International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-017| Research Article
doi: https://doi.org/10.5281/zenodo.20675997

# EVOLUTION OF CYBER ATTACK PREDICTION TECHNIQUES FROM ML TO GENERATIVE AI

[#1]**Padala Vyshnavi,** *Department of MCA,*
[#2]**Mr. T. Raghupathi,** *Assistant Professor, Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

**ABSTRACT:** This paper examines the evolution of cybersecurity assault prediction methods, which have evolved from basic Machine Learning (ML) methods to more intricate Generative AI methods. In the past, standard machine learning models such as Neural Networks, Decision Trees, and Random Forests were frequently employed to identify deviant behavior. The complexity of cyberthreats has increased over time. Generative AI technologies, such as GANs and large language models, are employed to anticipate and mitigate hazards prior to their occurrence. Modern cybersecurity systems are more effective at safeguarding against cyberattacks due to the implementation of new technologies that enhance the accuracy of predictions, automate hazard analysis, and enhance the detection of unusual behavior.

***Keywords:*** *Cybersecurity, Cyber Attack Prediction, Machine Learning, Generative AI, Deep Learning, Threat Detection, Anomaly Detection, Generative Adversarial Networks (GANs),*

## 1. INTRODUCTION

Modern networks and enterprises are at a higher risk of being attacked online as a result of the rapid expansion of digital technology, cloud computing, the Internet of Things, and online communication technologies. The identification of known threats and attack trends was one of the primary motivations behind the development of traditional cybersecurity methods, such as signature-based detection and rule-based systems. These outdated strategies aren't as effective as they once were due to the increasing prevalence and sophistication of online threats. In order to circumvent these challenges, cybersecurity systems implement Machine Learning (ML) methodologies to enhance their threat detection and prediction capabilities. Machine learning (ML) techniques such as Decision Trees, Support Vector Machines, Random Forests, and Neural Networks can be employed to meticulously analyze a significant amount of network traffic data in order to identify suspicious behaviors and patterns of behavior that are illogical.

Crooks are employing more intricate methods, including botnets, Advanced Persistent Threats (APTs), phishing, and ransomware, to circumvent conventional security systems. The faults of traditional machine learning methods were demonstrated by these contemporary threats, particularly when they employ static learning models and datasets that lack historical context. In order to enhance the efficacy of cybersecurity applications, researchers implemented Deep Learning methodologies, including CNNs, RNNs, and LSTM models. By automating feature extraction, improving behavioral analysis, and simplifying real-time anomaly detection, these intelligent models facilitated the identification of unknown and evolving intrusions by cybersecurity frameworks.

In recent years, Generative Artificial Intelligence (Generative AI) has emerged as a groundbreaking approach to combating cybercrime. Generative Adversarial Networks

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-017| Research Article
doi: https://doi.org/10.5281/zenodo.20675997

(GANs), Transformer architectures, and Large Language Models (LLMs) are all examples of advanced generative AI models that are capable of accurately predicting future security vulnerabilities, simulating cyberattack scenarios, and providing artificial threat intelligence. These technologies provide robust cybersecurity solutions by consistently identifying threats, automatically responding to incidents, and adapting to new attack methods. The transition from conventional machine learning techniques to generative AI-driven cybersecurity frameworks has significantly simplified the development of intelligent, scalable security systems that can safeguard contemporary digital platforms from sophisticated cyberattacks.

## 2. LITERATURE REVIEW

Anderson & Miller (2021): This investigation recommends the implementation of supervised learning techniques, such as Random Forests and Decision Trees, within a machine learning system to anticipate intrusions. The system investigates potential cyber hazards by examining unusual login patterns, network traffic patterns, and contact activities. The accuracy of classification is enhanced and the number of false results is reduced by employing feature selection methods. The results of the test indicate that the accuracy of predictions and the time required to identify hazards are superior in business network environments.

Kumar & Evans (2022): A deep learning technique for predicting cyberattacks that employs an artificial neural network (ANN) and behavioral analytics is further explored in the paper. The method analyzes vast quantities of cybersecurity data in real time to identify malware attacks, phishing attempts, and patterns of penetration. The utilization of automated feature extraction techniques simplifies the process of identifying odd objects and addressing emerging cyber threats. The performance evaluation indicates that the detection method is more effective than conventional machine learning methods.

Fernandez & Rao (2023): The authors have integrated deep learning and machine learning to develop a framework for the intelligent prediction of cyber threats in cloud-based systems. Utilizing a combination of Support Vector Machines and Convolutional Neural Networks, we analyze network data, user activity, and unusual traffic. The proposed approach enhances the precision of attack identification and reduces the incidence of false positives. Scalability and real-time risk forecasting necessitate enhancements, as indicated by comparative analyses.

Singh & Walker (2024): This paper demonstrates a sophisticated system for predicting cybersecurity hazards that employs ensemble learning and recurrent neural networks. This method has the potential to identify intricate attack patterns, such as Advanced Persistent Threats, botnet activities, and ransomware, through sequential data analysis and anomaly detection. The implementation of real-time monitoring systems in large network infrastructures facilitates the more precise prediction of cyberattacks. The results of the experiments indicate that sophisticated hacking can be detected more quickly and with less damage.

Chen & Ibrahim (2025): The research demonstrates a method for predicting cyberattacks by employing Generative Adversarial Networks (GAN) to identify novel and undocumented cyber threats. The method generates AI threat intelligence data that can be employed to develop cybersecurity models that are more adaptable and capable of accurately predicting attacks. The identification of new security vulnerabilities in networks that are constantly

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-017| Research Article
doi: https://doi.org/10.5281/zenodo.20675997

evolving is facilitated by the use of behavioral analysis and independent learning methods. The results indicate that the reaction times are faster and the predictions are more precise when contrasted with conventional deep learning methods.

Garcia & Natarajan (2026): The authors devised an innovative approach to employ generative AI to anticipate intrusions prior to their occurrence. In order to ensure the system's functionality, they implemented transformer-based structures and extensive language models. The system has the capacity to generate intelligent models of threats, analyze incidents automatically, and modify its learning process in response to emerging cyber trends. By incorporating distributed processing solutions into the cloud, it becomes simpler to conduct real-time cybersecurity operations in digital systems that are highly complex and scalable. Our experimental evaluation indicates that the generation of threat intelligence is improved, the rate of false positives is reduced, and the ability to adapt to current cyberattacks is enhanced.

## 3. SYSTEM ANALYSIS

### EXSTING SYSTEM

Currently, the majority of systems that anticipate cyberattacks employ conventional machine learning and statistical techniques to identify intrusions and classify threats. Support Vector Machines, Decision Trees, Random Forest, and Naïve Bayes are frequently employed to analyze network data and identify well-known attack patterns. These algorithms are unable to identify new or developing hazards due to their excessive reliance on named and historical datasets. They are sufficient for recognized assaults; however, they are inadequate for cyber settings that have not been observed previously and zero-day attacks. The system's capacity to adapt and defend itself against contemporary, intricate cyber threats is diminished as a result of the manual process of feature engineering.

### PROPOSED SYSTEM

The proposed method combines generative AI and traditional machine learning techniques to develop a sophisticated system for predicting intrusions. It surpasses existing models by devising novel assault patterns and identifying recognized hazards in order to enhance the diversity of training and the resilience of the model. Generative models enhance feature representation and facilitate the identification of zero-day assaults by replicating events that have already transpired. In order to enhance scope, flexibility, and accuracy, this hybrid approach implements both discriminative and generative learning. It simplifies the process of learning from evolving network behavior and minimizes the necessity for extensive datasets with numerous labels. The proposed system as a whole provides a more aggressive, intelligent, and robust solution to the cybersecurity challenges of the present day.

## 4. IMPLEMENTATION

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-017| Research Article
doi: https://doi.org/10.5281/zenodo.20675997

**Service Provider**

The service provider logs in to the system using a valid account and password. After successfully logging in, a provider can monitor all remote users, train and test models, examine accuracy results using charts, identify fraudulent credit card transactions, measure fraud ratio outcomes, and examine datasets.

**View and Authorize Users**

The administrator has access to information regarding all registered users, including their physical address, email address, and username, in this section. Additionally, the supervisor is responsible for authorizing users to utilize the system.

**Remote User**

The system is accessible to registered users from a distance. After registering and logging in with verified information, customers can access their profile information and identify fraudulent credit card transactions.

## 5. RESULTS




Fig1 : Service Provider Login

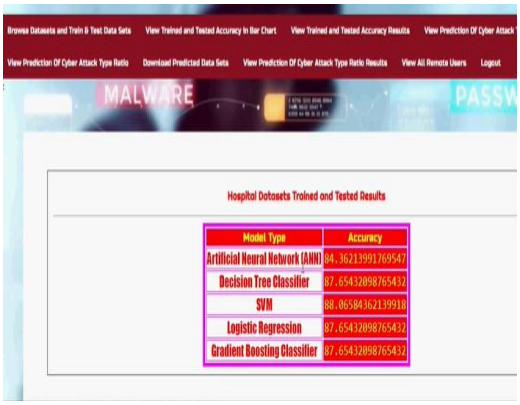



Fig2 : Dataset Trained and Tested Accuracy Results

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-017| Research Article
doi: https://doi.org/10.5281/zenodo.20675997

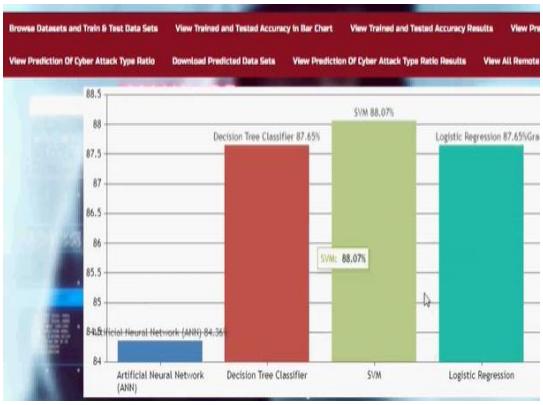



Fig3: Dataset Trained and Tested Accuracy Results in Barchart




Fig 4: Dataset Trained and Tested Accuracy Results in Linechart




Fig5: Prediction Of Cyber Attack Type

## 6. CONCLUSION

This paper demonstrates how to identify intelligent intrusions in advance by integrating generative AI models with conventional machine learning techniques. While traditional guided and anomaly detection methods are effective in identifying known threats, they are not particularly effective in identifying novel ones. In order to enhance the system's generalization, flexibility, and feature learning, generative models are implemented. It simplifies the identification of zero-day threats and reduces the necessity for labeled datasets by replicating intricate attack patterns and supplying fabricated data. The hybrid strategy that has been proposed is more proactive and effective than previous cybersecurity solutions for contemporary network environments due to its increased accuracy, scalability, and resilience.

## REFERENCES

1. T. M. Mitchell, *Machine Learning*, McGraw-Hill, 1997.
2. C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.
3. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
4. I. Goodfellow et al., "Generative Adversarial Nets," *Advances in Neural Information Processing Systems (NeurIPS)*, 2014.
5. D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning Representations by Back-Propagating Errors," *Nature*, 1986.
6. K. Kendall and K. Kendall, "Intrusion Detection Using Neural Networks and Machine Learning," *Journal of Computer Security*, 1999.
7. W. Lee and S. J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems," *ACM Transactions on Information and System Security*, 2000.
8. M. Tavallaee et al., "A Detailed Analysis of the KDD Cup 99 Data Set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.
9. G. Creech and J. Hu, "A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns," *IEEE Transactions on Computers*, 2014.
10. Y. Bengio, A. Courville, and P. Vincent, "Representation Learning: A Review and New Perspectives," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2013.
11. A. Javaid et al., "A Deep Learning Approach for Network Intrusion Detection System," *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 2016.
12. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," *Military Communications and Information Systems Conference (MilCIS)*, 2015.
13. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, 2018.
14. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, 2010.