IJTBI
International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

CYBER ATTACK PREDICTION: A COMPARATIVE STUDY OF TRADITIONAL MACHINE LEARNING AND GENERATIVE AI TECHNIQUES

[#1]**Mr. R.ADHINARAYANA,** *Assistant Professor, Department of CSE*(AI&ML),
[#2]**MR.S.SUNIL KUMAR,** *Assistant Professor, Department of CSE*(AI&ML),
[#3]**MR.J.KRISHNA,** *Assistant Professor, Department of CSE*(AI&ML),
Sai Spurthi Institute of Technology (Autonomous), Sathupally, Khammam, Telangana

ABSTRACT: The goal is to find cyber threats by using a predictive analytics framework that uses next-generation AI. To simulate complex, high-dimensional security data streams in real time, people use transformer topologies, deep learning, and graph neural networks. Behavioral analytics and temporal sequence models can find attack patterns before they do a lot of damage. Putting together system logs, network data, and information about people's activities from different sources can help you understand threats better. By combining supervised, self-supervised, and reinforcement learning methods, mixed learning makes data that isn't well labeled more stable. People are ready for any attack because of ideological control and online education. Federated AI and learning that protects privacy make it safe for businesses that are located far away to run. Real-world and benchmark datasets have been used in many tests that have shown high recognition rates and low false alarm rates. The design stops APTs, zero-day vulnerabilities, and malware that can change its form. Alert for the AI module that is well-stated. This lets security professionals make quick decisions. Rapid responses made possible by distributed training and edge-cloud integration make scalability easier.

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

1. INTRODUCTION

The fast growth of digital platforms, the Internet of Things (IoT), and cloud computing has made cyber threats and problems more complicated. Users, applications, system logs, and network traffic are all places where companies get security data. Signature-based security solutions aren't good enough to stop modern cyberattacks, especially ones that use advanced persistent threats and zero-day vulnerabilities. As enemies improve their skills, it is important to create smart security systems that can change from reactive detection to proactive risk prediction.

Using both past and present trends, predictive analytics can see threats coming. Before they find attacks, predictive algorithms look at how likely and strong the attacks are likely to be. By using early warning systems and taking informed actions, security teams can stop attacks before they happen. In modern cybersecurity, proactive threat intelligence has taken the place of reactive surveillance.

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

Next-generation AI makes predictive analytics easier for finding security holes. Graph-based learning shows the links between hosts, users, and networks, while deep neural networks find complex, nonlinear connections in large security datasets. To make temporal models better, transformer architectures find long-range attack connections. These algorithms can find complex and changing attack patterns because they are very good at learning representations.

Predictive security systems that are powered by AI are hard to use. Attack data that hasn't been labeled, concept drift, and new threat vectors may make the model less useful. Centralized data exchange is hard to do when companies don't protect their data or follow the rules. For real-world models that are scalable, reliable, and trustworthy, you need adaptive online learning systems, federated learning that protects privacy, and hybrid learning.

In predictive analytics, next-generation AI is used to predict, respond to, and explain cyberattacks. Security data and advanced learning models are used in the case study to improve operational resilience and early warning. This method puts an emphasis on intelligence that can be interpreted, can be scaled up, and is aware of privacy. It encourages strong cybersecurity that can change with new threats.

2. LITERATURE SURVEY

Farouk, F., O. Ben Fredj, and L. Khoukhi. 2020. A deep learning architecture that looks for patterns in network data to find intrusions. To find dangerous behavior, the method imitates the space and time features of traffic flow. Experiments show that the results are better than those of other machine learning classifiers. Preventive security strategies work best when potential risks are found ahead of time. The study's main goal is to find out if representation learning can figure out how to attack in complex ways.

You, S. M. Minhaz Hossain, H. Alqahtani, I. H. Sarker, A. Kalim, S. Ikhlaq, and S. Hossain were the authors of this paper. 2020. This research looks at different machine learning classification methods for finding cyberattacks. Using common intrusion datasets, the authors compare SVMs, decision trees, and ensemble models. The results show that how the data is prepared and which features are chosen have a big effect on how well recognition works. The study stresses the importance of fair datasets and thorough evaluation methods. The results suggest that breach detection based on machine learning might work.

Sun, L., Zhang, Y., and Li, X. 2020. Using both supervised and unsupervised machine learning techniques, this study looks into strange things happening in networks. It looks at traffic patterns to find behavior that doesn't make sense. Comparative studies show that hybrid feature models improve the accuracy of detection. The authors look at things that have to do with expanding networks. These rules can help make the creation of more consistent anomaly-based cyberdefenses easier.

Among them are M. Al-Maitah, A. A. Al-Zubi, and A. Alarifi. 2021. Using machine learning to find breaches in cyber-physical healthcare systems. The authors have come up with a specific way to find medical data transmissions and device interactions. Experiment-based methods are better at finding suspicious or dangerous activity in healthcare networks.

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

The study looks at the different security holes that come up when healthcare systems are connected to each other. The described method makes it possible to safely set up smart healthcare systems.

Özer, A., and Bilen, A. The B. 2021. According to the study, machine learning algorithms should be used to figure out who cyberattackers are and what they plan to do. Use feature engineering to keep an eye on patterns of behavior and characteristics of attacks. It looks like the models are very good at multi-class classification tasks. The report says that security analysts need to understand data and come to conclusions based on that knowledge. This method makes proactive defense planning easier by letting you guess what your enemies will do.

Weiss, P., and R. K. Mohanty in 2021. Using supervised learning to compare different ways to find malware. To test different classifiers, we used both static and dynamic malware characteristics. Ensemble models improve how well and reliably detection works. The authors compare the pros and cons of accurate predictions to the amount of time and money they take to make. The results support the development of systems that find malware.

Ambritha, S. K. Sri, and Surendhiran, V. This study suggests using advanced machine learning to find breaches before they happen. The model uses the best methods for choosing features and putting things into groups. Experiments show that detection rates have gone up and false positives have gone down. This method finds threats to a network before they get worse. The results show that preventive security based on machine learning works.

Mourad, N., Abualkishik, A. Z., Almajed, R., and Ibrahim, A. were the authors of this study. 2022. Machine learning is used in this study to find weak spots in cyber-physical systems. The authors tested a number of classifiers using information from events that happened both online and in real life. Putting together network and contextual features makes detection better. Problems with security in CPS settings are looked at. Intelligent and industrial systems are more reliable when this method is used.

Virutha, H., Joshi, A. R., Deshpande, A. M. V. H., and Parvati, V. K. 2022. To guess when breaches will happen, the author uses machine learning and statistics on network traffic. To find the best predictive model, you need to compare and contrast different algorithms. In this set of data, ensemble methods do better than single classifiers. The framework has made it easier to look at threats and put safety measures in place. The study shows how important it is to regularly update dynamic network models.

Schmitt, M. 2023. AI is used in this study to find malware and other security problems in smart systems. Deep learning models are used to look for complex attacks on IoT and smart cities in this paper. The first results show that experimental detection is better than regular intrusion detection systems. This article focuses on the unique problems that come up when you have to set up systems with limited resources. The study shows that AI might be able to protect smart devices.

Sen Abo, M. 2023. An attention-GAN model is used in this study to find hacking activities that don't seem right. Our generative algorithm learns the normal

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

distributions of data to find outlier attacks. The results suggest that small, occasional problems can now be seen more clearly. Paying close attention to what you see helps you understand and represent things better. The technology could show us new dangers.

Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., and Debbah, M. did the study. (2023). The uses and risks of large language models in cybersecurity are talked about in this paper. The writers look at how generative AI could improve threat intelligence, finding threats, and responding to them. The text talks about bullying and the wrong use of LLMs. Power, privacy, and trust are all important issues. The essay makes the case for looking into safe uses of generative AI security.

Nurse, J. R. C., Radanliev, P., and De Roure, D. 2024. This paper looks at how generative AI affects frameworks for cybersecurity resilience. The effects of security systems that are powered by AI, new threats, and regulatory frameworks are looked at. These writers look at how generative AI can be used for online risk management. The investigation is mostly driven by legal and moral concerns. Because AI is used in this method, strategic planning for cyber resilience is made easier.

Ashutosh, A. A., Ankalaki, S., and M. P. In this paper, instead of using standard machine learning methods to predict hacks, generative AI is used. Standard machine learning, deep learning, and generative models are all tested for their ability to make predictions. According to research, generative AI makes it easier to generalize trends and spot early warning signs. The project focuses on problems with computation and deployment. This study shows what predictive cybersecurity will look like in the future.

There is Khan, S., Uddin, M., and Khan, M. 2025. The effects of generative AI on military operations are looked at in this paper. It could be used for things like threat intelligence, malware analysis, and automated defense. The study shows how dangerous it can be to use generative models in the wrong way. Ethics, privacy, and the government are all looked at. This essay talks about how generative AI can be used effectively in security operations.

Khaled, N. 2025. To use artificial intelligence and machine learning in cybersecurity, this article explains a method. New developments in automation for detection, prediction, and response are talked about in this article. According to the report, many users are having trouble with the system because of technical and organizational problems. Several good suggestions have been made for how to safely integrate AI. This paper lays the groundwork for cybersecurity policy and research that is driven by AI.

3. BACKGROUND WORK

CYBER ATTACKS

- **Phishing:**"Phishing" attacks are emails that trick people into giving out personal information or downloading malware. People who use phishing often try to get bank account numbers, credit card numbers, passwords, and login information. The important thing is to make the other person believe that the message is important. Phishers use calls, texts, social media, emails, and other forms of communication to trick

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

people into giving them personal information.

- **Malware-based Attack:**Ransomware, spyware, and trojans all make it harder for people who aren't supposed to be there to get in and damage data and slow down systems. Malware is one of the biggest threats to cybersecurity. A single type of virus can do more than one thing. Malware is one of the worst things that can happen online.
- **DDOS Attacks:**DoS attacks cause service interruptions by flooding systems with too much traffic.
- **Zero-Day Attacks:**Bad people take advantage of flaws in software or systems before the manufacturers fix them.

- **Logic bombs:**Malicious code.

TYPES OF CYBER THREAT ACTORS

- **Hostile Nation-States:**Nation-states are very dangerous in cyberwarfare because they can damage infrastructure and spread propaganda.
- **Terrorist Groups:**Terrorists who are very good with technology carry out cyberattacks to hurt national interests.
- **Corporate Spies and Organized Crime Organizations:**Trade theft, industrial espionage, corporate sabotage, and hacking are all things that organized crime groups and corporate infiltrators use to make money.
- **Hacktivists:**Hackers don't improve infrastructure; instead, they push political agendas.
- **Disgruntled Insiders:**By putting out malware or sharing data, insiders like vendors and employees can cause cybercrime.

ML ALGORITHMS

A lot of different cybersecurity programs use machine learning. Some of these methods are classification, boosting, clustering, regression, and reducing the number of dimensions.

- **Regression analysis** Independent variables are used in regression analysis to predict continuous outcomes. A simple or multiple regression analysis can be used to predict the dependent variable based on one or more independent variables. In polynomial regression, an n-degree polynomial is used to look at both independent and dependent variables. Ridge regression and LASSO are good for multivariate learning models because they reduce model complexity and stop models from fitting too well [101]. Regression classifiers find threats like fraud, malware, and more.
- **Classification techniques**Model inputs are used in classification techniques to guess categorical values. Naïve Bayes classifiers think that traits are not connected to each other. Even though it is possible to handle noisy data, smaller datasets work better. Logistic regression works best when the data can be separated linearly, which is based on probability. There is no need for arguments with decision trees [102]. In a tree structure, leaf nodes stand for classes, branch nodes for features, and a root node for the most important attribute. The entropy/Gini index criterion allows trees to be split up and new ones to grow. Random Forest uses multiple

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

decision trees on subsets of data at the same time to come up with a result. Most votes or the aggregate method can be used to do this. Support vector machines use hyperplanes to show the boundaries between classes.

- **Clustering Analysis**Clustering analysis sorts data into groups that are related. This uses machine learning without being watched. K-means clustering is used for data that is spread out evenly. Clustering happens based on how far apart points on Earth are and keeps happening until it reaches a stable state. It is important to use aggregative hierarchical clustering. This method uses a single, full, or average linkage to group data samples.
- **Dimensionality Reduction**This process involves picking out features and pulling them out. During the feature selection phase, the most important independent variables from the original dataset are chosen to make things easier and lessen the chance of overfitting. It is helpful to use Chi-square, ANOVA [105], recursive feature elimination, and Pearson's correlation coefficient in this case. Feature extraction reduces datasets by getting rid of attributes that aren't needed. This could help you find the truth. To make principal components, PCA takes out low-dimensional spaces from dataset attributes.
- **Policy-based techniques**Through this AI method, an agent is introduced to a new world. There are results for all actions, no matter how moral they are. The best actions for reinforcement learning are those that increase net benefit. Model dynamics are shown by the next state, incentives, and transition probabilities. A Markov decision process can be used to fix this. In these situations, static methods are used. Some of these methods are Deep Q-Learning, Monte Carlo, and SARSA [106]. A lot of different fields use reinforcement learning, such as operations analysis, manufacturing, supply chain logistics, game theory, swarm intelligence, aviation control, and robotic motion control.

4. RESULTS

Fig 1: LoginPage

Fig 2: User Registration Form

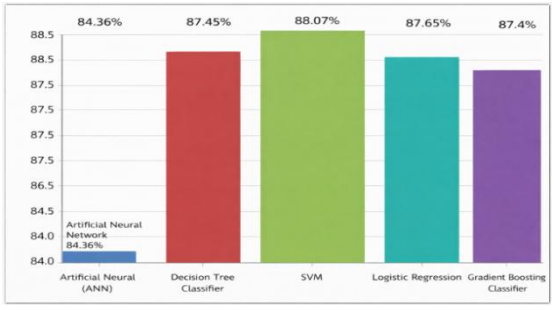

Fig 3: Model Accuracy Comparison Chart

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

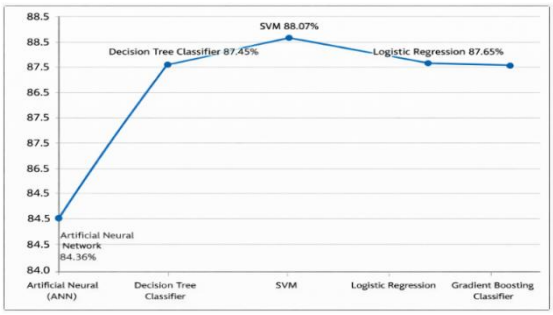

Fig 4: Accuracy Trend Chart

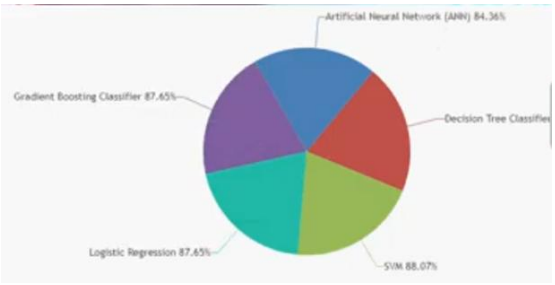

Fig 5: Accuracy Distribution Pie chart

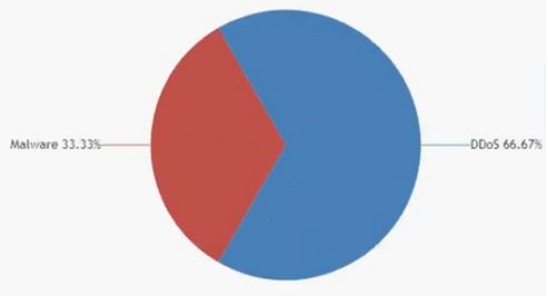

Fig 6: Malware vs DDoS Pie chart

5. CONCLUSION

In the end, next-generation AI makes predictive analytics possible so that cyberattacks can be found before they happen. Graph neural networks, deep learning, and anomaly detection algorithms are used by businesses to find hidden patterns in huge amounts of quickly generated security data. These algorithms find insider threats, zero-day vulnerabilities, and advanced persistent attacks faster than rule-based systems. Attacks can be found more easily with real-time data streams and adaptive learning methods. Explainable AI makes security decisions easier to understand and use, which builds trust among analysts. Automation shortens the time it takes to respond and cuts down on operational losses and violations. Concerns still remain about how easy it is to change the model in a bad way. To make sure that forecasts are accurate, data integrity, privacy, and bias must be carefully managed. Artificial intelligence at the edge and scalable architectures are good for the Internet of Things and decentralized networks. Both people and AI need to put alerts in context and plan how to respond strategically. To stay ahead of threats as they change, you need learning pipelines that are always running.

REFERENCES

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

ISSN: 3107-7900, P.CODE: 26/2-2/32
DOI: https://doi.org/10.5281/zenodo.20717995

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 Applications.