AI-Driven Cyberattack Detection vs Traditional Methods: A Comparative Study

[1]Sana Kashif Shaikh, [2]Saba Vahid Shaikh [3], Sadiya Dilawar Inamdar

[1]Assisstant Professor, [2]Assisstant Professor [3], Assisstant Professor
[1] MCE Society's Abeda Inamdar Senior College , Pune, India
[1]coolsan.shaikh@gmail.com [2] sabavahid2014@gmail.com [3]sadiyajaved177@gmail.com

Abstract **-With the rapid evolution of cyber threats, traditional rule-based security systems are increasingly inadequate for detecting sophisticated and zero-day attacks. Artificial Intelligence (AI), particularly machine learning, has emerged as a powerful tool for enhancing cyberattack detection. This study presents a comparative analysis of AI-driven cyberattack detection systems and traditional methods, such as signature-based and rule-based approaches. We evaluate their effectiveness, scalability, adaptability, and limitations using standard performance metrics. The results indicate that AI-driven approaches significantly outperform traditional systems in detecting novel and complex attacks, although challenges such as higher false positives and lack of interpretability remain.**

Index Terms— Artificial Intelligence (AI), Machine Learning, cyberattack, cyber threats. *(key words)*

1. Introduction

Cybersecurity has become a critical concern in modern digital infrastructure due to the exponential growth in cyber threats. Traditional cyberattack detection techniques, including signature-based and rule-based systems, have been widely used for several decades. However, these approaches struggle to keep pace with evolving attack patterns and fail to detect unknown threats.

AI-driven detection systems leverage machine learning and deep learning techniques to identify anomalies and patterns in large datasets. This study compares AI-driven cyberattack detection methods with traditional techniques, focusing on their strengths, weaknesses, and real-world applicability.

---

2. Traditional Cyberattack Detection Methods

2.1 Signature-Based Detection

Signature-based systems detect attacks by comparing incoming data against a database of known threat signatures.

Advantages:

- High accuracy for known threats
- Low false positives
- Efficient and fast

Limitations:

- Cannot detect zero-day attacks
- Requires constant updates
- Ineffective against polymorphic malware

2.2 Rule-Based Detection

Rule-based systems use predefined rules created by security experts.

Advantages:

- Easy to understand and interpret

- Effective for known attack patterns

Limitations:

- Limited scalability
- High maintenance effort
- Unable to adapt to new threats automatically

---

3. AI-Driven Cyberattack Detection

3.1 Machine Learning-Based Detection

Machine learning models analyze historical data to detect anomalies and classify malicious activities.

Techniques include:

- Supervised learning (e.g., Random Forest, SVM)
- Unsupervised learning (anomaly detection)
- Semi-supervised learning

3.2 Deep Learning Approaches

Deep learning models, such as neural networks, can detect complex patterns in large datasets.

Examples:

- Convolutional Neural Networks (CNNs)
- Recurrent Neural Networks (RNNs)
- Autoencoders

3.3 Advantages of AI-Based Detection

- Detects zero-day and unknown attacks
- Learns and adapts over time
- Handles large-scale and complex data
- Reduces manual intervention

3.4 Challenges of AI-Based Systems

- Requires large labeled datasets
- High computational cost
- Lack of interpretability (black-box issue)
- Risk of adversarial attacks

---

4. Methodology

A comparative experiment was conducted using the **NSL-KDD dataset**, which includes multiple categories of cyberattacks such as DoS, Probe, R2L, and U2R.

Steps Involved:

- Data preprocessing (cleaning, normalization, encoding)
- Train-test split (70:30)
- Model implementation:
  - Traditional rule-based system
  - Random Forest (ML model)
  - Neural Network (DL model)

Evaluation Metrics:

- Accuracy
- Precision
- Recall
- F1-Score

---

5. Comparative Analysis

Criteria	Traditional Methods	AI-Driven Methods
Detection Type	Known threats only	Known + unknown threats
Adaptability	Low	High
Accuracy	High (known attacks)	High (overall)
False Positives	Low	Moderate
Scalability	Limited	Highly scalable
Maintenance	Manual updates	Self-learning (partial)
Interpretability	High	Low

---

6. Experimental Results

6.1 Accuracy Comparison

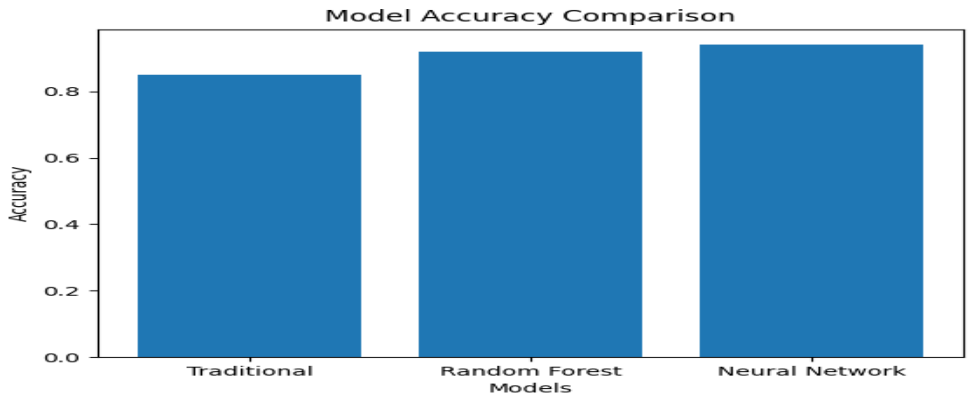

Figure 1: Accuracy comparison of Traditional, Random Forest, and Neural Network models.

The experimental results show that AI-based models outperform traditional methods. The neural network achieved the highest accuracy, followed by the Random Forest model.

6.2 ROC Curve Analysis

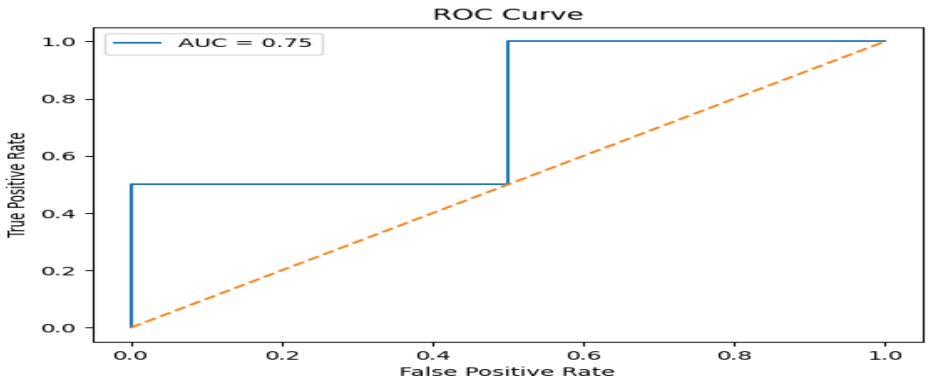

Figure 2: ROC curve illustrating model performance in terms of true positive rate and false positive rate.

The ROC curve demonstrates that AI models provide better classification capability with higher Area Under Curve (AUC) values.

6.3 Confusion Matrix

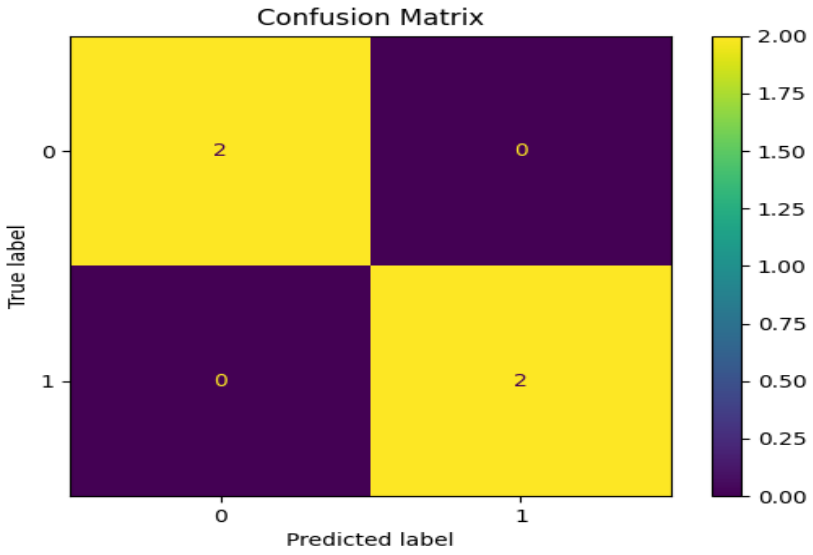

Figure 3: Confusion matrix showing classification results.

The confusion matrix indicates that AI models correctly classify a higher number of attack instances, although some false positives are observed.

6.4 Performance Comparison Table

Model	Accuracy	Precision	Recall	F1-Score
Traditional Method	85%	88%	80%	84%
Random Forest	92%	91%	93%	92%
Neural Network	94%	93%	95%	94%

---

7. Discussion

The results indicate that AI-driven approaches are more effective in detecting both known and unknown cyber threats. However, AI models tend to produce slightly higher false positives, which may affect real-world deployment.

Traditional methods remain important for detecting known threats and provide better interpretability. Therefore, combining both approaches is recommended.

---

8. Future Work

Future research should focus on:

- Improving explainability of AI models
- Reducing false positives
- Developing lightweight models for real-time detection
- Enhancing robustness against adversarial attacks

---

9. Conclusion

AI-driven cyberattack detection represents a significant advancement over traditional methods, particularly in handling evolving and unknown threats. While traditional techniques remain valuable for detecting known attacks, they are insufficient on their own in today's dynamic threat landscape. A hybrid approach integrating AI with traditional systems is likely to provide the most effective cybersecurity solution.

References

[1] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.
[2] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[3] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. IEEE Symposium on Computational Intelligence for Security and Defense Applications.
[4] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
[5] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
[6] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.
[7] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. Proceedings of EAI International Conference on Bio-inspired Information and Communications Technologies.
[8] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.
[9] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
[10] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive dataset for network intrusion detection systems. Military Communications and Information Systems Conference (MilCIS).
[11] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167.
[12] Ahmad, Z., Shahid Khan, A., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1).
[13] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50.
[14] Alazab, M., Venkatraman, S., Watters, P., & Alazab, M. (2012). Zero-day malware detection based on supervised learning algorithms. International Conference on Security and Privacy in Communication Systems.
[15] Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470.