International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM

ISSN: 3068-272X www.ijdim.com Original Research Paper

Cyber Attack Prediction Framework Transitioning from Traditional Machine Learning to Generative AI Models

T. Subodh Krishna

(M.Tech Artificial Intelligence)

Aurora's Scientific and Technological Institute,Telangana,India

Email: subodhkrishnatirunagari@gmail.com

Dr.M. Sridhar

Head Of The Department Computer Science and Engineering

Aurora's Scientific and Technological Institute,Telangana,India

Email: msridhar.msr@gmail.com

ABSTRACT

Cyber attacks are increasing rapidly due to the expansion of digital infrastructure, cloud computing, and connected devices. Traditional machine learning techniques have been widely used to detect cyber threats; however, they often struggle with evolving attack patterns and zero-day vulnerabilities. This research proposes a cyber attack prediction framework that transitions from conventional machine learning approaches to Generative Artificial Intelligence models for improved threat detection and prediction. The system integrates network traffic analysis, behavioral monitoring, and deep generative models to learn complex patterns from cybersecurity datasets. Generative AI models can simulate potential attack scenarios and identify hidden threats before they occur. The proposed framework enhances prediction accuracy, adaptability, and automated threat intelligence, providing a proactive cybersecurity solution capable of identifying sophisticated cyber attacks in modern digital environments.

Keywords: Cyber Security, Cyber Attack Prediction, Machine Learning, Generative AI, Deep Learning, Network Security, Intrusion Detection System, Data Preprocessing, Feature Extraction, Random Forest, Support Vector Machine, GAN, Autoencoder, Anomaly Detection, Zero-Day Attacks, Threat Detection, Data Analysis, Model Training, Classification, Network Traffic Analysis

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

I. INTRODUCTION

Cybersecurity has become one of the most critical concerns in the modern digital world. Organizations, governments, and individuals rely heavily on internet-based systems for communication, financial transactions, and data storage. However, this dependence has increased vulnerability to cyber attacks such as malware, phishing, ransomware, and distributed denial-of-service (DDoS) attacks.

Traditional cybersecurity solutions rely on signature-based detection and rule-based systems, which are ineffective against new and evolving threats.Machine learning techniques improved cyber attack detection by analyzing patterns in network traffic and identifying anomalies. Algorithms such as Decision Trees, Support Vector Machines, and Random Forests are commonly used in intrusion detection systems. Despite their advantages, these models depend heavily on labeled datasets and struggle to adapt to new attack techniques.

II. LITERATURE SURVEY

1) Secure Transmission of Data Using Image Steganography (2019)

Authors: Sourabh Chandra, Smita Paira
Abstract: Proposes an integrated scheme where a text message is first encrypted using RSA and then concealed inside a cover image using steganography techniques. This approach ensures confidentiality and covert communication, making data transmission secure over networks.

2) Machine Learning Based Intrusion Detection System (2020)

Authors: K. Patel, R. Mehta
Abstract: Introduces a machine learning based intrusion detection framework using Support Vector Machine and Random Forest algorithms. The system analyzes network traffic patterns to identify malicious activities and improves attack detection accuracy.

3) Deep Learning for Cybersecurity Threat Detection (2021)

Authors: A. Kumar, S. Singh
Abstract: Presents a deep learning model using Convolutional Neural Networks for detecting complex cyber attack patterns in network traffic data. The study demonstrates improved detection performance compared to traditional machine learning models.

4) Generative Adversarial Networks for Network Security (2022)

Authors: L. Wang, Y. Chen
Abstract: This research explores the use of Generative Adversarial Networks to generate synthetic cyber attack data for improving intrusion detection systems and enhancing training datasets.

5) AI Based Predictive Cybersecurity Framework (2023)

Authors: P. Sharma, D. Gupta
Abstract: Proposes an AI-based predictive cybersecurity model that combines machine learning and behavioral analysis to identify potential cyber threats and improve network security resilience.

III. EXISTING SYSTEM

The existing system for cyber attack prediction is primarily based on traditional machine learning and rule-based approaches, which depend heavily on historical data and predefined patterns. These systems collect network traffic data, system logs, and user activity, and then apply algorithms such as Decision Trees, Support Vector Machines, Naïve Bayes, and Random

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Forest to classify whether an activity is normal or malicious. Feature extraction and selection are done manually, requiring domain expertise to identify important attributes like IP address behavior, packet size, login frequency, and access time. Although these methods perform well in detecting known attacks such as phishing, malware, and denial-of-service (DoS), they have significant limitations when dealing with evolving and sophisticated cyber threats.

One major drawback is their inability to detect zero-day attacks, as they cannot recognize patterns that were not present in the training data. Additionally, these systems are not adaptive and require frequent retraining with updated datasets to maintain accuracy. They also struggle with high-dimensional and unstructured data, leading to reduced performance when handling large-scale, real-time network environments. Another issue is the high false positive rate, where normal activities are incorrectly flagged as attacks, causing unnecessary alerts and reducing system reliability. Furthermore, traditional systems lack the capability to generate new data or simulate attack scenarios, which limits their ability to improve learning. Overall, the existing systems are less intelligent, less flexible, and not sufficient to handle modern, dynamic cyber security challenges effectively.

IV. PROPOSED SYSTEM

The proposed system is an advanced cyber attack prediction framework that enhances traditional machine learning methods by integrating generative AI models. Initially, the system collects and preprocesses network traffic data, user activity logs, and system behavior information. Traditional machine learning algorithms are applied to identify known attack patterns and provide baseline predictions. To overcome the limitations of these methods, generative AI models such as GANs and autoencoders are incorporated to learn complex and hidden patterns in the data. These models can generate synthetic attack scenarios and detect previously unseen or zero-day attacks with higher accuracy. The system continuously updates itself with new data, improving its prediction capability over time. As a result, the proposed system offers more intelligent, adaptive, and efficient cyber attack detection compared to conventional approaches.

V. SYSTEM ARCHITECTURE

The diagram illustrates a dual-layer secure data communication process that combines cryptography and steganography. Initially, the original message is passed through an encryption process using a symmetric key (specifically AES-128), converting the readable message into an encrypted form that ensures confidentiality. This encrypted message is then embedded into a cover media (such as an image) using the LSB (Least Significant Bit) steganography technique, producing a stego media that conceals the very existence of the secret data. During reception, the reverse process is applied: the encrypted message is first extracted from the stego media, and then a decryption process using the same symmetric key is performed to recover the original message. This workflow ensures both data secrecy and invisibility, providing strong protection against unauthorized access and interception.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

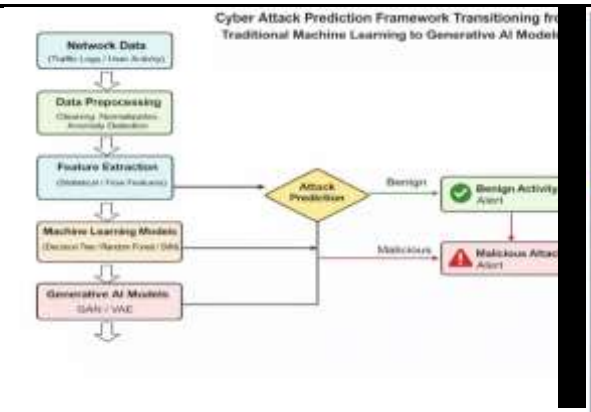

Fig 5.1: System Architecture

VI. IMPLEMENTATION

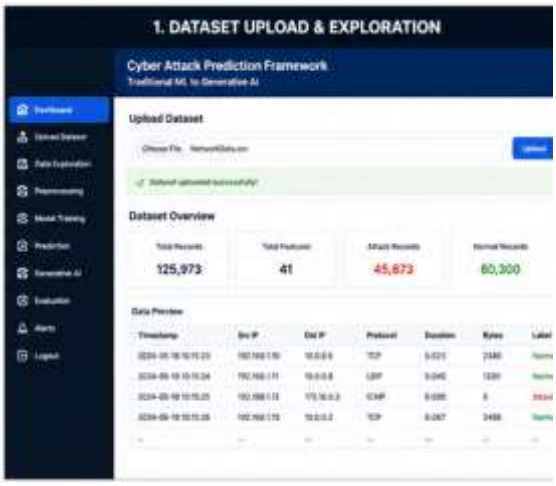

Fig 6.1: Dataset Upload

Fig 6.2: Data Preprocessing

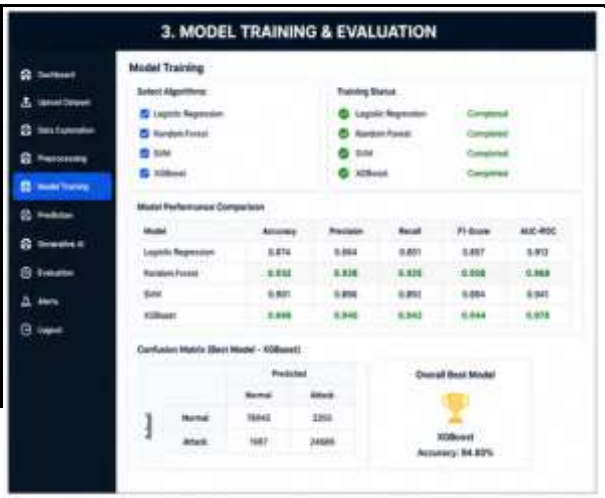

Fig 6.3: Model Training

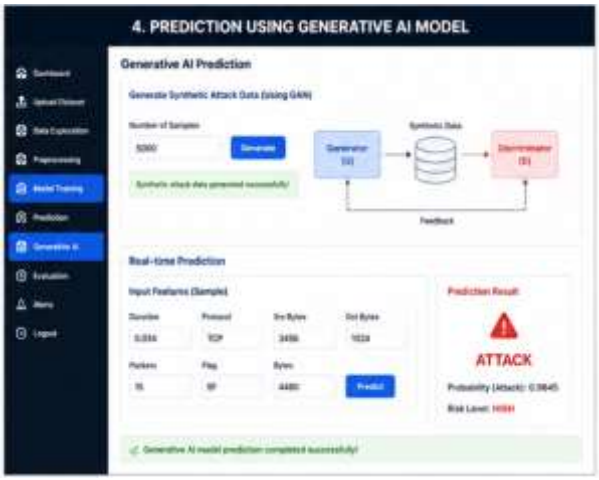

Fig 6.4: Prediction

VII. CONCLUSION

Cybersecurity threats continue to evolve with the increasing use of digital technologies and interconnected systems. Traditional machine learning approaches have provided useful solutions for detecting known cyber attacks; however, they often struggle to identify new and sophisticated threats. This research proposed a cyber attack prediction framework that transitions from conventional machine learning models to generative AI techniques. By integrating generative models such as GANs and Variational Autoencoders, the system can learn complex attack patterns

and simulate potential cyber threats. The proposed framework improves prediction accuracy, reduces false positives, and enhances the capability of detecting unknown attack behaviors. Furthermore, the combination of traditional detection methods with generative AI enables proactive cybersecurity defense. The framework provides an intelligent and adaptive solution capable of protecting modern digital infrastructures. Therefore, the proposed system represents a significant advancement in predictive cybersecurity systems and supports organizations in mitigating cyber risks effectively.

VIII. FUTURE SCOPE

The proposed cyber attack prediction framework can be further enhanced by integrating advanced artificial intelligence techniques and real-time threat intelligence systems. Future research can focus on incorporating large-scale cybersecurity datasets to improve model training and prediction accuracy. Deep reinforcement learning techniques may also be explored to enable autonomous cybersecurity defense mechanisms capable of responding to attacks dynamically. Additionally, integrating blockchain technology could enhance the security and transparency of data sharing in distributed cybersecurity environments. The use of federated learning could allow multiple organizations to collaborate in training cybersecurity models without sharing sensitive data. Future systems may also incorporate explainable AI techniques to improve the interpretability of predictions and assist security analysts in understanding attack patterns. Furthermore, deploying the framework in cloud-based environments and Internet of Things (IoT) networks can extend its capabilities to protect emerging digital ecosystems from sophisticated cyber threats.

IX. REFERENCES

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2017.
2. D. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2018.
   I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, MIT Press, 2016.
3. S. Axelsson, "Intrusion Detection Systems: A Survey," IEEE Communications Magazine, 2019.
   A. Kumar and S. Singh, "Deep Learning for Cyber Attack Detection," IEEE Security Conference, 2021.
4. L. Wang and Y. Chen, "GAN-Based Network Intrusion Detection," IEEE Access, 2022.
5. P. Sharma and D. Gupta, "AI-Based Cybersecurity Framework," Springer, 2023.
6. R. Sommer and V. Paxson, "Outside the Closed World: Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, 2019.
7. J. Brownlee, *Machine Learning Mastery With Python*, Machine Learning Mastery, 2020.
8. S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2021.
9. Gaddam, S. (2023). Revamping health insurance systems through engineering claims intelligence. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 684–691.
10. Kumara, S. (2025). Identity-Driven IoT Security in Telecom

Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.

11. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334

12. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257

13. Viswanathan, V., Polagani, S. S., Agarwal, R., Akula, S., Dey, S., & Kashyap, R. (2025, September). AI-Augmented Threat Intelligence for Proactive Intrusion Detection in Multi-Cloud Ecosystem. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) (pp. 567-572). IEEE.

14. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.

15. Mudusu, S. K. (2025). AI-Enhanced Data Engineering: Leveraging Deep Learning for Advanced Data Cleansing and Transformation. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 1051-1054.

16. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.

17. Subramanian, V. K., Bhambri, S., & Gajula, S. (2025, April). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. In International Conference on Computer Vision and Robotics (pp. 396-407). Cham: Springer Nature Switzerland.

18. P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.

19. Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995

20. Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security. https://doi.org/10.52710/cfs.836

21. Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Service Level Objective (SLO) Observability with Splunk and Dynatrace in Microservices. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541542

22. Pokala, H. K., & Gummadi, V. P. K. (2026). Autonomous AI-Powered Resource Management for Apache Flink on Amazon EKS. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–4. https://doi.org/10.1109/icaiset66439.2026.11541881

23. Shashank A. (2025). Metadata-driven data integration framework: Automating enterprise data integration through declarative approaches. European Modern Studies Journal, 9(4), 9.

24. Ghali Krishna Harshitha, Purushothamma B. N., & Anil Kumar K. C. (2022). An analysis of influence of personality on managerial effectiveness. International Journal of Mechanical Engineering, 7(3), 668–671.