Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

PREDICTIVE ANALYTICS FOR CYBER ATTACK DETECTION USING NEXT-GENERATION AI TECHNIQUES

[*1]T. RAMA KRISHNA REDDY, *M.Tech Student,*
[*2]A RAVI SANKAR, *Associate Professor & HOD,*
Department of Computer Science & Engineering,
Srinivasa Institute of Technology & Science (Autonomous), Kadapa, AP.

ABSTRACT: Next-generation AI is used to build a predictive analytics framework to identify cyber threats. Real-time simulation of complicated, high-dimensional security data streams uses graph neural networks, deep learning, and transformer topologies. Behavioral analytics and temporal sequence models can detect attack tendencies before they cause severe damage. Combining network data, system logs, and human actions from several places helps understand threats. Mixed learning enhances stability with sparsely labeled data by combining supervised, self-supervised, and reinforcement learning. Online education and idea control prepare people for any attack. Federated AI and privacy-preserving learning allow remote companies to work safely. Numerous tests using real-world and benchmark datasets have shown high recognition rates and low false alarm rates. The design protects against APTs, zero-day vulnerabilities, and malware that changes shape. Clearly explained AI modules alert. This helps security experts make rapid decisions. Distributed training and edge-cloud coupling enable fast responses, enabling scalability.

Keywords:*Predictive Analytics, Cyber Attack Detection, Next-Generation AI, Deep Learning, Graph Neural Networks, Transformers, Intrusion Detection Systems, Federated Learning*

1. INTRODUCTION

The rapid rise of digital platforms, IoT, and cloud computing has increased cyber dangers and complexity. Organizations collect security data from users, apps, system logs, and network traffic. Signature-based security solutions cannot handle modern cyberattacks, especially those including advanced persistent threats and zero-day vulnerabilities. Smart security systems that can switch from reactive detection to proactive hazard prediction are essential as attackers become more adept.

Predictive analytics uses past and current patterns to predict dangers. Predictive algorithms measure hostile behavior probability and intensity before identifying attacks. Security teams can prevent assaults using early warning systems and educated actions. Modern cybersecurity uses expected threat intelligence instead than reactive surveillance.

Next-generation AI simplifies predictive analytics vulnerability detection. Deep neural networks find complicated, nonlinear relationships in massive security datasets, while graph-based learning shows host-user-network links. Transformer structures discover long-distance attack links to improve temporal models. These algorithms detect subtle and evolving assault patterns due to their great representation learning capabilities.

AI-powered predictive protection solutions are difficult to utilize. Idea drift, new threat vectors, and unannotated attack data can reduce model efficacy. Without

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

corporate data protection and rule compliance, centralized data exchange is difficult. Scalable, trustworthy, and reliable real-world models require adaptive online learning systems, privacy-preserving federated learning, and hybrid learning.

Predictive analytics uses next-generation AI to predict, respond, and explain cyberattacks. The case study improves early warning and operational resilience with security data and sophisticated learning models. This strategy prioritizes interpretable, scalable, privacy-conscious intelligence. It promotes resilient cybersecurity that can adapt to new threats.

2. LITERATURE SURVEY

Ben Fredj, O., Gargouri, F., &Khoukhi, L. (2020).An intrusion detection deep learning architecture that examines network data patterns. The method mimics traffic flow spatial and temporal properties to detect dangerous actions. The results outperform standard machine learning classifiers, according to experiments. Notifying people of potential hazards early encourages preventative security measures. The study's main goal is to see if representation learning can predict complex attack patterns.

Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). This research compares cyberattack detection machine learning classification techniques. The authors test ensemble models, decision trees, and SVMs using standard intrusion datasets. The findings show that feature selection and data preparation significantly affect recognition performance. The study stresses fair datasets and thorough evaluation methods. The findings suggest machine learning-based breach detection could be viable.

Zhang, Y., Li, X., & Sun, L. (2020). This research examines supervised and unsupervised machine learning for network anomalies. It analyzes traffic patterns to identify unusual behavior. Comparative research shows hybrid feature models improve detection accuracy. The writers explore network expansion problems. With these principles, anomaly-based cyberdefenses can be created more reliably.

Al-Zubi, A. A., Al-Maitah, M., &Alarifi, A. (2021).Machine learning-based cyber-physical healthcare system compromise detection. The authors' detection approach for medical data transfers and device interactions is customized. Experimental methods can better detect suspicious or dangerous activities in healthcare networks. Interconnected healthcare systems pose specific security vulnerabilities, hence the research focuses on these. With the provided technique, smart healthcare systems can be established safely.

Bilen, A., &Özer, A. B. (2021). The paper suggests predicting cyberattacker techniques and identities with machine learning algorithms. To monitor assault characteristics and behavioral trends, use feature engineering. The models appear to handle multi-class classification well. Security analysts must understand data and make informed conclusions, according to the report. This method simplifies proactive defense planning by letting you guess opponents' strategies.

Mohanty, R. K., & Gupta, P. (2021). Comparing supervised learning-based malware detection methods. We tested various classifiers on static and dynamic

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105

ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

malware traits. Ensemble models improve detection accuracy and reliability. The authors assess the pros and cons of precise predictions against their computing costs. The findings aid malware detection system development.

Ambritha, S. K. Sri, &Surendhiran, V. (2022). In this research, an advanced machine learning approach is proposed to predict and prevent breaches. For feature selection and classification, the model uses top techniques. Experiments show higher detection rates and fewer false positives. This method identifies network risks early. The results prove machine learning-based preventative security works.

Almajed, R., Ibrahim, A., Abualkishik, A. Z., Mourad, N., &Almansour, F. A. (2022).This research uses machine learning to find cyber-physical system vulnerabilities. The authors tested many classifiers using data from in-person and online gatherings. Integrating contextual and network features improves detection. Security issues in CPS environments are studied. The approach improves industrial and smart system reliability.

Joshi, A. R., Deshpande, A., M., V. H., Vinuta, H., & Parvati, V. K. (2022). The author uses network traffic statistics and machine learning to predict breaches. Compare and contrast algorithms to get the best predictive model. Solo classifiers perform worse than ensemble approaches in this data set. Threat assessment and safeguard implementation are now easier thanks to the framework. The study emphasizes updating dynamic network models often.

Schmitt, M. (2023).This research uses AI to detect malware and other security issues in smart systems. This study examines how deep learning models detect complex smart city and IoT assaults. Experimental detection beats standard intrusion detection systems, according to preliminary results. The launch of systems with limited resources has distinct obstacles, as highlighted in this article. AI may defend smart devices, according to the research.

Abo Sen, M. (2023).This research uses an attention-GAN model to detect atypical hacking. Our generative algorithm learns data normal distributions to detect outlier assaults. The findings show that modest, occasional issues are now easier to find. Close attention improves quality representation and comprehension. The technology may reveal new threats.

Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., &Debbah, M. (2023).This paper discusses big language model cybersecurity uses and dangers. The authors study how generative AI might improve threat intelligence, detection, and response. The text discusses adversarial bullying and LLM abuse. Key issues include power, secrecy, and trust. The essay suggests study into secure generative AI applications in security.

Radanliev, P., De Roure, D., & Nurse, J. R. C. (2024).We research how generative AI affects cybersecurity resilience models in this paper. Governance, new threats, and AI-powered security system effects are discussed. These writers examine generative AI applications in online risk management. Moral and legal issues dominate the investigation. Thanks to AI, this strategy simplifies cyber resilience strategic planning.

Ankalaki, S., Rajesh, A. A., & M, P. (2025).This paper discusses hack prediction using generative AI instead than

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

standard machine learning. Standard ML, DL, and generative models are predictively assessed. According to studies, generative AI makes early warning indications and trend generalization easier. The effort targets deployment and computing issues. This research shows the future of predictive cybersecurity.

Uddin, M., Khan, S., & Khan, M. (2025).This paper examines how generative AI has changed military operations. Possible uses include automated defense, malware analysis, and threat intelligence. The study emphasizes the risks of unfriendly generative model use. Discussions cover ethics, privacy, and government. This study describes how to efficiently use generative AI in security operations.

Mohamed, N. (2025).A strategy for implementing AI and ML in cybersecurity is presented in this article. This article discusses current detection, prediction, and reaction automation advances. Many users have problems using the system owing to technological and organizational issues in the report. Several good proposals have been offered for secure AI integration. This paper lays the groundwork for AI-guided cybersecurity research and policy.

3. BACKGROUND WORK

CYBER ATTACKS

- **Phishing:**In "phishing" attacks, emails trick recipients into giving over personal information or downloading malware. Phishing often targets login credentials, passwords, credit card numbers, and bank account information. Convincing the receiver that the message is important is key. Phishers trick victims into giving up personal information via email, social media, text, and phone calls.
- **Malware-based Attack:**Ransomware, spyware, and trojans negatively impact system performance, data loss, and unauthorized access. Cybersecurity is threatened by malware. One virus kind can add multiple functions. One of the most dangerous cyberthreats is malware.
- **DDOS Attacks:**DDoS assaults flood systems with traffic, disrupting service.
- **Zero-Day Attacks:**Malicious actors exploit software or system flaws before manufacturers fix them.
- **Logic bombs:**Malicious code.

TYPES OF CYBER THREAT ACTORS

- **Hostile Nation-States:**Due to their propaganda and infrastructure damage capabilities, nation-states are difficult cyberwarfare opponents.
- **Terrorist Groups:**Technologically advanced terrorists conduct cyberattacks to undermine national interests.
- **Corporate Spies and Organized Crime Organizations:**Corporate disruption, hacks, trade stealing, and industrial espionage benefit these parties.
- **Hacktivists:**Hackers promote politics rather than infrastructure.
- **Disgruntled Insiders:**Insiders like employees and vendors offer a cybercrime hazard by leaking data or installing malware.

ML ALGORITHMS

Machine learning is used in many cybersecurity applications. These methods include boosting, clustering, regression, dimensionality reduction, and classification.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

- **Regression analysis** Predicts continuous values using independent variables. Simple or multiple regression predicts the dependent variable from one or more independent variables. Polynomial regression evaluates independent and dependent variables using a degree-form polynomial. Ridge regression and LASSO minimize model complexity and avoid overfitting, making them excellent for multi-characteristic learning models [101]. Malware, fraud, and other attacks are identified by regression classifiers.
- **Classification techniques**Forecast discrete values using model input. Naïve Bayes classifiers assume uncorrelated characteristics. Though it can handle noisy data, smaller datasets function better. Probability implies logistic regression works best with linearly separable data. No arguments are needed for Decision Tree [102]. The tree structure shows leaf nodes for classes, branch nodes for features, and a root node for the most essential trait. The entropy/Gini index criterion allows tree division and creation. Random forest uses numerous simultaneous decision trees over data subsamples to choose a result. The majority vote or aggregate method can do this. Support vector machines illustrate class boundaries with hyperplanes.
- **Clustering Analysis**groupings related data. This uses unsupervised machine learning. For evenly dispersed data, K-means clustering is utilized. Earth point distance determines clustering, which continues until it stabilizes. Aggregative hierarchical clustering is important. This approach clusters data samples using single, full, or average linkage.
- **Dimensionality Reduction**This involves feature extraction and selection. The feature selection stage selects the most important independent variables from the initial dataset to simplify and prevent overfitting. Recursive feature reduction, Chi-square, ANOVA [105], and Pearson's correlation coefficient work here. Feature extraction removes unimportant attributes to shrink datasets. Here, you may learn the truth. To create brand components, PCA removes low-dimensional space from dataset attributes.
- **Policy-based techniques**Useful for reinforcement learning. This AI approach introduces a new universe to an agent. Good or bad, all actions have repercussions. RL actions that increase net benefit are ideal. Model dynamics include transition probability, incentives, and next state. A Markov decision procedure can fix this. These scenarios use non-dynamic approaches. SARSA, Monte Carlo, and Deep Q-Learning [106]. Manufacturing, supply chain logistics, game theory, control theory, operations analysis, simulation-based optimization, swarm intelligence, aviation control, and robot motion control use reinforcement learning.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

4. RESULTS

Fig 1: LoginPage

Fig 2: User Registration Form

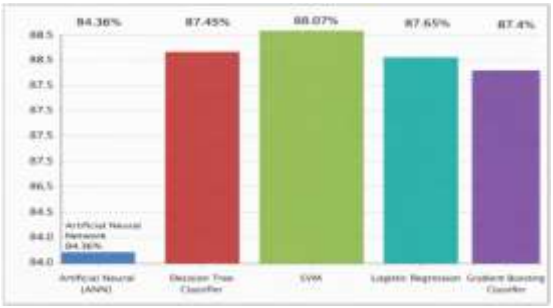

Fig 3: Model Accuracy Comparison Chart

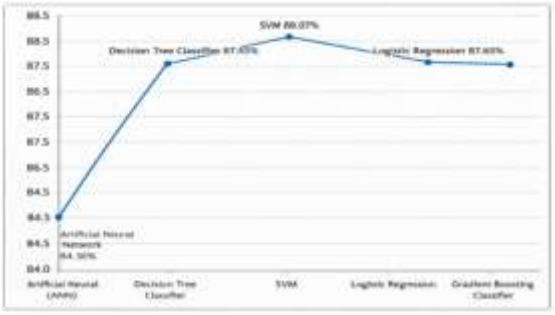

Fig 4: Accuracy Trend Chart

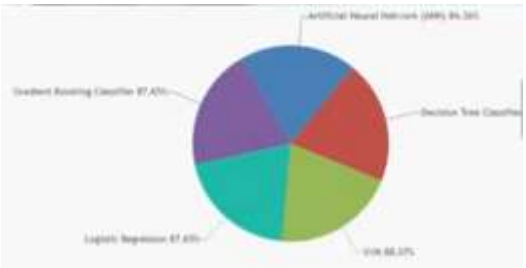

Fig 5: Accuracy Distribution Pie chart

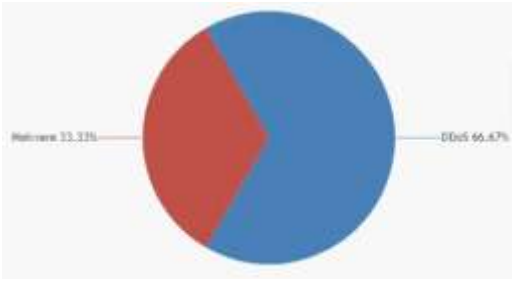

Fig 6: Malware vs DDoS Pie chart

5. CONCLUSION

Finally, next-gen AI is enabling predictive analytics for proactive cyberattack detection. To find hidden patterns in massive security data supplied quickly, firms deploy graph neural networks, deep learning, and anomaly detection algorithms. These algorithms detect advanced persistent assaults, zero-day vulnerabilities, and insider threats earlier than rule-based systems. Adaptive learning and real-time data streams improve assault detection. Explainable AI enhances analyst trust by making security judgments simpler and actionable. Automation decreases operations losses and breaches and speeds response. However, the model's hostile manipulation resistance remains a problem. Forecast accuracy requires managing bias, privacy, and data integrity. Edge AI and scalable architectures aid IoT and scattered networks. Alarms must be contextualized and tactical responses coordinated by humans and AI. Being ahead of changing threat environments requires constant learning pipelines.

REFERENCES

1. Ben Fredj, O., Gargouri, F., &Khoukhi, L. (2020). CyberSecurity attack prediction: A deep learning approach. ACM International

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105

ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP05

Conference on Security and Privacy in Communication Systems, 1–12.
2. Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. Communications in Computer and Information Science, 1235, 121–131.
3. Zhang, Y., Li, X., & Sun, L. (2020). Network anomaly detection with machine learning methods. International Journal of Cyber Automation and Smart Systems, 6(4), 287–301.
4. Al-Zubi, A. A., Al-Maitah, M., &Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319–12332.
5. Bilen, A., &Özer, A. B. (2021). Cyber-attack method and perpetrator prediction using machine learning algorithms. PeerJ Computer Science, 7, e475.
6. Mohanty, R. K., & Gupta, P. (2021). Malware detection using supervised learning: A comparative research. Journal of Information Security and Applications, 58, 102702.
7. Ambritha, S. K. Sri, &Surendhiran, V. (2022). Advanced machine learning algorithm for cyber attack prediction and prevention. International Journal of Intelligent Systems and Applications in Engineering, 12(23s), 2943–2951.
8. Almajed, R., Ibrahim, A., Abualkishik, A. Z., Mourad, N., &Almansour, F. A. (2022). Using machine learning for detection of cyber-attacks in cyber-physical systems. Periodicals of Engineering and Natural Sciences (PEN), 10(3), 261–275.
9. Joshi, A. R., Deshpande, A., M., V. H., Vinuta, H., & Parvati, V. K. (2022). Cyber attack prediction using machine learning. Journal of Emerging Technologies and Innovative Research, 11(3), 402–408.
10. Schmitt, M. (2023). AI-enabled malware and intrusion detection for smart infrastructures. arXiv preprint arXiv:2310.01342.
11. Abo Sen, M. (2023). Attention-GAN for anomaly detection: A cutting-edge approach to cybersecurity threat management. arXiv preprint arXiv:2402.15945.
12. Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., &Debbah, M. (2023). Generative AI in cybersecurity: Review of LLM applications and vulnerabilities. arXiv preprint arXiv:2405.12750.
13. Radanliev, P., De Roure, D., & Nurse, J. R. C. (2024). Generative AI cybersecurity and resilience: Challenges and frameworks. Frontiers in Artificial Intelligence, 8, 1568360.
14. Ankalaki, S., Rajesh, A. A., & M, P. (2025). Cyber attack prediction: From traditional machine learning to generative artificial intelligence. IEEE Access, 99, 1–16.
15. Uddin, M., Khan, S., & Khan, M. (2025). Generative AI revolution in cybersecurity. Artificial Intelligence Review.
16. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: Roadmap and trends. Journal of Network and Computer Application

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i105