quarantine and blocking questionable IP addresses, AI systems can automate security actions. Rapid reactions to security problems, such malware outbreaks, are made possible by these activities. AI is also capable of containing incidents by limiting their severity and initiating pre-programmed playbooks for blocking, patching, and isolating. This quickens containment efforts and boosts Service Organizations' (SOCs') operational and security effectiveness.

5. BENEFITS OF INFUSING AI INTO CLOUD CYBER SECURITY

By addressing sophisticated cyber threats and boosting the resilience of Cloud Cyber Security infrastructure, AI integration in Cloud Cyber Security assessment improves resilience and flexibility.

Vol. 16, No. 1, (2019)
ISSN: 1005-0930

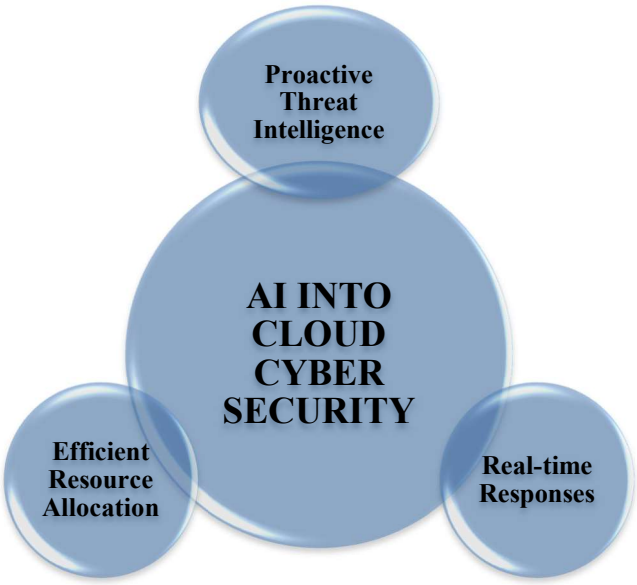

Figure 4: AI Into Cloud Cyber Security

The incorporation of artificial intelligence (AI) into cloud cyber security is a significant development in protecting digital assets from ever changing threats. Organisations may enhance their defences and battle sophisticated cyber threats in dynamic cloud settings by utilising AI-driven proactive threat intelligence, real-time response capabilities, and effective resource allocation.

5.1. Proactive threat intelligence

By examining anomalies in large datasets, AI-powered systems may predict security dangers. This helps enterprises recognise possible attacks before they materialize and strengthens their assertive security posture.

5.2. Real-time responses

AI's real-time capabilities is critical to improving cloud cyber security since it allows for immediate responses to any threats, guaranteeing prompt and effective actions to preserve the integrity of digital assets in dynamic cloud environments where prompt intervention is necessary.

5.3. Efficient resource allocation

The analytical power of AI facilitates the identification of the best resource allocation within Cloud Cyber Security frameworks, guaranteeing strategic deployment to high-risk regions, improving overall security, and simplifying resource management.

6. CONCLUSION

Vol. 16, No. 1, (2019)
ISSN: 1005-0930

To handle changing threats, a thorough architecture for AI-based threat intelligence in cloud cyber security must be developed. Organisations can greatly improve their cyber resilience by utilising AI's proactive capabilities for threat detection, real-time reactivity, and effective resource allocation. This framework opens the door for more secure cloud computing infrastructures by enhancing threat mitigation and guaranteeing strong protection of digital assets in dynamic cloud settings.

REFERENCES

1. *Ahmed, S. A. H. (2019). The Impact of Artificial Intelligence on Cyber Security.*
2. *Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., & Zahariadis, T. (2019). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. Sensors, 20(1), 109.*
3. *Bäck, A. (2019). Data driven decision making in Industrial Control Systems.*
4. *Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: state of the art and future research directions. International journal of production research, 57(7), 2179-2202.*
5. *Dhaliwal, N. (2019). Automating Analysis Workflows With Ai: Tools For Streamlined Data Upload And Review In Clinical Systems. Journal Of Basic Science And Engineering, 16(1).*
6. *Favour, O., & Potter, K. (2019). AI-driven Test Case Optimization for Performance Engineering.*
7. *Gerostathopoulos, I., Konersmann, M., Krusche, S., Mattos, D. I., Bosch, J., Bures, T., ... & Figalist, I. (2019). Continuous data-driven software engineering-towards a research agenda: Report on the joint 5th international workshop on rapid continuous software engineering (rcose 2019) and 1st international works. ACM SIGSOFT Software Engineering Notes, 44(3), 60-64.*
8. *IBRAHIM, A. (2019). The Cyber Frontier: AI and ML in Next-Gen Threat intelligence.*
9. *Liu, C., Li, H., Tang, Y., Lin, D., & Liu, J. (2019). Next generation integrated smart manufacturing based on big data analytics, reinforced learning, and optimal routes planning methods. International Journal of Computer Integrated Manufacturing, 32(9), 820-831.*
10. *Ramagundam, S., Das, S. R., Morton, S., Biswas, S. N., Groza, V., Assaf, M. H., & Petriu, E. M. (2014, May). Design and implementation of high-performance master/slave memory controller with microcontroller bus architecture. In 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings (pp. 10-15). IEEE.*
11. *Mawlad, A. A., Mohand, R., Agnihotri, P., Pamungkas, S., Omobude, O., Mustapha, H., ... & Razouki, A. (2019, November). Embracing the digital and artificial intelligence revolution for reservoir management-Intelligent integrated subsurface modelling IISM. In Abu Dhabi International Petroleum Exhibition and Conference (p. D011S004R004). SPE.*

12. *Ramagundam, S., Das, S. R., Biswas, S. N., Morton, S., Assaf, M. H., & Ozkarahan, I. (2013). AMBA-BASED AHB MASTER/SLAVE MEMORY CONTROLLER DESIGN. Transformative Science and Engineering, Business and Social Innovation, 23.*
13. *ORA-FR, L. B., Guillemin, F., Tępiński, R., Rosiński, M., Jegier, J., EUR, T. S., ... & EUR, A. K. (2019). Deliverable D4. 2 Final Report on AI-driven Techniques for the MonB5G Decision Engine.*
14. *Taskforce, H. M. A. E. M. A. J. B. (2019). Phase II Report:'Evolving Data-Driven Regulation'. European Medicines Agency.*
15. *Ramagundam, S. (2014). Design and Implementation of Advanced Microcontroller Bus Architecture High-performance Bus with Memory Controller in Verilog Hardware Description Language (Doctoral dissertation, Troy University).*
16. *Tu, W., Li, L., Shang, C., Liu, S., & Zhu, Y. (2019). Comprehensive risk assessment and engineering application of mine water inrush based on normal cloud model and local variable weight. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, 1-16.*
17. *Varney, A. (2019). Analysis of the impact of artificial intelligence to cybersecurity and protected digital ecosystems (Master's thesis, Utica College).*
18. *Wang, D., Zhang, D., Zhang, Y., Rashid, M. T., Shang, L., & Wei, N. (2019, December). Social edge intelligence: Integrating human and artificial intelligence at the edge. In 2019 IEEE First International Conference on Cognitive Machine Intelligence (CogMI) (pp. 194-201). IEEE.*