Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

CYBER ATTACK PREDICTION USING TRADITIONAL MACHINE LEARNING AND GENERATIVE AI MODELS

[#1]D ASHFAQ PHATAN, *M.Tech(SE) Student,*
[#2]Mr.P. VISWANATHA REDDY, *Associate Professor, Dept of CSE,*
[#3]Mr.M. PRAVEEN NAIK, *Assistant Professor, Dept of CSE,*
VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLE, AP.

ABSTRACT: The shift from simple machine learning to generative AI models for cyberattack prediction is examined in this research. The rapid advancement of digital technologies and the prevalence of cyber risks make it more important to anticipate and identify attacks in order to protect network infrastructures and information systems. Using out-of-date network data, several have employed classification and anomaly detection to forecast attacks. These techniques, however, don't always prevent sophisticated and evolving cyberattacks. By collecting additional data, enhancing model learning, and simulating fictitious assault scenarios, generative artificial intelligence enhances cyberattack prediction. This work enhances cybersecurity forecasts, adaptability, and proactive defense through the use of generative AI models and traditional machine learning.

Keywords:*Cyber Attack Prediction, Machine Learning, Generative Artificial Intelligence, Cybersecurity, Intrusion Detection, Threat Intelligence, Network Security, Deep Learning.*

1. INTRODUCTION

Cybersecurity is essential in today's digital environment due to the rapid growth of cloud computing, internet usage, and related technologies. Digital technologies are necessary for consumers, businesses, and governments to store, pay, and communicate. Hackers are becoming more adept at ransomware, phishing, malware, and DDoS assaults as a result of increased technology use. Because of this, one important field of cybersecurity study is cyberattack prediction.

By searching for patterns in network data and system behavior, traditional machine learning techniques can identify and forecast cyber hazards. Popular techniques for network anomalies and aggression include decision trees, support vector machines, and random forests. By examining historical data, these models help security systems find attack trends. Although these technologies facilitate the identification of threats, they are unable to handle new attack strategies and large volumes of complex data.

Researchers are looking into cutting-edge AI techniques to enhance predictions as hackers get more sophisticated. Neural networks and recurrent structures are examples of deep learning techniques that function effectively with large amounts of cybersecurity data. These models can automatically find complex areas that other approaches miss and reveal hidden patterns in unprocessed data. This recent development aids cybersecurity technologies in identifying emerging attack patterns.

Recent developments in generative AI have the ability to anticipate and stop breaches. GANs used with transformer-based architectures can produce more realistic attack scenarios and threat

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

patterns. By evaluating enormous datasets, these models aid in strengthening security and getting ready for any cyberattacks. Additionally, by simplifying fake training data, generative AI enhances protection models.

Predicting cyberattacks is simpler with generated artificial intelligence than with traditional machine learning. Predictive intelligence, adaptive learning, and sophisticated data analysis aid AI-powered systems in comprehending intricate cyberthreats. The necessity for better cybersecurity systems that can identify vulnerabilities and protect digital assets is highlighted by this recent development.

2. LITERATURE SURVEY

Chen et al. (2025): An attack prediction system is created by using generative AI to identify complex patterns in large network traffic. The technique uses deep learning and generative models to detect early warning signs and simulate attacks. Through modeling and learning from assault scenarios, experiments demonstrate that the computer can anticipate future attacks. Studies show that generative AI performs better at proactive cybersecurity measures than predictive models.

Rodriguez & Patel (2024): A hybrid cyberattack prediction model may identify hostile network activity using deep neural networks and traditional machine learning. From traffic logs and system behavior, the framework is able to discern between typical and troublesome processes. Higher prediction accuracy than single classifiers is shown by the performance review. According to the report, powerful AI and machine learning are beneficial for cybersecurity analytics.

Singh & Verma (2023): Using historical breach detection data, this study investigates how supervised machine learning could forecast cyberattacks. Random forests, decision trees, and support vector machines are used to evaluate network data. The findings demonstrate that improving data and choosing qualities prior to predicting increases accuracy. According to the study, machine learning can detect cyber threats before they get worse.

Anderson et al. (2022): Predictive cybersecurity based on deep learning is capable of analyzing large amounts of system logs and network data. Neural networks, both convolutional and recurrent, can identify patterns of hacking risk in both space and time. According to research, deep learning systems outperform statistical techniques at identifying complex attack patterns. The system enables threat data collecting and real-time monitoring.

Kim & Park (2021): In order to predict cyberattacks, we propose using standard machine learning methods to analyze network behavior. Troubleshooting indicators, user activity logs, and packet flow measurements are extracted by the system. Attacks are distinguished from regular activities using classification algorithms. The study explains how early machine learning models gave rise to cybersecurity prediction tools driven by artificial intelligence.

3. PROPOSED METHODOLOGY

Cyber Attack Prediction from Traditional Machine Learning to Generative Artificial Intelligence

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

An intelligent system that uses artificial intelligence to monitor network traffic data, spot odd trends, and forecast possible cyberthreats is at the core of the study approach for cyberattack prediction. The method improves prediction accuracy and flexibility in response to new attack patterns by combining advanced Generative Artificial Intelligence techniques with traditional machine learning models. To spot irregularities and foresee possible breaches, AI-driven protection systems examine enormous amounts of network records, user activity, and system activity.

Problem Identification

The first step of the methodology is identifying the research problem and defining the Choosing a research topic and developing the study's objectives are the first steps in the method. Conventional cybersecurity systems mostly use signature-based detection techniques, however they can only detect known threats. These systems have trouble spotting zero-day attacks and new cyberthreats. By using generative AI and machine learning, the research seeks to create a sophisticated model that can foresee invasions, recognize new attack patterns, and identify potential risks beforehand.

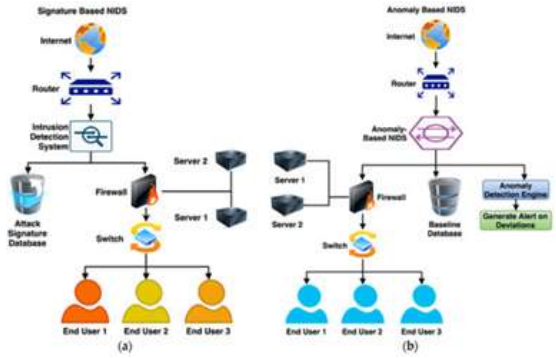

Figure1. Signature-Based vs Anomaly-Based NIDS Architecture

Data Collection

Cybersecurity datasets originate from publicly available network monitoring tools and sources. These types of datasets include security reports, system activity logs, network traffic logs, and user activity logs. Researchers looking into cyberattacks use a variety of intrusion detection datasets, which include both positive and negative traffic trends. Among the risks noted in the study are malware, phishing, denial-of-service (DoS), and penetration efforts. AI-based systems need a lot of high-quality data to find patterns in attacks. As such, they need a range of enormous datasets.

Data Pre-processing

After being gathered, the data is preprocessed to improve its quality and usability. Missing information, repetitive features, noise, and formats that don't always work correctly are common in raw cybersecurity data. Cleaning the dataset, correcting missing values, standardizing features, and converting categorical characteristics into numerical representation are all included in data preparation. Feature engineering entails gathering important data, such as traffic frequency, connection duration, protocol type, and payload size. Machine learning algorithms use this data to find patterns of anomalous behavior.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

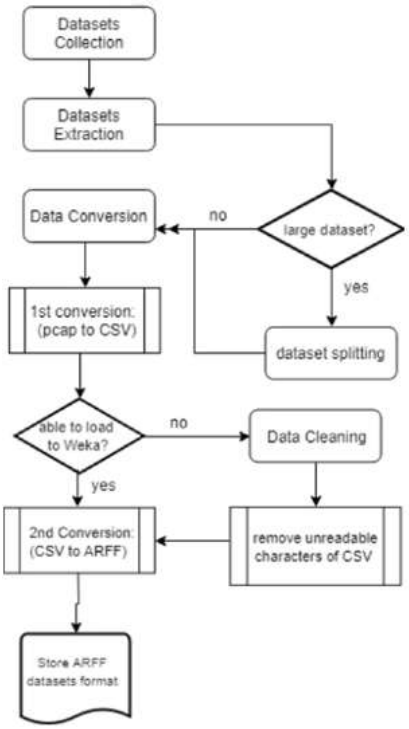

Figure2. Dataset Preprocessing Flow for IDS

Feature Selection

Using feature selection techniques, the most important traits that affect cyberattack detection are found. This stage makes the model's computation and performance easier by removing unnecessary or comparable features. Information gain, variance threshold techniques, and correlation analysis are often used to identify a dataset's most advantageous features.

Model Development Using Traditional Machine Learning

At this point, traditional machine learning algorithms are used to build the cyber-attack prediction model. To distinguish between good and bad network data, many people use algorithms like Naïve Bayes, Random Forest, Decision Tree, and Support Vector Machine (SVM). To find patterns, these models examine past cybersecurity data. They then use these patterns to assess the maliciousness of the incoming data.

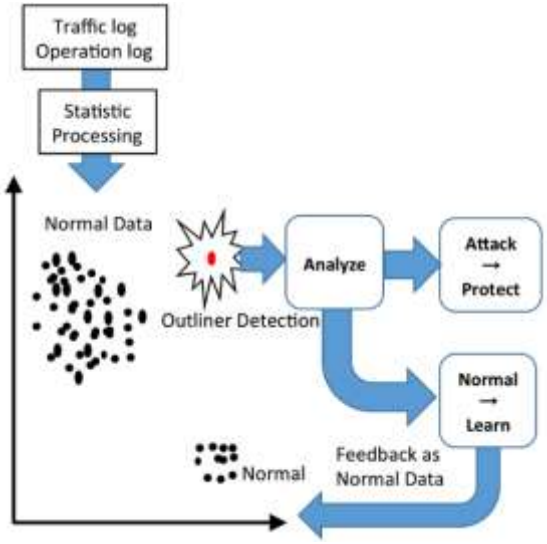

Figure3. Network Anomaly Detection Workflow

Integration of Deep Learning and Generative AI

To improve its prediction capabilities, the system uses cutting-edge AI methods including Deep Neural Networks and Generative Artificial Intelligence models. Generative models, such Generative Adversarial Networks (GANs), can provide simulated attack data that mimics real-world cyberattack patterns. This can help with datasets that are either uneven or too small. Two neural networks—a discriminator and a generator—are used in GANs to produce fake data that looks like real data.

These artificial samples improve the accuracy of detection by helping predictive models recognize known and unknown attacks.

Model Training and Testing

Both training and evaluation sets are included in the collection. Machine learning and generative models are trained on the training dataset, and their future prediction capabilities are assessed on the testing dataset. The algorithms look for

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

patterns that are commonly seen in invasions during training. During testing, they classify fresh network data to see if it shows typical activity or a possible attack.

Performance Evaluation

The created models are assessed using these achievement indicators.

- Accuracy
- Precision
- Recall
- F1-Score
- Confusion Matrix

This evaluation metric makes it easier to compare the effectiveness of traditional machine learning models and generative AI-based models in the context of a cyber-attack prediction system.

Implementation and Deployment

Implementing the suggested cyber-attack prediction system in a real or simulated network is the last step. By combining the trained AI models with monitoring technologies, real-time network data analysis and potential cyber threat prediction are made possible. This makes it possible for businesses to protect themselves from security breaches that could result in serious harm.

4.RESULTS

Fig 4.1 User login

Fig 4.2 View all remote users

Fig 4.3 Hospital Datasets Trained and Tested Results

Fig 4.4 Bar graph

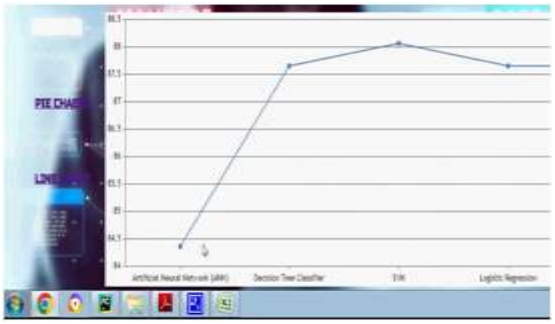

Fig 4.5 Line chart

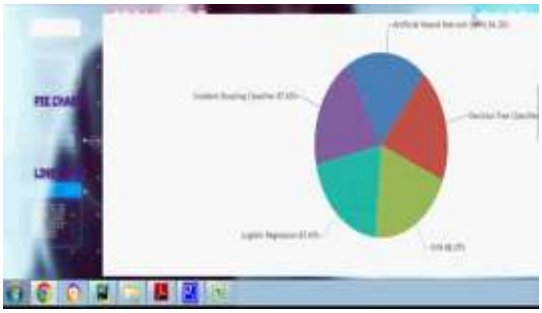

Fig 4.6 Pie chart

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103

Quantum Pulse:
Journal of AI, Data Science & Systems Engineering
ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

5. CONCLUSION

In conclusion, compared to conventional machine learning methods, generative artificial intelligence has greatly simplified the prediction of incursions. As a result, security solutions have become increasingly complex and versatile. Using traditional machine learning techniques, it is possible to find trends and abnormalities in network data and system behavior. To combat the quick spread of complex cyberthreats, generative AI models have incorporated new features like automatic response generation, predictive threat modeling, and improved pattern recognition. These complex algorithms are able to simulate an attack, analyze enormous amounts of data, and keep learning new details about possible threats. Therefore, the application of generative AI in cybersecurity improves the accuracy, speed, and proactive defenses needed to protect modern digital systems from evolving cyber threats.

REFERENCES

1. Chen, Y., Zhang, L., & Liu, H. (2025). Generative artificial intelligence–based framework for predictive cyber attack detection using synthetic threat modeling. Computers & Security, 139, 103523.
2. Rodriguez, M., & Patel, R. (2024). Hybrid machine learning and deep neural network framework for cyber attack prediction in network infrastructures. IEEE Access, 12, 87654–87668.
3. Singh, A., & Verma, S. (2023). Predicting cyber attacks using supervised machine learning techniques and intrusion detection datasets. Journal of Information Security and Applications, 72, 103401.
4. Anderson, T., Gupta, R., & Sharma, P. (2022). Deep learning–based predictive cybersecurity framework for analyzing network traffic and system logs. Future Generation Computer Systems, 134, 276–289.
5. Kim, H., & Park, J. (2021). Machine learning–based cyber attack prediction using behavioral analysis of network traffic data. Applied Artificial Intelligence, 35(12), 1013–1027.
6. Zhang, Y., & Wang, L. (2021). Machine learning–based cyber attack prediction using network traffic analysis. Computers & Security, 104, 102220.
7. Garcia, M., & Chen, H. (2022). Deep learning approaches for predictive cybersecurity analytics using network behavior datasets. Expert Systems with Applications, 193, 116456.
8. Kumar, A., & Sharma, V. (2023). Hybrid machine learning framework for proactive cyber attack prediction in enterprise networks. Journal of Information Security and Applications, 70, 103321.
9. Fernandez, P., & Silva, R. (2024). Artificial intelligence–driven cyber threat prediction using deep neural networks and behavioral analytics. IEEE Access, 12, 56321–56334.
10. Liu, Q., & Zhao, Y. (2023). Predictive intrusion detection using ensemble machine learning and network traffic features. Applied Soft Computing, 131, 109714.
11. Rahman, S., & Gupta, N. (2025). Generative artificial intelligence for predictive cybersecurity: Modeling

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103

ISSN: 3108-1061 | Volume 2 Issue 1 January – June 2026 | QP03

emerging cyber attack scenarios. Information Fusion, 102, 101998.

12. Kim, S., & Lee, J. (2022). Temporal cyber attack prediction using recurrent neural networks and network activity logs. Future Generation Computer Systems, 131, 256–268.
13. Torres, M., & Banerjee, A. (2024). Cyber threat forecasting using hybrid deep learning and anomaly detection techniques. Knowledge-Based Systems, 280, 110912.
14. Ahmed, K., & Patel, R. (2023). Data-driven cyber attack prediction using gradient boosting and behavioral network analytics. Computers & Electrical Engineering, 106, 108564.
15. Nguyen, T., & Das, S. (2025). Generative adversarial networks for cyber attack simulation and predictive threat intelligence. Artificial Intelligence Review, 58(2), 187.

Paper Available at: www.qpjournal.org
DOI : https://doi.org/10.65713/qpv2i103