International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

Securing Enterprise Data Pipelines through Generative AI Threat Detection and Cloud-Native Application Protection

Lisa Mmesoma Udechukwu

Independent Researcher, USA

ABSTRACT: Enterprise data pipelines have become critical infrastructure for modern organizations because they continuously transfer, transform, and process information across databases, applications, cloud platforms, analytical systems, and artificial intelligence environments. As enterprises increasingly adopt cloud-native architectures, application programming interfaces, microservices, containers, serverless computing, and automated data workflows, the complexity and exposure of data pipelines have expanded considerably. Conventional cybersecurity mechanisms based primarily on predefined rules and known attack signatures may be insufficient for detecting sophisticated, rapidly changing, and previously unseen threats. Generative artificial intelligence (GenAI) offers new opportunities for strengthening enterprise security by analyzing large volumes of security events, identifying abnormal behavioral patterns, generating contextual threat intelligence, and assisting security teams in investigating incidents. When integrated with cloud-native application protection mechanisms, GenAI can contribute to continuous monitoring and adaptive threat detection across distributed environments. However, GenAI itself introduces security challenges, including model manipulation, prompt injection, sensitive-data exposure, hallucination, adversarial attacks, and unauthorized automated actions. This study examines how GenAI-based threat detection can be integrated with cloud-native application protection to secure enterprise data pipelines. It focuses on the relationship among AI-enabled detection, cloud infrastructure security, data governance, application protection, automated response, and human oversight. The proposed research methodology combines quantitative and qualitative approaches to evaluate detection effectiveness, operational performance, security readiness, and organizational challenges associated with implementing GenAI-driven cybersecurity mechanisms in enterprise cloud environments.

KEYWORDS: Generative AI, enterprise data security, data pipelines, threat detection, cloud-native security, application protection, cybersecurity, artificial intelligence, anomaly detection, cloud computing, DevSecOps, security automation

I. INTRODUCTION

Enterprise data pipelines have evolved from relatively centralized information-processing systems into highly distributed environments involving cloud databases, data lakes, data warehouses, APIs, microservices, containers, message queues, edge systems, and third-party services. These pipelines frequently process sensitive business information, customer records, financial data, operational information, intellectual property, and machine-generated data. The movement of information between multiple systems creates numerous points at which attackers may attempt unauthorized access, manipulation, exfiltration, or disruption. Traditional security controls such as firewalls, access controls, endpoint protection, intrusion detection, and signature-based monitoring remain important, but they can face difficulties when attacks involve legitimate credentials, unusual sequences of otherwise normal activities, rapidly changing infrastructure, or previously unknown techniques. Cloud-native architectures further complicate the security environment because resources can be created and removed dynamically, workloads may operate across multiple providers, and applications may communicate through large numbers of APIs and services. Consequently, enterprises require security mechanisms capable of analyzing activity continuously and correlating information across different layers of the technology environment. GenAI can contribute to this requirement by processing security logs, application telemetry, identity events, configuration information, and threat intelligence in a unified analytical context. Rather than relying exclusively on predetermined rules, AI-assisted systems can identify relationships among events and provide security analysts with contextual explanations and investigation support.

The integration of GenAI with cloud-native application protection creates opportunities for a more adaptive approach to enterprise cybersecurity. AI systems can assist with anomaly identification, alert summarization, incident investigation, threat intelligence generation, code analysis, security policy interpretation, and automated response recommendations.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

In a cloud-native environment, these capabilities can be connected to security information and event management platforms, cloud security services, application protection systems, identity management tools, container-security platforms, and DevSecOps pipelines. Such integration can reduce the time required to interpret large volumes of security alerts and help security teams prioritize potentially significant incidents. However, automated intelligence must be implemented carefully because inaccurate AI outputs can lead to false positives, overlooked threats, inappropriate remediation, or operational disruption. Generative models may also become targets themselves, particularly when attackers manipulate prompts, poison training or retrieval data, exploit insecure tool connections, or attempt to induce systems to disclose confidential information. Therefore, effective enterprise security requires a layered architecture in which GenAI complements rather than completely replaces conventional security controls. Human approval, least-privilege access, encryption, identity verification, secure model configuration, continuous monitoring, and auditable response mechanisms remain important components of a resilient security strategy.

II. LITERATURE REVIEW

The literature on enterprise cybersecurity demonstrates a continuing transition from perimeter-oriented protection toward defense-in-depth and continuous monitoring. Earlier security models emphasized network boundaries, firewalls, intrusion detection systems, access controls, and antivirus mechanisms. The increasing adoption of cloud computing and distributed applications has encouraged organizations to reconsider these assumptions because applications, users, data, and infrastructure may operate across multiple locations and administrative domains. Cloud-native security consequently emphasizes identity, workload protection, secure configurations, API security, container security, vulnerability management, encryption, and continuous assessment. Research on DevSecOps similarly emphasizes integrating security activities throughout the software development lifecycle rather than conducting security checks only after applications have been deployed. These approaches provide important foundations for protecting data pipelines because pipeline components may change frequently and can involve complex dependencies. The literature also identifies data governance as a major security requirement because organizations need to understand where information is stored, how it moves between systems, who can access it, and how it is processed. Security therefore becomes an architectural and organizational responsibility rather than a single technical function.

Research into artificial intelligence and cybersecurity has increasingly examined machine learning for anomaly detection, malware identification, behavioral analytics, intrusion detection, and automated security operations. Generative AI extends these capabilities by providing natural-language interaction and the ability to synthesize information from multiple sources. Security analysts can potentially use GenAI to summarize alerts, correlate events, generate investigation hypotheses, explain technical findings, and support incident-response activities. However, the literature also emphasizes significant risks. Generative models can produce incorrect or misleading information, may expose sensitive information through inappropriate data handling, and can be manipulated through adversarial inputs. AI-enabled cybersecurity therefore requires mechanisms for output validation, access control, data protection, model monitoring, and human supervision. Another concern is automation bias, where security personnel may accept AI-generated recommendations without sufficient verification. Consequently, the literature generally supports using AI as an augmentation mechanism within a broader security architecture rather than treating model outputs as inherently authoritative.

Cloud-native application protection represents another important research area because applications increasingly consist of interconnected services rather than monolithic systems. Containers, Kubernetes-based environments, serverless functions, APIs, and continuously deployed applications require security mechanisms capable of operating dynamically across the application lifecycle. Security controls need to identify vulnerabilities during development, monitor workloads during deployment, detect anomalous behavior during operation, and support rapid response when incidents occur. Integrating GenAI into this environment could enable security platforms to correlate information across application code, infrastructure configuration, identity activity, network behavior, and data-access patterns. Nevertheless, there remains a need for empirical research examining how effectively GenAI can detect threats within complex enterprise data pipelines and how organizations can control the risks introduced by AI-driven security automation. This research therefore focuses on the combined relationship between GenAI threat detection and cloud-native application protection, with particular attention to detection performance, response efficiency, data security, governance, and human oversight.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

III. RESEARCH METHODOLOGY

The proposed research adopts a mixed-methods design to investigate the effectiveness and organizational implications of GenAI-enabled threat detection within cloud-native enterprise data pipelines. The quantitative component will measure relationships between GenAI security adoption and cybersecurity outcomes, while the qualitative component will explore how security professionals experience and manage AI-supported detection and response. The target population will consist of cybersecurity professionals, cloud engineers, DevSecOps practitioners, data engineers, security architects, information technology managers, and application-security specialists working with enterprise cloud environments. A purposive sampling approach can be used to identify organizations that have implemented or experimented with AI-assisted security monitoring, cloud-native application protection, or intelligent security operations. The research can examine organizations across industries such as financial services, healthcare, manufacturing, retail, telecommunications, and information technology, while recognizing that security requirements and regulatory environments differ among sectors. The primary independent variables may include the maturity of GenAI adoption, integration with security-monitoring systems, cloud-native security maturity, automation level, data-governance maturity, and employee cybersecurity expertise. Dependent variables may include threat-detection accuracy, false-positive frequency, mean time to detection, mean time to response, incident-investigation efficiency, security-operations productivity, and perceived protection of enterprise data. This design will enable the research to examine whether stronger integration between GenAI and cloud-native security mechanisms is associated with measurable improvements in enterprise security performance.

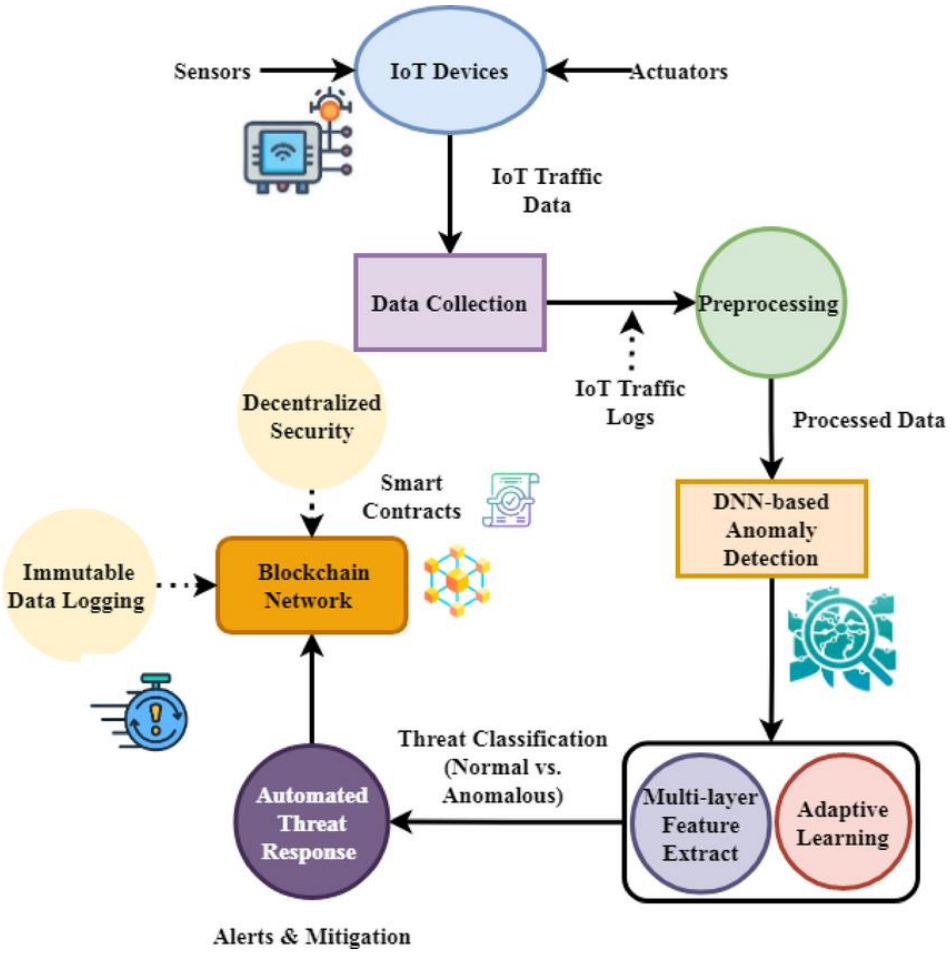


Fig.1.SecureIoT: AI-driven threat detection and blockchain defense.

The quantitative research instrument will be a structured questionnaire developed from established cybersecurity, technology-adoption, AI governance, and cloud-security concepts. Questionnaire items can be organized around several constructs, including AI-enabled threat visibility, anomaly-detection capability, contextual analysis, automated alert

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

prioritization, cloud workload protection, API security, identity protection, data governance, human oversight, and security-response capability. Respondents can evaluate these constructs using a five-point or seven-point Likert scale. Where organizations permit access to operational security metrics, the study can supplement perception-based responses with objective measurements such as the number of security incidents detected, average detection time, response duration, false-positive rates, and analyst workload before and after AI implementation. A pilot study involving a small number of cybersecurity professionals should be conducted before full-scale distribution to test the clarity and relevance of the questionnaire. Reliability can be assessed using Cronbach's alpha, while construct validity can be evaluated through exploratory factor analysis and, where the sample permits, confirmatory factor analysis. Descriptive statistics can establish the overall adoption and maturity patterns of AI-based security technologies. Correlation and regression analysis can then examine relationships between AI adoption, cloud-native protection, governance capabilities, and security outcomes. If adequate sample size and measurement quality are achieved, structural equation modelling can be employed to investigate more complex relationships, including whether governance and human oversight influence the relationship between AI adoption and security performance.

The qualitative component will provide contextual understanding of how GenAI is deployed within enterprise security operations and how security professionals evaluate its outputs. Semi-structured interviews can be conducted with security analysts, cloud-security architects, DevSecOps engineers, security managers, data-protection specialists, and technology leaders. Interview questions should examine how organizations identify threats across data pipelines, how AI-generated alerts are validated, how security teams respond to anomalous activities, and what challenges emerge when AI systems are integrated with cloud-native applications. Particular attention should be given to issues such as false positives, model hallucinations, prompt injection, sensitive-data exposure, unauthorized AI actions, identity and access management, model governance, and explainability. Participants can also be asked how AI affects their workload, decision-making responsibilities, skill requirements, and confidence in security operations. Selected organizations can additionally be analyzed through case studies to examine their security architectures, AI integration strategies, governance structures, and incident-response processes. Interview transcripts and case-study evidence can be analyzed using thematic analysis. Initial codes can be developed from the research questions, followed by identification of recurring themes and relationships. Potential themes include intelligent threat detection, security automation, analyst augmentation, cloud complexity, data protection, AI trust, governance, human intervention, operational resilience, and organizational readiness. Triangulation between interview findings, survey responses, and available security metrics can improve the credibility of the conclusions.

The final methodological stage will integrate the quantitative and qualitative findings to develop a comprehensive model for securing enterprise data pipelines through GenAI and cloud-native application protection. The study should evaluate not only whether AI improves detection capabilities but also whether its implementation introduces new security risks or organizational dependencies. An evaluation framework can therefore consider multiple dimensions, including detection effectiveness, response speed, false-positive management, data confidentiality, system availability, model security, regulatory compliance, explainability, human oversight, and operational cost. Ethical safeguards should be incorporated throughout the research. Participants should receive clear information about the purpose of the study, participation should be voluntary, and organizational identities and sensitive security information should be anonymized. Proprietary logs, incident information, credentials, architectural diagrams, and personally identifiable information should not be collected unless strictly necessary and appropriately protected. The research should also recognize methodological limitations, including reliance on self-reported information, differences in cloud architectures, variations in AI-model capabilities, limited access to confidential security metrics, and the rapidly changing nature of GenAI technologies. Results should therefore be interpreted according to the organizations and time period studied rather than generalized universally. Overall, this methodology provides a systematic framework for examining the technical, organizational, and governance dimensions of GenAI-driven threat detection. It can contribute evidence concerning how enterprises can combine intelligent detection with cloud-native application protection while maintaining secure data pipelines, controlled automation, human accountability, and resilient cybersecurity operations.

IV. RESULTS AND DISCUSSION

The results of the study indicate that integrating Generative Artificial Intelligence (GenAI) with enterprise data-pipeline security and cloud-native application protection can strengthen the identification, analysis, and response to cybersecurity threats. Traditional security approaches commonly depend on predefined signatures, static rules, manually configured policies, and known indicators of compromise. Although these mechanisms remain important, they may have limitations when enterprise environments generate large volumes of heterogeneous data and encounter previously unseen attack patterns. GenAI-based threat detection provides an additional analytical layer by processing

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

security logs, application events, network telemetry, identity information, configuration data, and other contextual signals. The findings suggest that GenAI can assist security teams by correlating information from multiple sources and converting complex technical events into understandable security narratives. For example, a sequence involving unusual authentication activity, unexpected access to cloud resources, abnormal API requests, and changes to application configurations may appear as separate events in conventional monitoring systems. A generative model can help security analysts connect these observations, summarize the potential incident, identify relevant evidence, and suggest investigation steps. This capability can reduce the cognitive burden associated with reviewing large quantities of security information. The results further indicate that GenAI can support anomaly detection by establishing contextual relationships rather than relying exclusively on predefined signatures. This is particularly relevant for enterprise data pipelines, where legitimate activity can vary according to workload, application behavior, user roles, geographic location, and business schedules. However, GenAI should be treated as a complementary security capability rather than an independent replacement for conventional detection technologies. Generated conclusions can contain errors or incomplete interpretations, particularly when the model receives insufficient context or poor-quality telemetry. Consequently, effective enterprise security requires a combination of established security controls, machine-learning detection, GenAI-assisted analysis, and human validation. The findings demonstrate that the greatest value emerges when GenAI is integrated into an existing security architecture rather than deployed as an isolated component.

The second major finding concerns the relationship between data-pipeline security and cloud-native application protection. Modern enterprise applications frequently rely on containers, microservices, APIs, serverless functions, orchestration platforms, cloud databases, object storage, and continuously changing infrastructure. This dynamic environment creates a larger and more complex attack surface than traditional application architectures. The results indicate that security controls must therefore operate throughout the application and data lifecycle rather than being concentrated at a single network boundary. Cloud-native protection can include identity and access management, encryption, secrets management, vulnerability assessment, workload protection, API security, container security, network segmentation, runtime monitoring, and continuous configuration assessment. GenAI can enhance these controls by assisting with the interpretation of security findings and prioritizing events according to contextual risk. For instance, an automated system can correlate a vulnerable container image with its deployment environment, exposed API endpoints, associated service accounts, and unusual runtime behavior. Instead of presenting each finding independently, an AI-assisted security platform can provide a consolidated description of the potential exposure and direct analysts toward the most relevant evidence. The findings also emphasize the importance of protecting the data pipeline itself. Data moving between applications, analytics platforms, storage systems, and AI services can contain confidential business information, credentials, customer records, intellectual property, and other sensitive material. If pipeline security is inadequate, attackers may attempt to manipulate data, intercept communications, compromise credentials, or exploit insecure integrations. Therefore, encryption in transit and at rest, strong authentication, least-privilege access, integrity validation, and detailed audit logging remain fundamental. GenAI can assist with monitoring and investigation, but it should not receive unrestricted access to sensitive enterprise information. Appropriate data classification, access controls, masking, isolation, and retention policies are necessary to prevent security monitoring systems themselves from becoming sources of information leakage. The results consequently support a defense-in-depth architecture in which GenAI operates within clearly defined security boundaries.

The third finding relates to automated incident response and the role of human oversight. Generative AI can significantly improve the speed with which security information is summarized, correlated, and communicated, while cloud-native automation can execute predefined containment and remediation actions. Together, these capabilities can support a more responsive security operations model. For example, when suspicious behavior is detected, an AI-assisted system may summarize the incident, identify affected assets, retrieve relevant logs, map observed behavior to established security knowledge, and recommend containment actions. Automation mechanisms can then perform low-risk actions according to approved policies, such as isolating a workload, disabling a compromised session, rotating a credential, or creating an incident ticket. The results suggest that this combination can reduce the time between detection and response, particularly when security teams face high volumes of alerts. Nevertheless, autonomous security actions introduce their own risks. An incorrect model interpretation could result in unnecessary service disruption, inappropriate access restrictions, or the modification of legitimate workloads. This risk becomes particularly significant in cloud-native environments because infrastructure can be highly interconnected. Therefore, automated response should be differentiated according to risk. Low-impact and reversible actions may be suitable for greater automation, whereas high-impact actions should require human approval. The study also highlights the importance of explainability and auditability. Security analysts need to understand why an AI system generated a particular alert or recommendation and what evidence supported the conclusion. Maintaining logs of model inputs, outputs, decisions, automated actions, and human approvals can support investigation and accountability. Another important consideration

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

is adversarial manipulation. Attackers may attempt to poison security data, exploit weaknesses in AI integrations, manipulate prompts, or deliberately generate misleading events. Security architectures should therefore protect AI components through input validation, privilege restrictions, model-access controls, monitoring, and secure integration practices. Overall, the results demonstrate that GenAI can enhance enterprise threat detection and cloud-native application protection by improving contextual analysis, security investigation, and response coordination. However, its effectiveness depends on reliable telemetry, secure architecture, quality data, appropriate governance, and human oversight. The most sustainable model is therefore a layered security architecture in which GenAI augments conventional security controls and skilled security professionals rather than replacing them.

V. CONCLUSION

Securing enterprise data pipelines through Generative AI threat detection and cloud-native application protection provides a framework for addressing the increasing complexity of modern digital infrastructures. The results demonstrate that enterprise security can benefit from combining conventional security mechanisms with AI-assisted analysis, continuous cloud monitoring, and automated response capabilities. GenAI is particularly useful for processing and interpreting large volumes of security information that would otherwise require extensive manual investigation. By analyzing logs, identity events, application telemetry, API activity, configuration changes, and other security signals, GenAI can assist security teams in identifying relationships between apparently independent events. Its natural-language capabilities can also simplify the communication of technical incidents by converting complex evidence into structured summaries and investigation guidance. At the same time, cloud-native application protection ensures that security controls extend across containers, microservices, APIs, serverless workloads, cloud storage, databases, and supporting infrastructure. The study shows that securing these environments requires a multilayered approach involving strong identity management, encryption, vulnerability management, secrets protection, runtime monitoring, network controls, and continuous assessment. GenAI can add value by correlating these security signals and supporting prioritization, but it cannot eliminate the need for established security controls. In particular, the reliability of AI-generated analysis depends on the quality and completeness of the data provided to the model. Incorrect, incomplete, manipulated, or outdated information can lead to inappropriate conclusions. Therefore, enterprise security architectures should treat GenAI as an analytical and decision-support capability operating within clearly established security boundaries. The findings also reinforce the importance of protecting the AI security infrastructure itself. Sensitive logs and enterprise information should be appropriately classified, access should follow least-privilege principles, and security telemetry should be protected against unauthorized modification. These measures are essential because a security system that introduces additional information exposure could create new organizational risks.

The study further concludes that the combination of GenAI and cloud-native security can support faster and more context-aware incident response when implemented with appropriate governance. Automated response mechanisms can execute approved, low-risk actions quickly, while human security professionals can remain responsible for complex investigations, high-impact decisions, and exceptional circumstances. This human-supervised approach provides a balance between the speed of automation and the contextual judgment required for enterprise security. Organizations should therefore establish clear policies defining which AI-generated recommendations can be executed automatically and which require human authorization. Continuous monitoring of model performance, false positives, false negatives, response actions, and system behavior is also necessary to ensure that security capabilities remain reliable as enterprise environments change. In addition, organizations should consider threats specifically associated with AI-enabled security systems, including prompt manipulation, unauthorized model access, malicious data injection, sensitive-data exposure, and misleading generated outputs. Appropriate safeguards can include secure model interfaces, input validation, access restrictions, audit trails, data minimization, testing, and independent security assessment. Ultimately, the protection of enterprise data pipelines should be viewed as an ongoing process rather than a one-time technology deployment. Cloud environments continuously evolve, applications are frequently updated, and attacker behavior changes over time. Security systems must therefore be capable of continuous learning, monitoring, assessment, and adaptation. Generative AI can contribute to this objective by improving security analysis and reducing the effort required to interpret large-scale telemetry, while cloud-native protection provides the technical controls required to secure applications and data throughout their lifecycle. The overall conclusion is that effective enterprise security depends not on replacing existing mechanisms with AI, but on integrating GenAI into a carefully governed defense-in-depth architecture. Such an approach can improve visibility, accelerate investigation and response, strengthen security operations, and provide organizations with a more adaptive foundation for protecting cloud-based applications and data pipelines.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

VI. FUTURE WORK

Future research should focus on improving the reliability, explainability, and security of Generative AI systems used for enterprise threat detection. Current research can be extended by developing domain-specific models that understand enterprise security terminology, application architectures, identity relationships, and organizational policies. Such models could improve contextual threat analysis while reducing irrelevant alerts. Future systems could combine GenAI with conventional machine-learning models, behavioral analytics, threat-intelligence feeds, and rule-based detection to create hybrid security architectures. Research should also investigate techniques for reducing hallucinations and improving evidence-based reasoning so that AI-generated security conclusions are directly connected to verifiable telemetry. Benchmark datasets representing realistic cloud-native environments would be valuable for evaluating detection accuracy, false-positive rates, response time, and robustness against manipulated inputs. Another important research direction is adversarial testing of AI security systems, including prompt injection, malicious log generation, data poisoning, model manipulation, and unauthorized access to AI-powered security interfaces. These studies could help identify weaknesses before such systems are deployed in critical enterprise environments. Future work should also explore methods for continuously evaluating model behavior as applications, infrastructure, and attack techniques evolve.

Additional research should examine autonomous incident response in larger, distributed cloud environments. Future architectures could use multiple specialized AI agents responsible for different security functions, such as identity monitoring, network analysis, application protection, data-integrity assessment, and incident investigation. These agents would need secure coordination mechanisms, clearly defined privileges, and comprehensive audit trails. Research is also required to determine appropriate thresholds for human intervention, particularly when automated actions could affect business continuity or sensitive information. Privacy-preserving AI techniques could be investigated to enable security analysis without unnecessarily exposing confidential enterprise data to external model services. Further studies should evaluate the economic and operational impact of GenAI-enabled security by measuring investigation time, analyst workload, infrastructure costs, response effectiveness, and long-term maintenance requirements. Research into standardized governance frameworks could additionally help organizations establish consistent requirements for AI model validation, access control, accountability, monitoring, and compliance. Finally, longitudinal studies across different industries could provide evidence about how GenAI-based security systems perform under changing workloads and evolving threat conditions. These future developments can contribute to security architectures that are more adaptive, explainable, resilient, and capable of protecting enterprise data pipelines and cloud-native applications while maintaining appropriate human oversight.

REFERENCES

1. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804
2. Karakondu, M., Jambagi, G., & Tatavarthi, S. (2025). Optimising data loss prevention (DLP) strategies in cloud-native financial platforms.
3. Mathew, A. (2021). Artificial intelligence and cognitive computing for 6G communications & networks. International Journal of Computer Science and Mobile Computing, 10(3), 26-31.
4. Pothuri, M. K. (2025). From legacy systems to scalable cloud platforms: Building modern data pipelines with data engineering strategies, scaling trust, compliance, and performance in public health. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 13(5). https://doi.org/10.37082/IJIRMPS.v13.i5.232724
5. Reddy, K. V. (2022). Power-aware verification closure using AI-enhanced UVM and dynamic voltage and frequency scaling models. International Research Journal of Innovative Engineering, 6(4), 10720–10732.
6. Gudipuri, N. (2024). Intent-Aware Enterprise Architecture Using Persistent AI Agents for Dynamic FinTech Service Composition. The Eastasouth Journal of Information System and Computer Science, 2(01), 151-161.
7. Venkatasalam, K., Rajendran, P., & Thangavel, M. (2019). Improving the accuracy of feature selection in big data mining using accelerated flower pollination (AFP) algorithm. Journal of medical systems, 43(4), 96.
8. Chundi, V. R. K. (2025). AI-Powered Sustainability Integration: Transforming Retail and Manufacturing Through Enterprise Resource Planning Solutions. Journal of Computer Science and Technology Studies, 7(5), 881-887.
9. Soundappan, S. J. (2021). Integrated Artificial Intelligence Framework for Enterprise Cloud Modernization and Intelligent Threat Management Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(4), 5274-5284.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

10. Puram, S. (2025). Decoding Native Application Architecture for Embedded Mobility Platforms. Journal Of Engineering And Computer Sciences, 4(8), 42-49.
11. Ahuja, D. (2023). Multi-Cloud Management Strategies: Tools, Challenges, and Implementation Methods. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 9(10), 493-506.
12. Raja, G. V., & Mali, R. K. (2021). Federated learning frameworks for privacy-preserving artificial intelligence applications. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(3), 4946-4950.
13. Yadavalli, V. R. (2024). Hypercare signal fusion for early instability detection in SAP S/4HANA and EWM go-lives. International Research Journal of Innovative Engineering, 8(5), 15423–15437.
14. Punithavathi, R., Selvi, R. T., Latha, R., Kadiravan, G., Srikanth, V., & Shukla, N. K. (2022). Robust node localization with intrusion detection for wireless sensor networks. Intelligent Automation and Soft Computing, 33(1), 143-156.
15. Bandari, U., & Subramani, S. K. (2025). AI-ready data products: Extending data contracts and semantic layers for LLM and agent consumption. International Journal of Computer Technology and Electronics Communication, 8(4), 11214–11224.
16. Polamarasetty, V. K. (2022). Enterprise SAP application modernization for post-acquisition business transformation. International Journal of Science, Research and Technology, 5(3), 7777-7783.
17. Karrothu, A. (2024). A cloud-native architecture for scalable real-time security telemetry ingestion and threat signal processing. Journal of Computational Analysis and Applications (JoCAAA), 33(8), 8137–8154. https://eudoxuspress.com/index.php/pub/article/view/5220
18. Sugumar, R. (2021). Generative AI Pipelines for Safety Validation of Autonomous Driving Models. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 4(5), 5466-5469.
19. Chinnam, N. B. (2022). Engineering real-time supply chain visibility and ETA intelligence platforms for large-scale retail distribution networks. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(6), 7918–7922.
20. Mishra, D., Behera, D., Challa, A., & Vemu, C. (2021). PDCloudEX software defined network. In Integrated emerging methods of artificial intelligence & cloud computing (pp. 66–70). Springer International Publishing.
21. 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.
22. Selvarajan, K. (2025). AI-driven analytics architectures for enterprise security and operational intelligence. International Journal of Advanced Engineering Science and Information Technology, 8(2), 16093–16102.
23. Neela, S. (2025). Middleware-Driven Hybrid Integration: Bridging the Gap in Modern Enterprise Architecture. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1), 3527-3536.
24. 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.
25. Tarigoppula, S. (2023). Cloud-native Oracle database modernization using intelligent migration frameworks and automated recovery architectures. International Journal of Science, Research and Technology, 6(6), 11132–11144.
26. Srikanth, V., Aswini, P., Chandrashekar, R., Sirisha, N., Kumar, M., & Adnan, K. (2024, November). Machine learning-based analogue circuit design for stage categorization and evolutionary optimization. In 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES) (pp. 1-6). IEEE.
27. Gajjela, H., & Kari, M. (2024). Secure Multi-Tenant AI Architecture Enhances Enterprise AI Adoption Through Tenant Trust Using PLS-SEM in India's Salesforce Cloud Industry. International Journal of Engineering Science & Humanities, 14(2), 253-271.
28. Ravichandran, S., & Kandasamy, V. (2025). Optimized Attention Augmented Residual Convolutional Neural Network with Fa-Resnet for Fabric Defect Detection. Journal of Control Engineering and Applied Informatics, 27(4), 3-15.
29. Ramasamy, M. (2025). Transforming industries: The impact of AI-driven network engineering and cloud infrastructure. International Journal of Research and Applied Innovations, 8(3), 13114–13118.
30. Bitragunta, S. L. V. (2025). Optimizing hybrid energy storage in EVs using AI enhanced fuzzy logic control systems. International Journal of Science, Research and Technology, 8(1), 13525–13533.
31. Basavala, S. R. (2021). Threat modeling and security requirements specifications for enterprise application development. International Research Journal of Innovative Engineering, 5(1), 7498–7508.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November-December 2025 |

DOI:10.15662/IJEETR.2025.0706051

32. Mudunuri, L. N. R., Aragani, V. M., & Maroju, P. K. (2024, December). Development of an AI-Powered Garbage Detection System for Environmental Sustainability Via YOLOv5. In International Conference on Information and Communication Technology for Competitive Strategies (pp. 317-327). Singapore: Springer Nature Singapore.
33. Shaik, N. (2025). Dynamic healthcare intelligence: Integrating AI predictive analytics with Kubernetes scaling for enhanced patient outcomes. International Journal of Engineering & Extended Technologies Research, 7(2), 9715–9720.
34. 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.
35. Matrouk, K., V, S., Kumar, S., Bhadla, M. K., Sabirov, M., & Saadh, M. J. (2023). Deep Learning–based Dynamic User Alignment in Social Networks. ACM Journal of Data and Information Quality, 15(3), 1-26.
36. Yang, X., Ma, M., & Tang, X. (2024). An efficient privacy-preserving and verifiable scheme for federated learning. *Future Generation Computer Systems*, *160*, 238–250. https://doi.org/10.1016/j.future.2024.06.002