myresearchgo

myresearchgo Volume 1, June Issue 4, 2025, ISSN: 3107-3816 (Online)

The use of Artificial Intelligence to improve Intrusion Detection and Prevention Systems

Mrs.Vandana Nainesh Chaurasia[1],
Assistant Professor in V.K.K. Menon College, Bhandup (East)
Mrs.Kalpana Dinesh Bandebuche[2],
Assistant Professor in V.K.K. Menon College, Bhandup (East)
Mr. Shriyans Dinesh Bandebuche[3]
Indala College Of Engineering, Kalyan

Abstract

With cyber threats evolving constantly, it's essential to safeguard network systems using Intrusion Detection and Prevention Systems (IDPS). Traditional IDPS approaches, such as signature and anomaly-based methods, often fall short when confronting complex attacks like APTs, polymorphic malware, or zero-day threats. One of the key drawbacks of these methods is their tendency to generate too many false alerts and their limited adaptability to unknown or subtle threats. One of the key drawbacks of these methods is their tendency to generate too many false alerts and their limited adaptability to unknown or subtle threats. This paper explores the use of AI to improve IDPS's proactive response capabilities as well as its detection accuracy. Without depending exclusively on predetermined signatures, AI-based IDPS can independently learn from vast network data, spot subtle irregularities, and uncover suspicious patterns linked to cyberattacks. AI-based IDPS can independently learn from vast network data, spot subtle irregularities, and uncover suspicious patterns linked to cyberattacks. We also go over the difficulties in putting AI-driven IDPS into practice, including the requirement for huge datasets, problems with interpretability, and the possibility of adversarial assaults on AI models. In conclusion, we suggest avenues for further research, such as hybrid approaches integrating AI with conventional techniques, employing AI for threat intelligence prediction, and creating more transparent and comprehensible AI models for cybersecurity.

The results of this study demonstrate the revolutionary potential of AI in creating IDPS that are more intelligent, adaptable, and resilient and that can successfully counteract the ever-changing nature of modern cyber threats.

Keywords: Artificial Intelligence (AI), Intrusion Detection and Prevention Systems (IDPS), Machine Learning (ML), Deep Learning (DL), Cybersecurity, Anomaly Detection.

Key aspects of Literature review

Although traditional IDPS techniques have been crucial to cybersecurity, they are becoming less and less effective in combating the intricacy and sophistication of contemporary cyberthreats. Their efficacy is limited by their reliance on static detection techniques, incapacity to identify novel or evolving assaults, and difficulties with scalability, false positives, and real-time reaction. These drawbacks show that in order to meet the increasing needs of contemporary network security, more intelligent, adaptable systems—like those driven by artificial intelligence (AI)—are required.

Problem under investigation or research Questions

1. How could AI increase the precision of systems for preventing and detecting intrusions?
2. What are the advantages of utilizing AI in IDPS for real-time threat detection and reaction?
3. How can advanced persistent threats (APTs) and zero-day assaults be detected by AI-based IDPS?
4. How difficult is it to incorporate AI into the IDPS frameworks that are already in place?
5. How might artificial intelligence improve IDPS's scalability in expansive and dynamic network environments?
6. How may AI-based IDPS be affected by adversarial attacks?
7. How does AI integration in IDPS enhance the understanding and traceability of model predictions and decisions?
8. What are the best methods for implementing AI-powered IDPS in various network settings (such as on-premises, cloud, and IoT)?

Hypothesis

"Integrating machine learning algorithms into Intrusion Detection and Prevention Systems will enhance their ability to detect and respond to unknown and emerging cyber threats more effectively than traditional rule-based systems."

Approaches adopted

1. Data Collection and Preprocessing

Data Collection

- **Source Identification** To build effective models, researchers collect data from sources:
  - Open-access datasets (like KDD 1999 and CICIDS).
  - Real-time traffic logs from companies.
  - Honeypots that intentionally capture malicious behaviour.

Preprocessing Techniques

- **Data Cleaning**: Refers to the process of eliminating duplicate records, fixing inaccuracies, and discarding data that is not relevant.
- **Handling Missing Values**: Techniques such as mean/mode imputation, interpolation, or removing incomplete records are used.
- **Normalization/Standardization** To maintain uniform input for machine learning models, features are often scaled using methods like Min-Max or Z-score normalization.

2. Feature Engineering

Feature Selection

- **Correlation Analysis**: Identifying features that have a strong correlation with the target variable (e.g., attack labels) using techniques like Pearson's correlation.

- **Feature Importance**: Employing methods such as Random Forest importance scores or Recursive Feature Elimination (RFE) to select significant features that contribute to model performance.

Dimensionality Reduction

- **Principal Component Analysis (PCA)**: PCA helps simplify complex datasets by reducing their dimensions but keeping most of the critical information intact.
- **t-Distributed Stochastic Neighbour Embedding (t-SNE)**: Visualizing high-dimensional data in two or three dimensions to identify clusters of normal and malicious behaviour.

3. Model Development

Machine Learning Algorithms

- **Supervised Learning**: Algorithms trained on labeled datasets:
  - **Decision Trees**: Simple, interpretable models that split data based on feature values.
  - **Random Forests**: An ensemble of decision trees to improve accuracy and reduce overfitting.
  - **Support Vector Machines (SVM)**: Work particularly well when classifying data into two categories, even in cases where there are many features.
- **Unsupervised Learning**: Identifying patterns in unlabeled data:
  - **Clustering**: Techniques like k-means and DBSCAN to group similar data points and identify outliers.
  - **Isolation Forest**: Specifically designed for anomaly detection by isolating anomalies instead of profiling normal data.
- **Semi-supervised Learning**: Combining labeled and unlabeled data to enhance learning. It proves useful when there is a shortage of annotated data.

4. Deep Learning Approaches

Neural Networks

- **Feedforward Neural Networks**: Basic neural networks where information moves in one direction, useful for simple classification tasks.
- **Convolutional Neural Networks (CNNs)**: Effective for pattern recognition in structured data, such as image-like inputs derived from network traffic.
- **Recurrent Neural Networks (RNNs)**: Suitable for sequential data, capturing temporal dependencies in network traffic over time.

Autoencoders

- **Training Autoencoders**: Autoencoders learn to condense and rebuild input data. If the model struggles to accurately recreate certain inputs, those may be flagged as suspicious.

5. Evaluation Metrics

Performance Evaluation

- **Accuracy**: Measures the proportion of correct predictions out of all predictions made.
- **Precision and Recall**:
  - **Precision** measures the accuracy of positive predictions.
  - **Recall** indicates how effectively the model identifies all relevant or actual positive cases.
- **F1-Score:** Strikes a balance between precision and recall, offering a single measure of a model's performance.
- **ROC-AUC**: Reflects the area under the Receiver Operating Characteristic curve and assesses the model's skill in separating different classes.

Confusion Matrix

- By examining the confusion matrix, researchers can assess true positives, false positives, true negatives, and false negatives to better understand how the model performs.

6. Testing and Validation

Cross-validation

- **k-Fold Cross-validation**: Dividing the dataset into k subsets and training the model k times, each time using a different subset as the test set and the remaining as the training set.

Stress Testing

- By mimicking different cyberattack scenarios—like DDoS or SQL injection—researchers can test how resilient the IDPS is under pressure.

7. Implementation and Integration

Prototype Development

- **System Architecture**: Designing a prototype that integrates AI models into existing IDPS frameworks, ensuring compatibility and scalability.

Real-time Processing

- **Stream Processing**: Implementing systems that can analyze incoming data streams in real-time, using frameworks like Apache Kafka or Apache Flink for scalability and efficiency.

8. User Feedback and Iteration

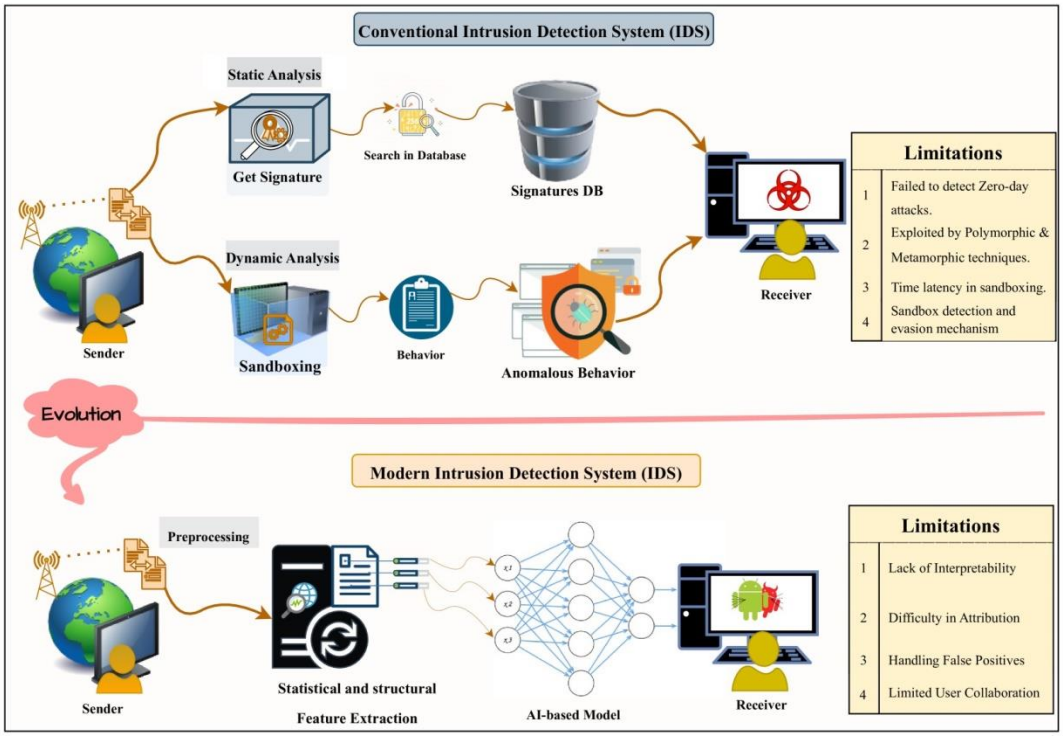
Feedback Loop

- **Analyst Input**: Incorporating feedback from security analysts who review alerts and false positives to refine models, focusing on specific types of attacks.

Continuous Learning

- **Model Updating**: Regularly retraining models with new data to adapt to evolving threat landscapes, using techniques such as transfer learning to leverage existing models.

Results of Implementing AI in Intrusion Detection and Prevention Systems (IDPS)



Modern Intrusion Detection Systems Fig. [1]

1. **Improved Detection Rates**
   - **Higher True Positive Rates**: Compared to older systems, AI-powered IDPS are better at correctly identifying genuine threats, reducing the chance of missing a real attack.
   - **Broader Threat Detection**: The ability to recognize a wide variety of attacks (e.g., zero-day vulnerabilities, advanced persistent threats) that traditional methods may miss.
2. **Reduced False Positives**

- **Lower Alarm Fatigue**: Since AI can better tell harmless actions from actual threats, it triggers fewer unnecessary alerts, saving time and effort. .
- **Enhanced Trust in Alerts**: Security personnel can trust the alerts generated by the system, leading to quicker and more efficient incident response.

3. **Faster Response Times**
   - **Automated Threat Mitigation**: AI can automate responses to detected threats, such as blocking suspicious IP addresses or isolating infected devices, which leads to quicker containment of incidents.
   - **Proactive Defence**: Real-time analysis allows for proactive measures rather than reactive responses to security incidents.
4. **Adaptive Learning**
   - **Dynamic Adaptation**: AI systems keep learning as new data comes in, which helps them stay updated and responsive to changing attack methods.
   - **Behavioural Insights**: AI systems provide deeper insights into user behavior, enabling organizations to identify potential insider threats or policy violations.
5. **Cost Efficiency**
   - **Reduced Operational Costs**: By minimizing the time security teams spend on false positives and repetitive tasks, organizations can optimize their resources and reduce operational costs.
   - **Enhanced Resource Allocation**: With automated responses and accurate detections, teams can focus on strategic initiatives rather than routine monitoring.
6. **Comprehensive Security Posture**
   - **Holistic Threat Coverage**: AI systems can analyse multiple data points and attack vectors, providing a comprehensive view of the security landscape.
   - **Integration with Other Security Tools**: AI-enhanced IDPS can work in conjunction with firewalls, SIEM systems, and endpoint protection solutions to create a robust security framework.

Implications of AI-Enhanced IDPS

1. **Security Strategy Evolution**
   - **Shift to Proactive Security**: With smarter tools like AI-based IDPS, companies can take preventive action against threats instead of just reacting after an attack.
   - **Continuous Improvement**: The ability to adapt and learn over time necessitates a culture of continuous improvement in security practices.
2. **Regulatory Compliance**
   - **Enhanced Compliance**: Improved detection and reporting capabilities can help organizations meet regulatory requirements related to data protection and breach notification.
   - **Documentation and Auditing**: AI systems can provide detailed logs and reports, facilitating audits and compliance assessments.
3. **Skills and Training Needs**
   - **Up skilling Workforce**: As AI technologies become integral to security operations, there will be a greater need for cybersecurity professionals to have skills in AI, machine learning, and data analysis.
   - **Change in Roles**: The roles of security analysts may evolve from detection and monitoring to focusing on interpreting AI insights and strategic decision-making.
4. **Ethical Considerations**

- **Privacy Concerns**: The use of AI in monitoring and analyzing user behavior raises privacy concerns, necessitating transparent practices and compliance with data protection laws.
- **Bias and Fairness**: If not carefully managed, AI systems might pick up biases from the data they're trained on, which could lead to unfair or inaccurate results.

5. **Investment and Resource Allocation**
   - **Increased Investment in AI**: Organizations may need to invest in AI technologies, tools, and training, leading to a shift in budget priorities.
   - **Long-Term Commitment**: Bringing AI into cybersecurity isn't just a quick fix—it's a long-term commitment that involves consistent upgrades, learning, and fine-tuning.

References:

Books

1) **"Machine Learning and Security: Protecting Systems with Data and Algorithms"**
By Clarence Chio and David Freeman
This book explores various machine learning techniques and their applications in enhancing cybersecurity, including intrusion detection systems.

2)**"Artificial Intelligence for Cybersecurity: A Practical Guide"**
By A. D. Keromytis and V. K. Gupta
This book offers a comprehensive overview of how AI can be integrated into cybersecurity practices, focusing on threat detection and response.

Conference Papers

1) **M. S. A. A. R. Shaligram, "A Survey on Intrusion Detection System Based on Machine Learning,"**
Proceedings of the 2019 IEEE International Conference on Computer Communication and Control Technology (I4CT), pp. 184-189, 2019.
This paper presents a survey of machine learning techniques for intrusion detection systems.
2) **A. D. V. K. B. K. B. S. K. G. Manogaran, "Intrusion Detection Systems using Deep Learning: A Review,"**
Proceedings of the 2020 International Conference on Computer Communication and Control Technology (I4CT), pp. 191-196, 2020.

Image source :

Fig[1] - https://arxiv.org/html/2408.03335v1