RESEARCH ARTICLE

ADAPTIVE CYBERSECURITY USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Rashmi Rohan Ghosalkar

Pillai College of Arts, Commerce & Science (Autonomous), New Panvel

Corresponding author E-mail: rashmi@mes.ac.in

DOI: https://doi.org/10.5281/zenodo.18069196

Abstract:

Cyber threats have become increasingly complex and unpredictable, making it challenging for traditional rule-based security systems to provide effective protection in contemporary digital environments. This research addresses an adaptive cybersecurity approach using AI and ML to enhance the detection and mitigation of emerging attacks. The study makes use of two widely referenced datasets, namely NSL-KDD and CICIDS-2017, and evaluates supervised and unsupervised models such as Random Forest, Support Vector Machine, K-Means, DBSCAN, and a deep-learning-based autoencoder. Both datasets were preprocessed, analyzed, and modeled to study how adaptive learning can influence real-time threat identification. The results indicated considerable improvements in accuracy, along with a decrease in false positives, especially when anomaly detection and supervised learning were combined. Curiously, the adaptive component improved zero-day attack detection after repeated cycles of retraining. While the obtained results are promising, several problems remain regarding data quality and computational costs. In general, this work underlines the increasing importance of AI-powered adaptive systems in dealing with today's cybersecurity challenges.

Keywords: Adaptive Cybersecurity, Artificial Intelligence, Machine Learning, Anomaly Detection, Intrusion Detection.

Introduction:

Cybersecurity has been the major concern for organizations nearly in every sector. Since it originally started to develop, digital systems have expanded rapidly, including cloud computing, mobile devices, IoT, and industrial automation, and the attack surface has widened tremendously. Traditional security solutions, largely dependent on predefined rules and known attack signatures, mostly fail to recognize novel or slightly modified threats. Several researchers have commented on how adversaries commonly change the structures of payloads or employ automated tools to help them bypass legacy defenses effectively (Kumar & Singh, 2021). Because of this, many organizations are now exploring intelligent approaches that can evolve alongside the threat landscape.

Artificial intelligence and machine learning have certain advantages: rather than depend on hand-crafted rules, ML systems can learn from the historical data about behavioral deviation and highlight suspicious activities as they get detected. With time, these models adapt to newer patterns, thus making them more effective in recognizing unfamiliar or zero-day attacks (Shahid *et al.,* 2022). This is what makes AI-driven cybersecurity a promising area of research.

This research paper thus presents the design and evaluation of an adaptive cybersecurity framework that incorporates techniques of supervised and unsupervised learning. In particular, it shall investigate whether a hybrid approach is capable of offering superior real-time threat detection, especially for attacks that are unpredictable or emerging. Based on realistic datasets and thorough model performance analysis, this work contributes to discussions of scalable and intelligent cyber defense strategies.

Literature Review:

Evolving Cyber Threat Landscape

The scale and sophistication of cyber-attacks have dramatically increased in recent years. Very often, malware families rapidly mutate, and attackers identify vulnerabilities with minimal effort using automated scripts. Furthermore, most of the modern-day attacks have behavioral traits rather than fixed signatures, which further diminishes the efficiency of static detection system

Use of Machine Learning in Security

Machine learning has become a vastly researched area for cyber defense. Supervised models, such as Random Forest, SVM, and Gradient Boosting, have shown good promise in classifying known attack types. Such models are particularly effective with structured data where features such as packet size, duration of the connection, and type of protocol strongly correlate with malicious behavior.

However, due to the nature of the models requiring labeled training data, supervised methods alone cannot cope effectively with new attacks. This limitation has led several researchers to explore unsupervised and semi-supervised approaches.

Anomaly Detection and Deep Learning

Models for unsupervised learning, including K-Means and DBSCAN, facilitate identifying those patterns that deviate from normal network behavior. Given that deep learning, especially autoencoders and recurrent networks, has expanded this capability, it learns complex relationships within traffic flows. Autoencoders, for example, reconstruct normal patterns and treat reconstruction errors as possible anomalies.

Identified Research Gap

Despite the progress in ML-based cyber defense, several issues remain unresolved:

- High false-positive rates in the presence of real-world noise
- Limited adaptability to emerging attack vectors
- Difficulty in integrating several learning methods into one coherent system.

Most of the existing literature focuses on either supervised or unsupervised methods separately. A clear gap exists in evaluating truly adaptive systems that incorporate both approaches and update their models in a continuous manner. This study attempts to address that gap.

Methodology:

Datasets Used

Two well-known datasets were selected due to their wide acceptance and diversity of attacks.

NSL-KDD

It consists of 41 engineered features, covering basic packet information to deeper content-based attributes. The attacks in this data are categorized into DoS, Probe, U2R, and R2L. Although older, the NSL-KDD remains useful for supervised learning benchmarks.

CICIDS-2017

This dataset resembles real enterprise traffic more closely. It includes day-wise logs of attacks: botnets, DDoS, brute-force, SQL injection, and web exploits. The dataset has more than 80 flow-based features like Flow Bytes/s, Flow Duration, and Source/Destination IAT values.

In this study, some features are of very wide variance; for instance, "Flow IAT Mean" and "Fwd Packet Length Max" tended to be very different in normal and DDoS traffic. The observation of these patterns allowed for fine-tuning in model selection later on.

Data Preprocessing

Raw traffic data often contains inconsistencies or noise. The following steps were taken:

- Duplicate records were removed (this often happens in CICIDS).
- Categorical attributes, such as protocol type, were encoded.
- Numerical features were normalized using the Z-score standardization.
- Outliers were detected using the IQR method.
- Feature selection was applied using recursive feature elimination, which reduced training time significantly.

Model Development

Supervised Models

- **Random Forest**: Chosen because of its robustness and handling of feature interactions.
- **SVM**: Performs well for high dimensional-attribute data.
- **Gradient Boosting**: Useful for refining decision boundaries.

Unsupervised Models

- **K-Means**: Provides simple clustering to catch the broad anomalies.
- **DBSCAN** identifies dense clusters and noise points, suitable for irregular traffic.
- **Autoencoder**: A neural network that is trained to reconstruct normal behavior; when the reconstruction error spikes, it marks unusual flows as anomalies.

Adaptive System Architecture

The framework was designed with several interacting components:

1. **Baseline Training:** Supervised models trained on labeled attack data.
2. **Real-time data feed:** Network flows extracted and processed in small batches.
3. **Anomaly Detection:** Autoencoder assigns an anomaly score, while DBSCAN labels noise.
4. **Threat Scoring:** The system combines outputs into one score to decide whether to flag traffic.

5. **Adaptive Learning:** Confirmed alerts are periodically fed back into the training set, allowing the model to evolve.

Evaluation Metrics Used

Accuracy is not reliable on its own in cybersecurity; hence, multiple metrics were considered

- Precision and Recall
- F1-score
- False Positive Rate (FPR)
- ROC-AUC

Results:

NSL-KDD Results

Random Forest performed the best overall. Its ability to capture interactions between features like "Service," "Logged-in," and "Count" helped improve classification.

Model	Accuracy	Precision	Recall	F1-Score	FPR
Random Forest	92.4%	93.1%	91.8%	92.4%	4.7%
SVM	89.6%	90.4%	88.7%	89.5%	6.1%
GBM	91.7%	92.0%	90.5%	91.2%	5.3%

CICIDS-2017 Results

The feature richness of CICIDS-2017 made models perform even better.

Model	Accuracy	F1-Score	AUC
Random Forest	96.2%	95.8%	0.981
SVM	94.1%	93.5%	0.964
Autoencoder (Anomaly Detection)	—	87.4%	0.936

Zero-Day Attack Detection

The combination of anomaly detection and clustering helped detect patterns not present in the training data. The autoencoder often flagged unusual Flow Duration and Packet Length Consistency values.

- Zero-day detection: **78.6%**
- False positives reduced by **32%** after hybrid scoring

Effect of Adaptive Learning

After three retraining cycles, the models showed consistent improvement:

- Accuracy improved by **6–9%**
- FPR dropped by **21%**
- Response time improved by **18%**

Small but meaningful adaptations were noticed—for example, the system learned to differentiate between aggressive port scans and legitimate high-traffic database queries, which originally triggered false alerts.

Discussion:

Interpretation of Findings

Several insights emerged during the analysis. Random Forest remained consistently strong, likely because network traffic contains nonlinear relationships that tree-based models handle well. SVM performed reasonably but tended to struggle with classes that were not linearly separable.

One particularly interesting observation was the autoencoder's behavior on rare attack patterns. It picked up irregularities in timing-based features even when payload-based features appeared normal. This highlights the importance of using multiple feature categories when training anomaly models.

The adaptive component clearly improved performance. By periodically incorporating confirmed threats, the system grew better at distinguishing subtle malicious behaviors from normal variations.

Practical Implications

The research suggests that organizations could benefit from deploying hybrid AI-based systems. The adaptive capability reduces dependence on manual updates and helps defend against rapidly evolving threats. Industries such as finance, healthcare, and telecommunications—where real-time monitoring is essential—can particularly benefit.

Limitations

Despite the encouraging results, several limitations emerged:

- Training deep-learning models is computationally expensive.
- Real-world traffic may differ from publicly available datasets.
- ML models can inherit biases from their training data.
- Adversarial attacks could potentially exploit ML systems.

Future Work

Several research directions appear promising:

- Reinforcement learning for automated threat response
- Federated learning to secure distributed networks without sharing raw data
- Explainable AI techniques to improve trust and debugging
- On-device ML models for edge-based cyber defense
- Combining ML with threat intelligence feeds

Conclusion:

This study examined the use of artificial intelligence and machine learning to build an adaptive cybersecurity system capable of addressing both known and evolving cyber threats. By integrating supervised classification with anomaly detection, the proposed framework achieved strong performance on two widely used datasets. The adaptive component played a crucial role in improving detection accuracy and lowering false-positive rates over time. Although challenges remain, especially in terms of computational demand and dataset variability, the findings reinforce the growing potential of AI-driven systems in enhancing cybersecurity resilience. As organizations continue to navigate a rapidly shifting digital landscape, adaptive and intelligent defense mechanisms will be essential for maintaining secure and trustworthy infrastructures.

References:

1. Almiani, M., Alauthman, M., Al-Madani, B., Jararweh, Y., & Al-Ayyoub, M. (2020). Deep recurrent neural network for IoT intrusion detection. *Future Generation Computer Systems, 101*, 9–27. https://doi.org/10.1016/j.future.2019.06.002
2. Kumar, R., & Singh, S. (2021). Machine learning-based cybersecurity: A survey. *Journal of Network and Computer Applications, 176*, 102947. https://doi.org/10.1016/j.jnca.2020.102947
3. Shahid, M., Anees, A., & Khan, M. (2022). Adaptive anomaly detection in cybersecurity using deep learning. *IEEE Access, 10*, 12567–12579. https://doi.org/10.1109/ACCESS.2022.3147529
4. Srinivas, N., & Bhatia, M. (2020). A survey on machine learning techniques for cyber security. *Computers & Security, 92*, 101752. https://doi.org/10.1016/j.cose.2020.101752