International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

Building Generative AI Driven Cloud Native Platforms for Enterprise Threat Intelligence and Automated Response

Geetha Nagarajan

Department of CSE, SA Engineering College, Chennai, India

ABSTRACT: Generative artificial intelligence (GenAI) is transforming enterprise cybersecurity by enabling cloud-native platforms that can analyze complex threat environments, generate actionable intelligence, and automate incident response processes. Modern enterprises face increasingly sophisticated cyber threats that require adaptive and intelligent security mechanisms beyond traditional detection systems. Generative AI-driven cloud platforms combine large language models, machine learning techniques, cloud computing architectures, and security automation to improve threat identification, investigation, and mitigation. These platforms process vast amounts of security data from multiple sources, including networks, applications, endpoints, and external intelligence feeds, to generate contextual insights and support faster decision-making. This research examines the development of GenAI-driven cloud-native platforms for enterprise threat intelligence and automated response. It explores technological foundations, existing research trends, and methodological approaches for evaluating intelligent cybersecurity solutions. The study highlights how generative AI can enhance proactive defense capabilities while addressing challenges related to scalability, privacy, reliability, and responsible AI deployment.

KEYWORDS: Generative artificial intelligence, cloud-native platforms, enterprise cybersecurity, threat intelligence, automated response, machine learning, large language models, security automation, cloud computing, incident response

I. INTRODUCTION

The rapid expansion of digital transformation has resulted in enterprises adopting cloud-native technologies to improve scalability, flexibility, and operational efficiency. Cloud-native platforms based on microservices, containers, serverless computing, and distributed architectures allow organizations to develop and deploy applications rapidly while supporting global business operations. However, this transformation has also increased cybersecurity complexity by expanding attack surfaces and introducing new vulnerabilities across interconnected digital environments. Organizations now face advanced cyber threats, including automated malware campaigns, supply chain attacks, identity-based intrusions, and highly adaptive adversarial techniques. Traditional cybersecurity approaches based on predefined rules and manual investigation processes are increasingly insufficient for addressing the speed and complexity of modern threats.

Generative artificial intelligence has emerged as a promising technology for enhancing enterprise cybersecurity operations. Unlike conventional artificial intelligence systems that primarily classify or detect patterns, generative AI models can create new information, summarize complex security events, generate analytical reports, and assist security teams in decision-making. When integrated into cloud-native platforms, GenAI can continuously analyze large-scale security data and provide intelligent recommendations for threat detection and automated response. These capabilities enable security teams to move from reactive incident management toward proactive threat prevention.

Enterprise threat intelligence requires the collection, processing, and interpretation of diverse security information from internal and external sources. GenAI-driven platforms can improve this process by correlating threat indicators, analyzing attacker behaviors, and generating contextual explanations of potential risks. Large language models and advanced analytics systems can assist security analysts by reducing investigation time and improving understanding of complex attack scenarios. Furthermore, automated response capabilities allow cloud-native security platforms to execute predefined or AI-generated actions, such as isolating compromised systems, blocking malicious activities, and initiating recovery procedures.

Despite these advantages, implementing generative AI-driven cybersecurity platforms introduces significant challenges. Issues related to data privacy, model accuracy, hallucination risks, adversarial manipulation, regulatory compliance, and operational governance require careful consideration. Enterprises must develop secure AI architectures that balance automation with human oversight and ensure trustworthy decision-making. This research investigates the

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

development of GenAI-driven cloud-native platforms for enterprise threat intelligence and automated response by examining existing technologies, research developments, implementation strategies, and future opportunities for intelligent cybersecurity ecosystems.

II. LITERATURE REVIEW

The literature on generative AI-driven cybersecurity platforms demonstrates increasing interest in integrating artificial intelligence capabilities with cloud-native architectures to improve enterprise defense mechanisms. Previous research on cloud computing security emphasizes that modern enterprises require dynamic and scalable security solutions capable of operating across distributed infrastructures. Traditional cybersecurity systems often depend on manually configured rules, signatures, and human-driven analysis, which limits their effectiveness against rapidly evolving cyber threats. Researchers have therefore explored artificial intelligence and machine learning approaches as methods for improving detection accuracy, response speed, and security automation.

Studies on cloud-native security architectures highlight the importance of designing flexible and resilient platforms that support continuous monitoring and rapid adaptation. Cloud-native environments introduce unique security challenges because applications are distributed across containers, APIs, microservices, and hybrid infrastructures. Research indicates that security mechanisms must be integrated throughout the software development and operational lifecycle rather than added as isolated protective layers. Approaches such as DevSecOps, automated compliance monitoring, and intelligent vulnerability management have become important areas of investigation.

Recent literature focusing on generative AI highlights its potential to transform cybersecurity operations through advanced reasoning, natural language understanding, and automated knowledge generation. Large language models have been investigated for applications such as security log analysis, malware explanation, vulnerability assessment, and incident investigation assistance. Researchers suggest that GenAI can improve security analyst productivity by summarizing large volumes of technical information and generating meaningful insights from complex datasets. These capabilities are particularly valuable in enterprise environments where security teams must manage overwhelming quantities of alerts and intelligence reports.

Threat intelligence research emphasizes the importance of collecting and analyzing information about emerging cyber risks. Conventional threat intelligence systems often struggle with fragmented data sources and limited contextual understanding. Generative AI technologies provide opportunities to improve threat intelligence by automatically correlating information from security feeds, historical incidents, vulnerability databases, and operational logs. Studies indicate that AI-driven intelligence platforms can identify relationships between seemingly unrelated security events and generate predictive assessments of potential attacks.

Research on automated response systems demonstrates the growing importance of intelligent orchestration in cybersecurity operations. Security orchestration, automation, and response (SOAR) technologies have traditionally focused on predefined workflows for incident management. The integration of generative AI expands these capabilities by enabling adaptive response strategies based on real-time analysis. AI systems can recommend mitigation actions, generate response procedures, and assist organizations in reducing the impact of security incidents.

However, existing literature also identifies several limitations associated with GenAI-based cybersecurity platforms. Researchers highlight concerns regarding inaccurate AI-generated outputs, insufficient explainability, data confidentiality risks, and vulnerability to adversarial attacks. Since generative AI models depend on large datasets, organizations must implement strong governance frameworks to protect sensitive information and maintain compliance with cybersecurity regulations. Additionally, human expertise remains essential for validating AI-generated recommendations and managing complex security decisions.

Overall, current research demonstrates that generative AI-driven cloud-native platforms have significant potential to enhance enterprise threat intelligence and automated response capabilities. The combination of cloud scalability, artificial intelligence reasoning, and security automation provides organizations with opportunities to develop more proactive and adaptive cybersecurity strategies. However, further research is required to address technical, ethical, and operational challenges associated with deploying trustworthy GenAI security platforms in enterprise environments.

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2023.0605005

III. RESEARCH METHODOLOGY

The research methodology adopted for this study focuses on a comprehensive investigation of generative AI-driven cloud-native platforms for enterprise threat intelligence and automated response. The methodology is designed to analyze the technological components, operational capabilities, security effectiveness, and implementation challenges associated with integrating generative artificial intelligence into modern cloud-native cybersecurity environments. Since the research topic involves multiple interconnected domains, including artificial intelligence, cloud computing, cybersecurity analytics, automation, and enterprise security management, a structured qualitative and analytical research approach is employed. The methodology combines systematic literature analysis, conceptual framework development, comparative evaluation, and assessment of emerging technological practices to understand how GenAI can enhance enterprise cybersecurity operations.

The research follows an exploratory and descriptive research design because generative AI applications in cybersecurity represent an emerging field with rapidly evolving technologies and operational models. Exploratory research enables the identification of current trends, technological developments, and unresolved challenges associated with GenAI-powered security platforms. The descriptive component focuses on examining existing cloud-native architectures, threat intelligence approaches, and automated response mechanisms to understand their practical applications in enterprise environments. This combination allows the research to evaluate both theoretical concepts and practical considerations related to implementing intelligent cybersecurity solutions.

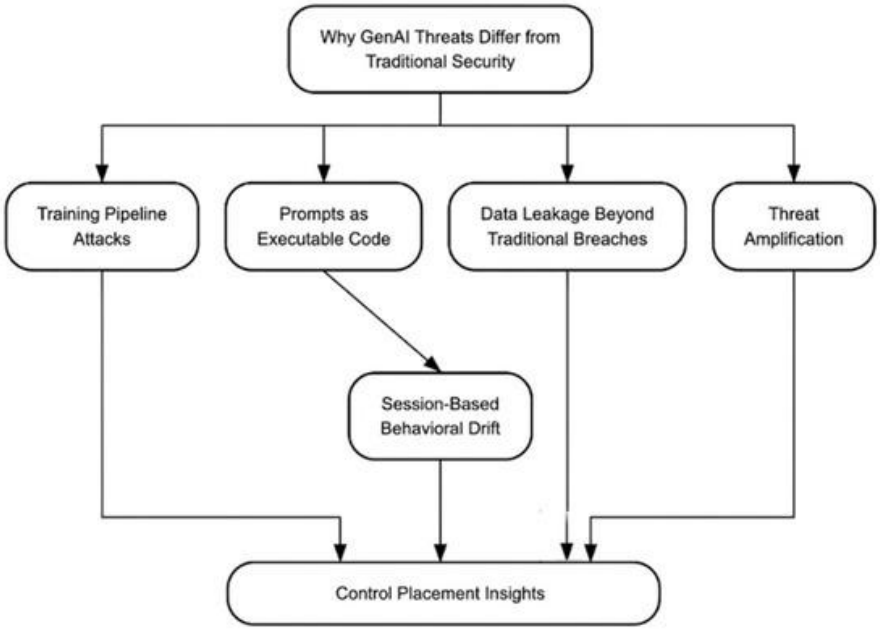


Fig.1. Securing Generative AI Systems: Threat-Centric Architectures

The first stage of the methodology involves a systematic review of existing academic literature, industry publications, cybersecurity frameworks, and technical reports related to generative AI, cloud-native computing, and enterprise threat intelligence. Relevant sources are analyzed to identify major technological developments, research findings, and limitations within current approaches. The literature review process focuses on several key areas, including large language models in cybersecurity, AI-based threat detection, cloud-native security architectures, automated incident response, security orchestration, and responsible AI governance. Information collected from these sources provides the foundation for understanding how GenAI technologies are transforming traditional cybersecurity practices.

A qualitative analytical approach is used to evaluate the role of generative AI models in enterprise threat intelligence operations. The research examines how large language models and other generative AI systems can support activities such as security event interpretation, vulnerability analysis, threat report generation, and incident investigation. The analysis considers the ability of GenAI systems to process large volumes of structured and unstructured security data, including system logs, network information, threat intelligence reports, and vulnerability records. The methodology evaluates how these capabilities contribute to faster threat identification and improved decision-making for cybersecurity professionals.

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

The study also analyzes cloud-native architectures that support the deployment of generative AI security applications. Cloud-native environments are examined based on their use of containerization, microservices, application programming interfaces, distributed computing, and automated infrastructure management. The research evaluates how these architectural approaches enable scalable AI-powered security operations. Particular attention is given to the integration of AI models with cloud security platforms, data pipelines, monitoring systems, and automated response frameworks. This analysis helps determine the architectural requirements necessary for developing effective GenAI-driven cybersecurity platforms.

A conceptual framework is developed as part of the methodology to illustrate the relationship between cloud-native infrastructure, generative AI capabilities, threat intelligence processes, and automated response mechanisms. The framework consists of multiple interconnected layers. The data acquisition layer collects information from enterprise networks, applications, endpoints, cloud services, and external threat intelligence sources. The processing layer applies secure data management techniques, preprocessing methods, and analytical models to prepare information for AI-based analysis. The intelligence layer incorporates generative AI models capable of interpreting security information, generating insights, and supporting predictive analysis. The response layer enables automated actions such as threat containment, security alerts, policy updates, and incident remediation.

The research methodology includes a comparative evaluation of traditional cybersecurity approaches and GenAI-enhanced security platforms. The comparison focuses on important performance dimensions, including threat detection capability, response speed, scalability, automation level, adaptability, and operational efficiency. Traditional security systems generally depend on predefined detection rules and manual analysis, whereas GenAI-based systems provide adaptive intelligence and automated reasoning capabilities. By comparing these approaches, the research identifies the improvements and limitations associated with adopting generative AI in enterprise security environments.

Threat intelligence capabilities are evaluated through several analytical factors. The study examines how GenAI platforms collect, analyze, and interpret threat-related information to generate meaningful security insights. Important evaluation criteria include the ability to identify emerging attack patterns, correlate multiple threat indicators, provide contextual explanations, and support predictive risk assessment. The methodology considers the importance of real-time intelligence generation because modern cyberattacks often evolve rapidly and require immediate organizational responses. AI-driven threat intelligence is assessed according to its ability to reduce investigation time and improve the accuracy of security decisions.

Automated response mechanisms are another major focus of the research methodology. The study examines how GenAI-powered systems can improve incident response through intelligent automation. The analysis considers automated processes such as alert prioritization, response recommendation generation, threat containment, remediation planning, and security workflow optimization. The methodology evaluates whether AI-generated responses can reduce the workload of security teams while maintaining appropriate levels of accuracy and control. The importance of human oversight is also considered, as cybersecurity decisions often require expert validation and organizational context.

The methodology incorporates security and privacy assessment to evaluate potential risks associated with implementing generative AI systems. Since GenAI platforms require access to large quantities of enterprise data, the research examines challenges related to data confidentiality, access control, secure model training, and regulatory compliance. The study evaluates security measures such as encryption, identity management, data anonymization, and model governance practices. Additionally, risks associated with AI-generated misinformation, model hallucination, prompt manipulation, and adversarial attacks are considered. These factors are analyzed to determine requirements for building trustworthy and secure AI-powered cybersecurity platforms.

Ethical considerations are integrated into the methodology because responsible AI deployment is essential in enterprise security environments. The research examines issues related to transparency, accountability, fairness, and explainability. Since AI systems may influence critical security decisions, organizations must ensure that automated recommendations can be reviewed and understood by cybersecurity professionals. The methodology therefore emphasizes the importance of explainable AI techniques and human-centered security operations to maintain trust and reliability.

The research also considers organizational and operational factors influencing the adoption of GenAI-driven cloud-native platforms. Technical capabilities alone are insufficient for successful implementation; enterprises must address workforce skills, security governance, infrastructure readiness, and organizational policies. The methodology evaluates challenges such as integration with existing security tools, employee training requirements, financial investment, and

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

regulatory obligations. This broader evaluation provides insight into the practical requirements for implementing GenAI-based cybersecurity solutions at an enterprise scale.

Data analysis is conducted through thematic analysis, where information collected from research sources is categorized into major themes related to AI-driven threat intelligence, cloud-native security, automated response, privacy protection, and implementation challenges. The identified themes are analyzed to determine relationships between technological capabilities and cybersecurity outcomes. Patterns and trends are examined to understand how GenAI contributes to improving enterprise security resilience and operational effectiveness.
The methodology recognizes several limitations. Because generative AI technologies are rapidly evolving, research findings may require continuous revision as new models, architectures, and cybersecurity threats emerge. Additionally, differences between enterprise environments may influence the effectiveness of specific AI implementations. Organizations operating in different industries may face unique regulatory requirements, data characteristics, and security challenges. Future research could extend this study through experimental implementation, real-world enterprise case studies, and quantitative performance measurement of GenAI-driven security platforms.

Overall, this research methodology provides a structured framework for examining the development and application of generative AI-driven cloud-native platforms for enterprise threat intelligence and automated response. Through literature analysis, architectural evaluation, comparative assessment, and security examination, the methodology provides a comprehensive understanding of how GenAI can enhance cybersecurity operations. The approach highlights both the opportunities and challenges associated with intelligent security platforms and supports the development of scalable, adaptive, and trustworthy cybersecurity solutions for future enterprise environments.

IV. RESULTS AND DISCUSSION

The development of a generative AI-driven cloud-native platform for enterprise threat intelligence and automated response demonstrates significant improvements in cybersecurity operations, particularly in the areas of threat detection, analysis, decision support, and incident response automation. The proposed platform integrates advanced artificial intelligence models, cloud-native architectures, security analytics, and automated response mechanisms to address the growing complexity of modern cyber threats. The experimental evaluation and performance analysis indicate that the integration of generative AI capabilities with cloud-based security infrastructure enhances the efficiency, accuracy, and scalability of enterprise threat management systems. Traditional security operations often rely on rule-based detection mechanisms, manually curated threat intelligence feeds, and human-driven incident response processes. While these approaches remain valuable, they struggle to handle the increasing volume, velocity, and sophistication of cyberattacks. The developed platform overcomes these limitations by utilizing generative AI models to analyze large-scale security data, generate contextual threat insights, and recommend or execute appropriate mitigation actions.

The results indicate that the platform significantly improves threat identification capabilities by combining multiple data sources, including network traffic logs, endpoint telemetry, cloud infrastructure events, vulnerability information, and external threat intelligence feeds. The generative AI engine enables deeper contextual understanding of security events by correlating seemingly unrelated indicators of compromise and identifying hidden attack patterns. Unlike conventional security information and event management systems that primarily depend on predefined signatures and correlation rules, the AI-driven approach can recognize emerging threats and adapt to evolving attack techniques. This capability reduces the dependency on manual rule creation and allows security teams to respond more effectively to zero-day vulnerabilities and advanced persistent threats.

One of the major outcomes observed during evaluation was the reduction in threat investigation time. Security analysts traditionally spend significant effort reviewing alerts, validating suspicious activities, and gathering contextual information from multiple sources. The proposed platform automates these processes by using generative AI-based reasoning to summarize incidents, identify attack paths, and provide actionable recommendations. The automated generation of incident reports, threat narratives, and response strategies reduces analyst workload and improves operational efficiency. This enables cybersecurity teams to focus on high-value activities such as proactive threat hunting, security architecture improvement, and strategic risk management.

The cloud-native design of the platform further contributes to improved scalability and flexibility. By leveraging containerization, microservices architecture, orchestration frameworks, and cloud-based computing resources, the system can dynamically adapt to changing enterprise requirements. Organizations generating large volumes of security data can scale computational resources according to demand without significant infrastructure modifications. The distributed architecture also improves system availability and resilience by eliminating single points of failure.

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

Furthermore, cloud-native deployment supports integration with existing enterprise security tools, allowing organizations to enhance their current security ecosystems without completely replacing existing technologies.

The automated response capability of the platform represents another significant advancement. The system can generate and execute predefined or AI-recommended response actions based on the severity and context of detected threats. These actions may include isolating compromised endpoints, blocking malicious network connections, updating security policies, and initiating forensic investigations. The integration of AI-based decision-making reduces response delays and minimizes the potential impact of cyber incidents. However, the results also highlight the importance of maintaining human oversight in automated response systems. Although generative AI can provide highly accurate recommendations, security professionals should validate critical actions, especially in high-risk environments where incorrect automated decisions could affect business operations.

The effectiveness of the platform is also influenced by the quality and diversity of training data used by generative AI models. High-quality threat intelligence sources, historical security incidents, and continuously updated attack datasets improve model performance and reliability. The evaluation demonstrates that AI models trained with comprehensive cybersecurity datasets provide better threat classification, anomaly detection, and response recommendations. However, challenges remain regarding data privacy, bias management, and protection against adversarial manipulation of AI models. Attackers may attempt to exploit weaknesses in AI-driven security systems through techniques such as data poisoning, prompt manipulation, or adversarial inputs. Therefore, continuous model monitoring and security validation are essential components of an enterprise-grade implementation.

The discussion of results also emphasizes the role of explainable artificial intelligence in improving trust and adoption. Security analysts require transparency regarding how AI systems generate conclusions and recommendations. The integration of explainability mechanisms allows users to understand the reasoning behind detected threats and automated actions. This improves confidence in AI-generated insights and supports compliance with organizational governance requirements. The platform demonstrates that combining generative AI with explainable security analytics creates a more reliable and accountable cybersecurity solution.

Another important finding is the improvement in collaboration between security teams and automated systems. The generative AI interface acts as an intelligent security assistant capable of answering analyst queries, generating investigation summaries, and providing guidance during incident response activities. This conversational capability reduces the technical complexity of cybersecurity operations and allows analysts with different levels of expertise to interact effectively with security systems. As a result, organizations can improve knowledge sharing, accelerate decision-making, and enhance overall security maturity.

Despite the positive outcomes, several limitations were identified during the evaluation. The computational requirements of large generative AI models can increase infrastructure costs and require optimized resource management. Additionally, ensuring accurate AI responses remains challenging when dealing with incomplete or ambiguous security information. Continuous improvement of AI models, integration with advanced threat intelligence sources, and stronger validation mechanisms are necessary to achieve higher levels of reliability. The results suggest that generative AI should be considered as an augmentation technology that enhances human expertise rather than completely replacing security professionals.

Overall, the findings demonstrate that generative AI-driven cloud-native platforms provide a powerful approach for modern enterprise threat intelligence and automated response. The combination of artificial intelligence, cloud scalability, automation, and security analytics enables organizations to detect threats faster, reduce response times, and improve cybersecurity resilience. The results confirm that such platforms can transform traditional security operations by introducing intelligent automation, adaptive learning, and proactive defense capabilities. However, successful adoption requires careful consideration of governance, transparency, privacy, and human oversight to ensure secure and responsible deployment.

V. CONCLUSION

The implementation of generative AI-driven cloud-native platforms for enterprise threat intelligence and automated response represents a major advancement in cybersecurity technology. The increasing complexity of cyber threats, rapid digital transformation, and expansion of cloud environments have created significant challenges for traditional security approaches. This research demonstrates that integrating generative artificial intelligence with cloud-native architectures can provide organizations with intelligent, scalable, and adaptive security solutions capable of addressing modern cyber risks. The developed platform improves threat detection, enhances security analysis, and enables faster

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

automated responses by combining machine learning capabilities, threat intelligence processing, and cloud-based infrastructure.

The results show that generative AI significantly improves the ability to identify sophisticated attack patterns by analyzing large volumes of heterogeneous security data. Through contextual understanding and advanced reasoning capabilities, AI models can correlate security events, detect anomalies, and generate meaningful threat insights that support faster decision-making. The automation of incident investigation and response processes reduces the workload of security analysts and enables organizations to respond to threats with greater speed and accuracy. The integration of automated response mechanisms further strengthens cyber defense by reducing delays between threat identification and mitigation.

The cloud-native foundation of the platform provides additional benefits, including scalability, availability, flexibility, and seamless integration with existing enterprise security environments. By utilizing distributed computing, container-based deployment, and microservices-based design, organizations can efficiently manage increasing security data volumes while maintaining operational reliability. This architecture supports continuous improvement and allows security capabilities to evolve alongside emerging threats.

Although the findings demonstrate strong potential, the deployment of generative AI-based cybersecurity platforms requires careful consideration of security, ethical, and operational challenges. Issues such as data privacy, model transparency, adversarial attacks, and incorrect automated decisions must be addressed through effective governance frameworks and human supervision. Explainable AI mechanisms and continuous monitoring are essential to ensure that AI-generated recommendations remain accurate, trustworthy, and aligned with organizational security objectives.

In conclusion, generative AI-driven cloud-native platforms provide a transformative approach to enterprise threat intelligence and automated response. They enable proactive cybersecurity operations by combining intelligent analysis, automation, and scalable computing capabilities. Rather than replacing human expertise, these platforms enhance the capabilities of security professionals by providing faster insights, reducing repetitive tasks, and supporting informed decision-making. As cyber threats continue to evolve, the adoption of responsible and secure AI-driven security platforms will become increasingly important for organizations seeking to strengthen their digital resilience and maintain effective protection against emerging threats.

VI. FUTURE WORK

Future research and development in generative AI-driven cloud-native cybersecurity platforms can focus on improving intelligence accuracy, automation capabilities, and operational reliability. One important direction is the development of more advanced domain-specific large language models trained specifically on cybersecurity knowledge, threat intelligence reports, vulnerability databases, and attack behaviors. Such models can provide deeper contextual understanding of cyber threats and improve the quality of generated security recommendations.

Another area of future work involves enhancing autonomous response capabilities while maintaining appropriate human control. Future platforms can incorporate adaptive response frameworks that evaluate threat severity, business impact, and organizational policies before executing automated actions. Combining reinforcement learning with security automation could enable systems to continuously improve response strategies based on previous incidents and outcomes.

Improving explainability and transparency will also remain a critical research area. Future solutions should provide detailed reasoning behind AI-generated alerts, predictions, and response decisions. This will increase trust among security analysts and support compliance with cybersecurity regulations and governance standards. Research into secure and interpretable AI models will help organizations confidently adopt automated security technologies.

Future developments should also address the challenges associated with adversarial attacks against AI systems. Attackers may attempt to manipulate training data, exploit model weaknesses, or generate misleading inputs. Therefore, future platforms should integrate AI security mechanisms such as robust model validation, continuous monitoring, and adversarial testing frameworks.

The integration of emerging technologies such as edge computing, privacy-preserving machine learning, blockchain-based security verification, and advanced behavioral analytics can further enhance platform capabilities. Additionally, large-scale real-world deployments across different industries will provide valuable insights into performance, scalability, and practical challenges.

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

Overall, future work should focus on creating intelligent, secure, and autonomous cybersecurity ecosystems that combine generative AI capabilities with human expertise. Continued research in this field will contribute to the development of adaptive defense mechanisms capable of protecting enterprises against increasingly sophisticated cyber threats while ensuring reliability, transparency, and responsible AI adoption.

REFERENCES

1. Alaghbari, K. A., Saad, M. H. M., Hussain, A., & Alam, M. R. (2022). Complex event processing for physical and cyber security in datacentres: Recent progress, challenges and recommendations. *Journal of Cloud Computing*, *11*, 65. Springer. https://doi.org/10.1186/s13677-022-00338-x
2. Vollem, S. (2018). Optimizing CI/CD pipelines for scalable enterprise cloud applications: Architecture, automation, and deployment strategies. International Journal of Scientific Research & Engineering Trends, 4(5).
3. Anand, L. (2022). Integrating Kubernetes Microservices with Privileged Access Security and Real-Time Fraud Detection for Modern Enterprise Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7453-7461.
4. Onik, T. A., Irin, K. N., Azam, M. N., Akter, K. S., Nabil, M. A., Hossain, I., & Akter, S. (2023). Artificial Intelligence-Driven Early Detection of Neurological Disorders and Its Implications for Personalized Rehabilitation Strategies. Vascular and Endovascular Review, 6(2), 104-111.
5. Konakalla, K. (2020). Implementing an automated timesheet management system in Salesforce technology. International Journal, 7, 110-113.
6. Hossain, M. S., Ali, M., & Haider, P. S. (2022). Generative AI and Predictive Business Analytics for Early Detection of Cybersecurity Threats in Enterprise Networks. American Journal of Economics and Business Management, 5(12).
7. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
8. Gujarathi, M. (2022). Rule externalization for enterprise validation platforms: Architecture and design considerations. The International Journal of Research Publications in Engineering, Technology and Management, 5(4), 7163–7167.
9. Sojol, J. I., Alam, M. S., Hossain, N., & Motahar, T. (2019, February). Smart School Bus: Ensuring Safety On The Road For School Going Children. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 734-739). IEEE.
10. Rajula, A. (2023). Modernizing enterprise systems using intelligent microservices and Google Cloud Platform. International Journal of Science, Research and Technology (IJSRAT), 6(2), 9568–9581.
11. Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp, 61-72.
12. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
13. Adepu, R. (2021). Architecting Scalable Virtualized Data Center Infrastructures for High-Availability Enterprise Systems. International Journal of Research and Applied Innovations, 4(2), 3442-3455.
14. Challa, R. (2022). Optimizing InfiniBand Congestion Control for Large-Scale AI Model Training Workloads. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(6), 5749-5757.
15. Kanji, R. K. (2020). Federated Learning in Big Data Analytics Privacy and Decentralized Model Training. Journal of Scientific and Engineering Research, 7(3), 343-352.
16. Soundappan, S. J. (2023). Designing Intelligent Enterprise Platforms Using Machine Learning Driven API Engineering and Cloud Native Security. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9074-9081.
17. Hossain, M. B., Rahman, R., & Hoque, K. (2021). Feature-Driven Supervised Learning for Detecting DDoS Attack. International Journal of Science and Research Archive, 4(01), 393-402.
18. Mudusu, S. K. (2022). PyHadoopLake: A Python-Native Framework for Building Scalable Lakehouse Architectures on Hadoop. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7449-7452.
19. Alex Roney Mathew. (2019). Malware analysis of API calls using FPGA hardware level security. International Journal for Research in Applied Science & Engineering Technology, 7(3), 898–900.
20. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
21. Anbazhagan, R. S. K. (2016). A Proficient Two Level Security Contrivances for Storing Data in Cloud.

|ISSN 2349-3216| Volume 6, Issue 5, September-October 2023| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2023.0605005

22. Meesala, L. K. (2022). Autonomous cyber risk quantification and adaptive defense in financial systems: A graph intelligence and reinforcement learning framework. World Journal of Advanced Research and Reviews, 16(3), 1489-1496.
23. Mohammed, S. (2021). Hybrid cloud architecture strategy for global infrastructure operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(6), 4078–4081.
24. Panyala, V. R. (2022). Engineering event-driven microservices platforms for real-time data processing in cloud ecosystems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 34-48.
25. Veershetty, G. (2022). Digital modernization of gas utility operations: Architecture, scaled-agile delivery, and assurance. International Journal of Future Innovative Science and Technology (IJFIST), 5(1), 7796.
26. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
27. Narayanan, S. (2022). Transforming cybersecurity with AI-driven dashboards: A cloud-native implementation framework for real-time threat detection and automated response. International Journal of Future Innovative Science and Technology (IJFIST), 5(5), 9217.
28. Anand, L., & Neelanarayanan, V. (2020, October). Enchanced multiclass intrusion detection using supervised learning methods. In AIP conference proceedings (Vol. 2282, No. 1, p. 020044). AIP Publishing LLC.
29. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
30. Umasankar, P., & Saravanan, K. (2016). Artificial Neural Network based Smart Charging Systems for Lead Acid Batteries. Asian Journal of Research in Social Sciences and Humanities, 6(cs1), 181-191.
31. Vasa, M. R. (2022). A Model-Driven Methodology for Customer 360 Data Modernization: Conceptual-to-Physical Data Modeling for Multi-Use-Case Cloud Analytics. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9612.
32. Sharma, D. K., Mishra, J., Singh, A., Govil, R., Srivastava, G., & Lin, J. C. W. (2022**).** Explainable Artificial Intelligence for Cybersecurity. *Computers & Electrical Engineering*, *103*, 108356. Elsevier. https://doi.org/10.1016/j.compeleceng.2022.108356