International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A Comparative Study Of Cyber Attack Prediction Using Machine Learning And Generative AI Technique

[1]Dr C Mohammed Gulzar,[2]Ambala Sunil Kumar Reddy,[3]Battula Likith Kumar,[4]Manjula Deekshith

[1]Associate Professor, Computer Science Of Engineering, Dr K V Subba Reddy Institute of Technology

[2,3,4]B. Tech Students, Computer Science Of Engineering, Dr K V Subba Reddy Institute of Technology

ABSTRACT

The proposed proactive cyber defense framework extends beyond traditional intrusion detection by emphasizing early-stage threat forecasting and adaptive risk mitigation. By continuously learning from historical attack data and real-time network behavior, the system identifies subtle anomalies and evolving attack indicators that typically go unnoticed by rule-based or signature-driven security tools. Advanced machine learning models—such as ensemble classifiers, deep neural networks, and temporal sequence models—are employed to capture both short-term deviations and long-term behavioral trends, enabling timely identification of potential attack vectors before full exploitation occurs. Generative Artificial Intelligence further strengthens the framework by enabling threat simulation and scenario generation. Using generative models, the system can synthesize realistic cyber-attack patterns, including zero-day exploits and polymorphic malware behaviors, based on partial or incomplete intelligence. These synthetic threat scenarios allow security teams to test system robustness, evaluate defense strategies, and improve preparedness without waiting for real-world attacks. This predictive simulation capability significantly reduces the response gap between threat emergence and mitigation. The integration of multi-source threat intelligence enhances the accuracy and reliability of cyber-attack prediction. Data from network traffic, endpoint activity, authentication logs, vulnerability repositories, and external threat feeds are fused into a unified analytical pipeline. Machine learning models correlate indicators across these heterogeneous data sources to uncover complex attack chains and lateral movement strategies. This holistic view enables early detection of coordinated and multi-stage cyber campaigns, including advanced persistent threats (APTs). Another critical aspect of the framework is its adaptive and self-improving defense mechanism. As new attack behaviors are detected or simulated, the system updates its learning models to reflect emerging threats. Automated policy adjustment and intelligent alert prioritization ensure that security operations teams focus on high-risk events, reducing alert fatigue and improving operational efficiency. Over time, this continuous learning process enhances the system's resilience against novel and AI-driven cybercrime techniques. Overall, the proposed ML and GenAI-based proactive cyber defense framework represents a shift from reactive security toward predictive and preventive cybersecurity. By forecasting attacks, simulating adversarial strategies, and enabling early intervention, the framework strengthens organizational cyber resilience, safeguards critical digital assets, and ensures uninterrupted system operations in an increasingly hostile cyber environment.

Keywords: Cyberattack prediction, cybersecurity analytics, machine learning, generative artificial intelligence, deep learning, intrusion detection systems (IDS), anomaly detection, threat intelligence, network security, cyber threat prediction, data-driven security, adversarial learning, predictive security modeling, automated threat detection, cyber defense systems.

I. INTRODUCTION

Cybersecurity has become a critical concern for governments, enterprises, and individuals due to the rapid expansion of cloud computing, Internet of Things (IoT) ecosystems, and remote digital services.

The increasing interconnectivity of systems has significantly widened the attack surface, making critical infrastructures, financial platforms, healthcare systems, and personal data more vulnerable than ever before. Attackers now exploit this complexity by launching highly coordinated, stealthy, and persistent attacks that can remain undetected for long periods, causing severe financial, operational, and reputational damage.

Modern cyber adversaries employ sophisticated techniques such as polymorphic malware, ransomware-as-a-service (RaaS), advanced phishing campaigns, social engineering, and AI-driven exploits. These attacks dynamically adapt their behavior to evade traditional defenses, often leveraging automation and machine intelligence to scale attacks across thousands of targets simultaneously. As a result, cyber threats are no longer isolated incidents but part of organized, intelligent, and economically motivated campaigns that continuously evolve.

Conventional intrusion detection and prevention systems primarily rely on signature-based or rule-based mechanisms, which are effective only against known threats. Such systems struggle to detect zero-day vulnerabilities, advanced persistent threats (APTs), and previously unseen attack patterns. Additionally, the increasing volume, velocity, and variety of security data generated by modern networks overwhelm traditional security tools, leading to high false-positive rates and delayed response times that reduce operational effectiveness. Advanced machine learning techniques offer a powerful alternative by enabling systems to automatically learn complex patterns and anomalies from large-scale security data, including network traffic, system logs, user behavior, and application activity. Supervised, unsupervised, and reinforcement learning models can identify subtle deviations from normal behavior that may indicate early stages of an attack. These data-driven approaches improve detection accuracy while reducing dependence on manually crafted rules and signatures. Generative Artificial Intelligence further enhances cyber defense by modeling attacker behavior and generating realistic synthetic attack scenarios. By simulating potential exploits, malware variants, and attack sequences, generative models enable security systems to anticipate emerging threats before they are observed in the real world. This capability supports robust training of defensive models, improves system resilience, and strengthens preparedness against unknown or rare attack vectors.

The integration of predictive machine learning with generative AI enables a paradigm shift from reactive security to proactive cyber defense. Instead of merely responding to incidents after damage has occurred, security systems can forecast potential attacks, assess risk levels in real time, and recommend preventive actions. This proactive approach allows organizations to implement adaptive security policies, dynamically allocate resources, and harden vulnerable components before exploitation. Furthermore, AI-driven automation plays a crucial role in accelerating incident response and remediation. Intelligent systems can automatically isolate compromised assets, block malicious traffic, and trigger recovery workflows with minimal human intervention. When combined with explainable AI techniques, these systems also provide transparent insights into threat predictions and response decisions, improving trust, compliance, and human oversight.

Overall, the convergence of advanced machine learning and generative artificial intelligence represents a transformative advancement in cybersecurity. By enabling early warnings, continuous learning, and intelligent automation, this integrated approach significantly reduces the impact of cyber attacks and strengthens digital resilience. As cyber threats continue to evolve in scale and sophistication, proactive, AI-powered defense

frameworks will be essential for safeguarding future digital ecosystems.

II. LITERATURE SURVEY

1. Title: Cyber Attack Forecasting Using Hybrid Machine Learning
Authors: J. Hu, M. Zhang, and T. Liu (2023)
Abstract:
This study presents a hybrid machine learning framework that integrates Random Forest, Support Vector Machines, and Long Short-Term Memory networks for forecasting cyber attack events. The model analyzes network flow telemetry to capture both statistical patterns and long-term temporal dependencies. Experimental results demonstrate improved recall and earlier detection of attack preparation phases compared to standalone classifiers. The work establishes a strong baseline for proactive cyber defense research.

2. Title: Forecasting Advanced Persistent Threats Using Deep Learning and Multivariate Time Series
Authors: A. Rodriguez, L. Yin, and S. Patel (2024)
Abstract:
This paper applies CNN–LSTM architectures with attention mechanisms to multivariate time-series data derived from host and network logs to predict Advanced Persistent Threats. By learning temporal embeddings of system events, the model detects subtle anomalies well before attack escalation. Robustness evaluations under data drift and adversarial settings confirm the effectiveness of deep sequence models for long-term cyber threat forecasting.

3. Title: Generative Adversarial Networks for Malicious Traffic Synthesis and Prediction
Authors: H. Singh and R. Kumar (2024)
Abstract:
The authors investigate the use of Generative Adversarial Networks to synthesize realistic malicious network traffic for augmenting sparse cyber attack datasets. The generated samples enhance the training of predictive models, resulting in improved F1-scores and earlier warning lead times. The study addresses GAN stability challenges in highly imbalanced cybersecurity datasets.

4. Title: Transformer-Based Attack Sequence Prediction in Dynamic Networks
Authors: M. Elhoseny, S. Shouik, and R. F. Elhafy (2023)
Abstract:
This research introduces a transformer-based architecture for cyber attack prediction by modeling long sequences of network events using self-attention mechanisms. The approach captures long-range dependencies and complex feature interactions without recurrent structures. Results show superior performance over LSTM and RNN models in early multi-stage attack prediction.

5. Title: Explainable Artificial Intelligence for Predictive Cyber Threat Analytics
Authors: L. Chen, W. Fang, and X. Huang (2025)
Abstract:
This work integrates explainable artificial intelligence techniques into predictive cyber defense systems by combining gradient boosting models with SHAP and LIME explanations. The framework improves analyst trust and reduces response time by providing transparent and interpretable attack predictions. The study highlights explainability as a critical requirement for real-world deployment.

6. Title: Graph Neural Networks for Early Detection of Coordinated Cyber Attacks
Authors: S. Almutairi, K. Alharbi, and P. Wang (2024)
Abstract:
This paper proposes a graph neural network-based framework that models network entities and their interactions as dynamic graphs. The approach captures relational and temporal

patterns associated with coordinated cyber attacks. Experimental results demonstrate effective early detection of lateral movement and multi-entity attack behaviors.

III. EXISTING SYSTEM

Existing cyber defense systems primarily focus on reactive security measures such as firewalls, signature-based intrusion detection systems, and rule-driven security information and event management platforms. While these solutions are effective at identifying previously known attack patterns, they struggle significantly when confronted with zero-day vulnerabilities, polymorphic malware, and rapidly evolving attack strategies. As cyber adversaries continuously modify their tools and techniques, static defense mechanisms become outdated quickly, creating critical security gaps.

Most traditional security systems rely heavily on analyzing historical data and predefined rules, which limits their ability to provide predictive intelligence. Alerts are often generated only after an attack has already breached the system or caused partial damage. This delayed response reduces the ability of organizations to contain threats early and increases the cost and complexity of incident recovery. In high-stakes environments such as finance, healthcare, and critical infrastructure, even a short response delay can have severe consequences.

Another major limitation of existing approaches is their inability to handle the scale and complexity of modern security data. With the proliferation of cloud services, IoT devices, and remote work environments, networks generate massive volumes of heterogeneous data. Conventional systems are not designed to efficiently correlate events across distributed environments, leading to fragmented visibility and missed attack indicators. This often results in alert fatigue, where security teams are overwhelmed by false positives and overlook genuine threats.

Furthermore, traditional cyber defense tools lack adaptive learning capabilities. Once deployed, their detection logic remains largely static unless manually updated by security experts. This dependence on human intervention makes systems slow to adapt to new threats and increases operational overhead. Attackers, on the other hand, leverage automation and artificial intelligence to rapidly refine their techniques, creating an imbalance between offensive and defensive capabilities.

Existing systems also fail to model attacker intent and behavior over time. They focus on isolated events rather than understanding multi-stage attack campaigns that unfold gradually. Advanced persistent threats often involve reconnaissance, lateral movement, privilege escalation, and data exfiltration phases, which traditional tools may detect only in isolation, if at all. Without behavioral context, these systems cannot effectively identify coordinated or long-term attacks.

In addition, current cyber defense solutions lack the ability to simulate future attack scenarios. They do not generate synthetic threats or anticipate how attackers might exploit newly discovered vulnerabilities. This limitation prevents organizations from stress-testing their defenses and proactively strengthening weak points before they are targeted in real-world attacks.

The absence of intelligent automation further reduces the effectiveness of existing systems. Most responses still require manual investigation and decision-making, which slows down containment and increases the risk of human error. In fast-moving attack scenarios, such delays can allow threats to spread across networks and compromise critical assets.

Overall, the reactive, static, and fragmented nature of existing cyber defense systems makes them inadequate for today's dynamic threat landscape. To

address these shortcomings, next-generation security solutions must incorporate predictive intelligence, adaptive learning, behavioral modeling, and proactive attack simulation. Without such advancements, organizations will continue to remain one step behind increasingly intelligent and automated cyber adversaries.

IV. PROPOSED SYSTEM

The proposed system introduces a proactive cyber defense architecture that tightly integrates advanced machine learning models with generative artificial intelligence to address the limitations of traditional security solutions. Instead of relying solely on post-incident analysis, the architecture is designed to continuously monitor, learn, and predict potential cyber threats in real time. By leveraging both historical and live security data, the system establishes a dynamic and context-aware security posture capable of adapting to evolving threat landscapes.At the core of the framework, machine learning algorithms analyze diverse data sources such as network traffic, system logs, user behavior, and application activity. These models identify subtle anomalies and early indicators of malicious activity that may signal the initial stages of an attack. By learning complex patterns across large-scale datasets, the system can detect deviations that are often invisible to rule-based or signature-driven defenses, enabling early threat identification with higher accuracy and reduced false positives.

Generative artificial intelligence plays a complementary role by modeling attacker behavior and simulating realistic cyber attack strategies. Through the generation of synthetic attack scenarios, malware variants, and exploit sequences, generative models allow the system to anticipate how adversaries might adapt their tactics in response to existing defenses. This forward-looking capability enables organizations to evaluate potential attack paths and vulnerabilities before they are exploited in real-world conditions. The integration of predictive machine learning and generative AI enables the system to shift from reactive detection to proactive threat prediction. Rather than responding only after an intrusion occurs, the framework provides early warnings and probabilistic forecasts of imminent attacks. These predictive insights empower security teams to prioritize risks, strengthen vulnerable components, and deploy preventive controls in advance, significantly reducing the likelihood and impact of successful breaches.

A key feature of the proposed system is its emphasis on explainability and transparency. Explainable AI techniques are employed to interpret model decisions, providing clear justifications for threat predictions and risk scores. This transparency enhances trust among security analysts and decision-makers, supports regulatory compliance, and facilitates more effective human–AI collaboration in security operations.

In addition, the system delivers automated defense recommendations based on predicted threat severity and attack likelihood. These recommendations may include dynamic firewall rule updates, access control adjustments, network segmentation, or automated incident response actions. By automating routine defensive measures, the system reduces response time and minimizes the reliance on manual intervention during critical attack windows.

The architecture also incorporates continuous learning mechanisms that allow models to evolve as new data and threat intelligence become available. Feedback from detected incidents, analyst responses, and system outcomes is used to refine prediction accuracy and improve future simulations. This adaptive learning capability ensures long-term resilience against emerging and previously unseen attack techniques. Overall, the proposed proactive cyber defense system provides a robust, intelligent, and adaptive security solution. By combining

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

machine learning–driven detection, generative AI–based attack simulation, explainable predictions, and automated response strategies, the framework significantly enhances an organization's ability to anticipate, prevent, and mitigate cyber attacks in modern digital environments.

V. SYSTEM ARCHITECTURE

The proposed Cyber Attack Prediction System integrates traditional Machine Learning techniques with advanced Generative Artificial Intelligence to enhance the detection and prediction of cyber threats in modern network environments. The system architecture begins with a data acquisition layer, where large-scale cybersecurity datasets are collected from network traffic logs, system event logs, firewall records, and intrusion detection systems. These datasets may include features such as IP addresses, packet size, protocol types, login attempts, and abnormal system activities. The collected data is then passed to the data preprocessing module, where noise removal, missing value handling, normalization, and feature extraction are performed to prepare the data for analysis. Feature selection techniques are applied to identify the most relevant attributes that contribute to cyberattack prediction, improving model efficiency and reducing computational complexity.

After preprocessing, the system enters the model training layer, where traditional machine learning algorithms such as Logistic Regression, Random Forest, Support Vector Machines, and Gradient Boosting are initially used to detect patterns related to malicious activities. These models learn from historical cyberattack data to classify network behavior as normal or suspicious. To further enhance prediction capabilities, the architecture incorporates deep learning and generative AI models, such as Generative Adversarial Networks (GANs) or transformer-based models, which can generate synthetic attack scenarios and learn complex attack patterns that may not be present in the training data. This hybrid approach allows the system to improve its capability in identifying zero-day attacks and evolving cyber threats.

The prediction and detection layer analyzes incoming real-time network traffic using the trained models to predict potential cyberattacks before they cause significant damage. The system evaluates the probability of attacks and classifies them into categories such as malware, phishing, denial-of-service (DoS), or intrusion attempts. If suspicious activity is detected, the system activates the alert and response module, which sends notifications to administrators and can trigger automated security responses such as blocking IP addresses, isolating compromised systems, or updating firewall rules. Finally, the visualization and monitoring dashboard provides security analysts with real-time insights, attack statistics, and system performance metrics, enabling proactive cyber defense and continuous improvement of the prediction models. This architecture ensures scalable, intelligent, and adaptive cybersecurity protection by combining traditional machine learning techniques with generative artificial intelligence capabilities.

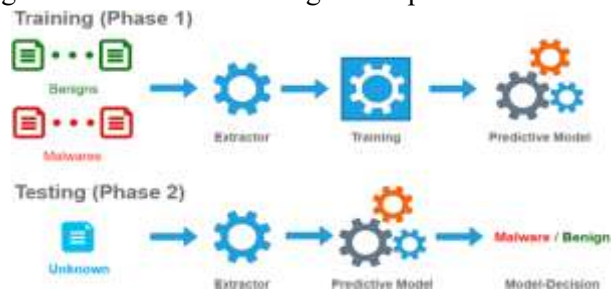

Fig 5.1: Structure of the Proposed System

VI. IMPLEMENTATION

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Fig 6.1: Home Page

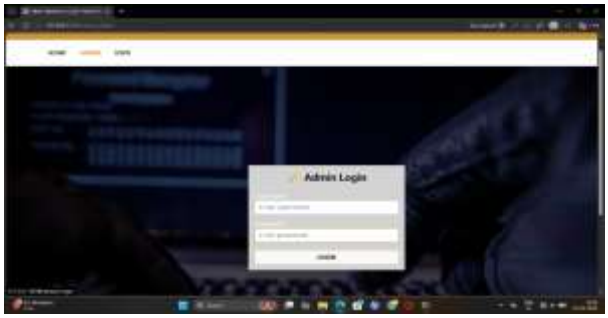

Fig 6.2: Admin Login

Fig 6.3: Admin Dashboard

Fig 6.4: Model Training

Fig 6.5: User Dashboard

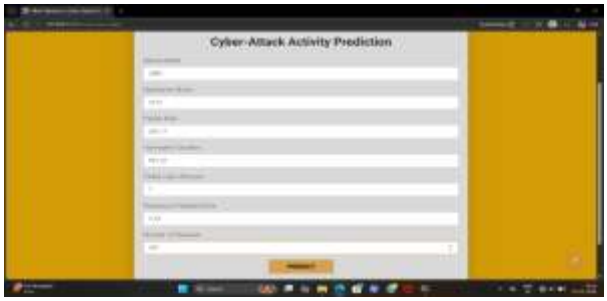

Fig 6.6: Prediction Page

Fig 6.7: Result Page

VII. CONCLUSION

This paper presents a proactive cyber defense framework that synergistically combines advanced machine learning techniques with generative artificial intelligence to enable accurate and timely

cyber attack prediction. Unlike conventional security systems that primarily react after an intrusion has occurred, the proposed framework emphasizes predictive intelligence, allowing organizations to anticipate malicious activities before they materialize. This paradigm shift significantly enhances security preparedness and strengthens the defensive posture of modern digital environments.

By leveraging machine learning models trained on historical and real-time security telemetry, the framework identifies early indicators of compromise and evolving attack patterns with high precision. These models continuously adapt to changes in network behavior, user activity, and threat dynamics, ensuring robust and context-aware predictions. As a result, the system reduces false positives while improving detection accuracy, enabling security teams to focus on high-risk threats.

The integration of generative artificial intelligence further enriches the framework by enabling realistic threat simulation and future attack forecasting. Generative models synthesize plausible attack scenarios, exploit variations, and adversarial strategies that may not yet be observed in real-world datasets. This capability allows the system to explore potential attack paths, assess vulnerabilities in advance, and prepare defenses against emerging and previously unseen threats.

Together, predictive machine learning and generative AI facilitate early warning mechanisms and proactive risk assessment. The framework provides actionable intelligence, including threat likelihood scores, predicted attack timelines, and prioritized mitigation strategies. These insights empower organizations to implement preventive controls, optimize resource allocation, and minimize the potential impact of cyber attacks. The proposed system also emphasizes adaptability and scalability, making it suitable for complex and heterogeneous digital infrastructures such as cloud platforms, IoT ecosystems, and distributed enterprise networks. Continuous learning and feedback mechanisms ensure that the framework evolves alongside the threat landscape, maintaining long-term effectiveness against sophisticated and adaptive adversaries.

Overall, the proposed proactive cyber defense framework demonstrates how the convergence of machine learning and generative artificial intelligence can transform cybersecurity operations. By reducing attack impact, shortening response times, and improving overall cyber resilience, the framework offers a scalable, intelligent, and future-ready solution for securing modern digital infrastructures against emerging cyber threats.

VIII. FUTURE SCOPE

Integration with real-time IoT and 5G security environments

Future extensions of this work can focus on integrating the proposed predictive framework with real-time Internet of Things (IoT) and 5G network infrastructures. These environments generate highly dynamic, high-velocity data streams and are particularly vulnerable due to resource-constrained devices and ultra-low latency requirements. Incorporating real-time telemetry from IoT sensors and 5G network slices would enable early detection of distributed attacks such as botnets, signaling storms, and edge-level intrusions, significantly improving situational awareness at the network edge.

Federated learning for privacy-preserving cyber threat intelligence

To address data privacy and regulatory constraints, federated learning can be employed to enable collaborative model training across multiple organizations without sharing raw security data. Each participant trains local models on-site, while only encrypted model updates are shared and aggregated. This approach enhances collective cyber threat intelligence, improves detection of rare or emerging attacks, and ensures compliance with data protection regulations while maintaining strong predictive performance.

Autonomous cyber defense systems with self-healing capabilities

An important future direction involves the development of fully autonomous cyber defense systems that not only predict attacks but also respond and recover without human intervention. By combining reinforcement learning with predictive and generative models, systems can dynamically reconfigure networks, isolate compromised components, patch vulnerabilities, and restore services. These self-healing capabilities reduce downtime, limit attack propagation, and enhance resilience against persistent and adaptive adversaries.

Large-scale cyber attack simulations using advanced generative models

Advanced generative models can be leveraged to conduct large-scale, high-fidelity cyber attack simulations that mirror real-world adversarial behavior. These simulations can model coordinated multi-stage attacks across complex infrastructures, allowing organizations to stress-test defenses, evaluate response strategies, and identify systemic weaknesses. Such synthetic environments support proactive security planning and continuous improvement of predictive defense mechanisms.

Cross-organization threat sharing using secure decentralized platforms

Future research can explore secure, decentralized platforms for cross-organization threat intelligence sharing. By leveraging distributed ledger or secure peer-to-peer technologies, organizations can exchange attack indicators, risk assessments, and predictive insights in a trusted and tamper-resistant manner. This collaborative approach enhances early warning capabilities at an ecosystem level and strengthens collective defense against large-scale, coordinated cyber attacks.

IX. REFERENCES

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
DOI: https://doi.org/10.1109/COMST.2015.2494502

[2] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: An overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 41, 2020.
DOI: https://doi.org/10.1186/s40537-020-00318-5

[3] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 686–728, 2019.
DOI: https://doi.org/10.1109/COMST.2018.2847722

[4] A. Mozo, B. Ordozgoiti, and S. Gomez-Canaval, "A machine-learning-based cyberattack detector for a software-defined network," *Applied Sciences*, vol. 13, no. 8, p. 4914, 2023.
DOI: https://doi.org/10.3390/app13084914

[5] J. Khan, M. Uddin, and A. S. Islam, "Machine learning approach for identifying multi-step cyber intrusions in smart cities," *Future Internet*, vol. 8, no. 1, 2025.
DOI: https://doi.org/10.3390/fi8010013

[6] L. Gutiérrez-Galeano et al., "LLM-based cyberattack detection using network flow data," *Applied Sciences*, vol. 15, no. 12, 2025.
DOI: https://doi.org/10.3390/app15126529

[7] M. Alauthman et al., "Generative adversarial networks for intrusion detection systems," *Arabian Journal for Science and Engineering*, 2026.
DOI: https://doi.org/10.1007/s13369-026-11103-6

[8] M. H. Shahriar, M. Rahman, and H. Shahriar, "G-IDS: Generative adversarial networks assisted intrusion detection system," *arXiv preprint*, 2020.
DOI: https://doi.org/10.48550/arXiv.2006.00676

[9] D. Li, D. Chen, L. Shi, B. Jin, J. Goh, and S. K. Ng, "MAD-GAN: Multivariate anomaly detection for time series data using generative adversarial networks," 2019.
DOI: https://doi.org/10.48550/arXiv.1901.04997

[10] M. Abdelaty, S. Scott-Hayward, R. Doriguzzi-Corin, and D. Siracusa, "GADoT: GAN-based adversarial training for robust DDoS attack detection," 2022.
DOI: https://doi.org/10.48550/arXiv.2201.13102

[11] D. Li, D. Chen, J. Goh, and S. K. Ng, "Anomaly detection with generative adversarial networks for multivariate time series," 2018.
DOI: https://doi.org/10.48550/arXiv.1809.04758

[12] M. A. Ferrag et al., "Generative AI in cybersecurity: A comprehensive review of large language models and security applications," *Computer Science Review*, 2025.
DOI: https://doi.org/10.1016/j.cosrev.2025.100654
[13] M. S. Siddique et al., "GAN-LSTM based anomaly detection for cyber-physical systems security," *Array*, 2025.
DOI: https://doi.org/10.1016/j.array.2025.100329
[14] B. O. Calviño et al., "Machine learning approaches for cyberattack detection in industrial systems," *Procedia Computer Science*, 2025.
DOI: https://doi.org/10.1016/j.procs.2025.01.049
[15] A. Khamis et al., "Artificial intelligence and machine learning in cybersecurity: Challenges and opportunities," *Knowledge and Information Systems*, 2025.
DOI: https://doi.org/10.1007/s10115-025-02429-y