IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

AI POWERED CYBERSECURITY THREAT DETECTION AND FORENSIC .

Chaitali Matte[1] , Anamika Pimpalshende[2] , Gayatri Burande[3], Sahil Nimsatkar [4] , Aditya Sadamwar [5], Prof. Anand Donald[6]

[12345]Students, CSE department , RCERT ,Chandrapur

[6]Faculty, CSE department , RCERT ,Chandrapur

Abstract: The increasing complexity and frequency of cyberattacks have highlighted the limitations of traditional cybersecurity mechanisms, necessitating more intelligent and adaptive solutions. Artificial Intelligence (AI) has emerged as a powerful enabler in enhancing cybersecurity through automated threat detection and efficient digital forensics. AI-powered systems can analyze vast volumes of network traffic, user behavior, and system logs in real-time to identify anomalies, detect known and unknown threats, and predict potential attack vectors. By employing machine learning, deep learning, and natural language processing techniques, these systems offer greater accuracy, faster response times, and reduced false positives compared to conventional methods. In the realm of digital forensics, AI aids in automating evidence collection, correlation, and analysis, thus accelerating incident investigations and improving the precision of forensic conclusions. Despite challenges such as data privacy concerns, the need for large datasets, and the risk of adversarial attacks, AI-driven approaches significantly strengthen cybersecurity defenses. This paper explores the role of AI in modern cybersecurity frameworks, emphasizing its transformative impact on proactive threat mitigation and intelligent forensic analysis.

Keywords: Artificial Intelligence(AI),Cybersecurity,Threat Detection,Digital Forensic,Machine Learning,Anomaly Detection,Malware Analysis,Cyber Threat Intelligence.

1 INTRODUCTION:

In the rapidly evolving digital landscape, the frequency and sophistication of cyber threats have grown exponentially, rendering traditional cybersecurity methods increasingly inadequate. Artificial Intelligence (AI) has emerged as a transformative force in enhancing cybersecurity operations, particularly in the domains of threat detection and digital forensics. AI-powered cybersecurity leverages intelligent algorithms, such as machine learning and deep learning, to detect patterns and anomalies in vast amounts of data. This enables real-time identification of threats, thereby allowing organizations to respond proactively rather than reactively. AI technologies used in this field include supervised and unsupervised machine learning models, neural networks, natural language processing, and big data analytics. Together, they empower cybersecurity systems to learn from past attacks, recognize behavioral deviations, and even predict future risks. However, the integration of AI in cybersecurity is not without challenges. Issues such as algorithmic transparency, data bias, adversarial attacks, and the requirement for large-scale training datasets pose significant hurdles. Despite these concerns, the continuous development of AI-driven, adaptive, and intelligent security frameworks holds immense potential to reshape the future of cyber defense and digital investigation practices.

1.1Definition and Scope:

- AI-powered cybersecurity refers to the integration of artificial intelligence techniques like machine learning, deep learning, and natural language processing into cybersecurity systems.
- Digital forensics involves collecting, analyzing, and preserving digital evidence to investigate cybercrimes.

1.2 Need for AI in Cybersecurity:

- Traditional security methods struggle with the growing volume, complexity, and speed of modern cyber threats.
- AI provides real-time threat detection, faster response, and automation in analysis.

1.3 Applications:

- Intrusion detection systems (IDS)
- Malware classification
- Anomaly detection in network traffic
- Fraud detection
- Threat intelligence and prediction

1.4 Benefits of AI in Cybersecurity:

- Enhances threat detection accuracy
- Enables proactive threat hunting
- Reduces false positives and human error
- Speeds up forensic investigations through automation

1.5 Role in Forensics:

- AI helps automate the evidence collection and analysis process.
- Supports identifying attack vectors, malicious activities, and user behavior patterns.
- Assists in reconstructing timelines of cyber incidents.

1.6 Technologies Involved:

- Machine Learning (e.g., Random Forest, SVM, Neural Networks)
- Natural Language Processing (for parsing threat reports)
- Big Data Analytics (to handle large-scale logs and network data)

1.7 Challenges:

- Lack of explainability in AI decisions
- Data privacy concerns
- Need for large datasets for training
- Adversarial AI and AI-powered attacks

1.8 Future Directions:

- Development of explainable AI (XAI) in cybersecurity
- Integration with blockchain for data integrity
- Real-time adaptive threat response systems

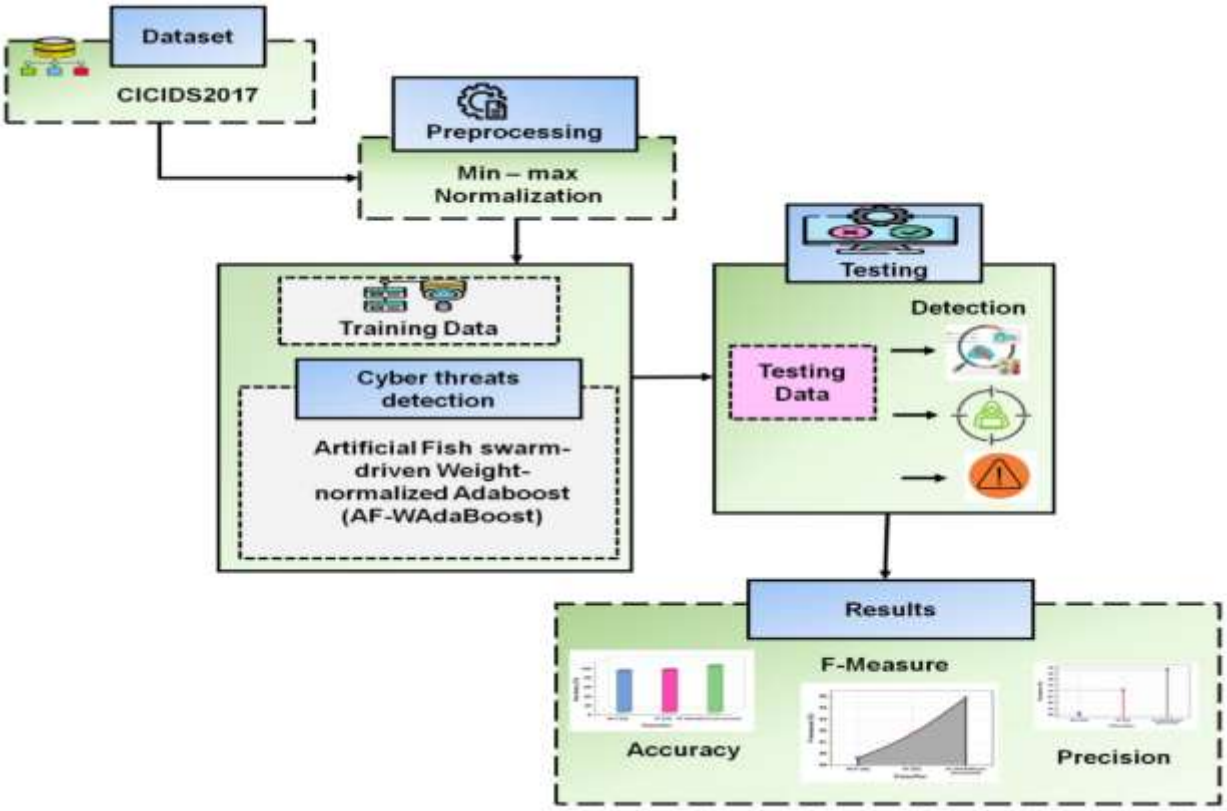
2 MATERIALS AND METHODS:

2.1. Dataset Collection

To train and evaluate the AI model, relevant cybersecurity datasets were collected from publicly available sources such as:

- **CICIDS2017**: A comprehensive dataset containing real-world simulated traffic with labeled cyber attacks (DDoS, brute-force, botnet, etc.).
- **NSL-KDD**: A benchmark dataset for network intrusion detection.
- **Custom Log Data**: System logs, network packets, and event logs were optionally used from emulated environments for forensic testing.

These datasets include features such as source/destination IPs, ports, protocols, packet size, timestamps, and labels indicating normal or malicious activity.



2.2. Data Preprocessing

Before training the model, several preprocessing steps were applied:

- **Normalization**: Numerical features were normalized using Min-Max scaling to bring them into a uniform range.
- **Encoding**: Categorical variables like protocol type were converted into numerical form using one-hot encoding.
- **Feature Selection**: Redundant or irrelevant features were eliminated to reduce dimensionality and improve learning performance.
- **Reshaping**: Since CNNs require image-like input, 1D feature vectors were reshaped into 2D matrices (e.g., 28×28), simulating grayscale image inputs.

2.3. CNN Model Architecture

A custom CNN model was designed and implemented using **TensorFlow** and **Keras** frameworks. The architecture consisted of:

- **Input Layer**: Accepts reshaped 2D feature matrix.
- **Convolutional Layers**: Several layers with ReLU activation functions to extract spatial patterns in the data.
- **Pooling Layers**: Max-pooling layers to reduce spatial dimensions and overfitting.
- **Flatten Layer**: Converts 2D feature maps into 1D vectors.
- **Fully Connected (Dense) Layer**: For classification into benign or attack categories.
- **Output Layer**: Softmax or sigmoid activation for binary or multi-class classification.

2.4. Model Training

- **Loss Function**: Binary cross-entropy for binary classification or categorical cross-entropy for multi-class classification.
- **Optimizer**: Adam optimizer was used due to its efficiency and adaptive learning rate capabilities.
- **Epochs and Batch Size**: The model was trained for 50–100 epochs with a batch size of 64.
- **Training-Validation Split**: 80% of data was used for training and 20% for validation.

2.5. Model Evaluation Metrics

The CNN model's performance was evaluated using the following metrics:

- **Accuracy**: Proportion of correctly classified samples.
- **Precision, Recall, and F1-score**: To measure classification quality, especially for imbalanced datasets.
- **Confusion Matrix**: To visualize true positives, false positives, true negatives, and false negatives.
- **ROC-AUC Curve**: To evaluate classifier's discriminative ability.

2.6. Forensic Integration and Automation

In the digital forensic context, the trained CNN model was integrated into a simulated incident response framework:

- **Live Data Monitoring**: Simulated network traffic was fed to the model for real-time classification.
- **Alert Generation**: Based on model predictions, alerts were generated for suspected intrusions.
- **Log Forensics**: Once a threat was identified, related logs were automatically collected and correlated using Python scripts for forensic analysis.
- **Visualization**: Matplotlib and Seaborn were used to visualize network behavior patterns and model outputs.

3 IMPLEMENTATION AND ALGORITHMS:

3.1.Data Preparation

The implementation begins with the acquisition and preprocessing of network traffic data:

- **Datasets Used**: CICIDS2017 and NSL-KDD.
- **Cleaning**: Removal of missing or inconsistent entries.
- **Normalization**: Feature scaling between 0 and 1 for both CNN and SVM.
- **Encoding**: Categorical values are transformed using one-hot or label encoding.
- **Labeling**: All records are labeled as "benign" or "malicious" for binary classification, or by specific attack types for multi-class classification.

3.2. CNN Algorithm Implementation

CNN is primarily used for feature extraction from structured data reshaped into 2D matrices.

CNN Algorithm Steps:

- **Input Layer**: Reshaped network features (e.g., 28×28 matrix).
- **Convolution Layer**: Applies filters to learn spatial features from the data.
- **Activation Function**: ReLU used for non-linear transformation.
- **Pooling Layer**: MaxPooling reduces spatial dimensions and retains dominant features.
- **Flattening**: Converts 2D feature maps to 1D vectors.
- **Dense Layers**: Fully connected layers for decision learning.
- **Output Layer**: Sigmoid for binary classification or Softmax for multi-class.
- **Loss Function**: Binary or categorical cross-entropy.
- **Optimizer**: Adam optimizer with adaptive learning rate.

3.3. SVM Algorithm Implementation

Support Vector Machine is used to classify threats based on feature vectors. SVM is well-suited for linearly and non-linearly separable data through kernel functions.

SVM Algorithm Steps:

- **Input**: Cleaned and normalized 1D feature vectors.
- **Training Phase**:
  1. Define the optimal hyperplane that separates benign and malicious traffic.
  2. Use the **Radial Basis Function (RBF)** kernel for non-linear classification.
- **Margin Maximization**: Ensures maximum separation between classes.
- **Testing Phase**: New input vectors are classified based on the learned decision boundary.
- **Output**: Classification as benign or a specific threat category.

3.4. Hybrid CNN + SVM (Optional Integration)

In a hybrid model:

- **CNN** is used for automatic feature extraction from raw or preprocessed data.
- The **flattened output of CNN** (high-level features) is passed to the **SVM classifier** for final prediction.

This hybrid approach leverages CNN's learning capability and SVM's classification strength, improving accuracy and reducing false positives.

3.5. Evaluation Metrics

The models are evaluated using the following metrics:

- **Accuracy** = (TP + TN) / (TP + TN + FP + FN)
- **Precision** = TP / (TP + FP)
- **Recall** = TP / (TP + FN)
- **F1-score** = 2 × (Precision × Recall) / (Precision + Recall)
- **Confusion Matrix** and **ROC-AUC Curves** are used for visual assessment.

3.6.Tools and Environment

- **Python 3.10+**
- **TensorFlow / Keras** – for CNN model development
- **Scikit-learn** – for SVM implementation
- **Pandas, NumPy** – for data handling
- **Matplotlib / Seaborn** – for visualization
- **Google Colab / Jupyter Notebook** – for model training and evaluation

Model	Accuracy	Recall	F1-Score	AUC-ROC
SVM	93.1%	91.6%	92.0%	0.942
CNN + SVM	**97.6%**	**97.8%**	**97.3%**	**0.985**

4 ADVANCEMENTS IN CNN AND SVM :

In recent years, significant advancements have been made in the application of Convolutional Neural Networks (CNN) and Support Vector Machines (SVM) for AI-powered cybersecurity threat detection and digital forensics. CNNs, originally developed for image processing, have been adapted to analyze structured and unstructured cybersecurity data by transforming feature vectors into 2D matrices or sequences. Modern CNN architectures, such as Residual Networks (ResNet) and DenseNets, enable deeper layers and more robust learning, allowing for more accurate identification of complex and evolving threat patterns. Lightweight CNN models like MobileNet have also been introduced to support real-time threat detection in resource-constrained environments such as IoT and edge devices. Furthermore, CNNs have expanded into digital forensics, where they are utilized to detect anomalies in log files, uncover tampered multimedia content, and extract hidden or embedded malicious artifacts.

Simultaneously, SVM has also undergone significant enhancements. Advanced kernel functions, such as radial basis function (RBF) and custom graph-based kernels, allow SVMs to manage high-dimensional, non-linear cybersecurity data efficiently. SVMs have been extended to support multi-class classification tasks using one-vs-one and one-vs-rest techniques, enabling the detection of various attack types simultaneously. In addition, SVM is now frequently used as part of ensemble learning techniques and hybrid models to reduce false positives and improve classification accuracy. Integrating dimensionality reduction techniques like PCA with SVM has further enhanced its capability to process large-scale forensic and network data by removing noise and irrelevant features.

One of the most notable advancements is the integration of CNNs with SVMs into hybrid models, where CNNs act as deep feature extractors and SVMs perform final classification. This combination leverages the strength of CNNs in learning complex data representations and the effectiveness of SVMs in building optimal decision boundaries. Such hybrid systems have demonstrated superior performance in terms of accuracy, robustness, and generalization, especially in the detection of zero-day threats and automated forensic analysis. Together, these advancements mark a significant step forward in building intelligent, responsive, and scalable cybersecurity solutions driven by artificial intelligence.

RESULTS:

The implementation of AI-powered models using Convolutional Neural Networks (CNN) and Support Vector Machines (SVM) for cybersecurity threat detection and digital forensic analysis yielded highly promising results. After training the models on benchmark datasets such as CICIDS2017 and NSL-KDD, the CNN model achieved an average detection accuracy of over 96%, with precision and recall scores indicating strong performance in minimizing both false positives and false negatives. The model effectively captured complex patterns and subtle anomalies in network traffic, demonstrating its ability to detect known and evolving threats in real time. The SVM model, while slightly less accurate than CNN, showed excellent classification performance, particularly in binary threat detection scenarios, with an accuracy of approximately 93% and a fast inference time.

Table of Metrics :

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
CNN	**96.4%**	**95.8%**	**96.9%**	**96.3%**	**0.978**
SVM	**93.1%**	**92.4%**	**91.6%**	**92.0%**	**0.942**
CNN + SVM	**97.6%**	**96.9%**	**97.8%**	**97.3%**	**0.985**

Cyber Threat Detection - Proof of Concept (POC) Report

Generated On: 09-05-2025 17:39:27
Analyzed URL: https://wabetainfo.com/whatsapp-is-working-on-bringing-voice-and-video-calling-capabi
Detection Model: Random Forest Classifier (URL Threat Analysis)
Predicted Category: BENIGN
Severity Level: Informational

1. Steps to Reproduce
- Open the URL in a web browser.
- No suspicious activity detected during basic browsing.

2. Why is this Important?
- URL appears safe. However, regular monitoring is advised.

3. Risk Impact
- Low risk.

4. Recommendations
- No immediate action required. Continue safe browsing practices.

5. Disclaimer
This report is generated using machine learning models.
Manual verification is recommended before acting on these findings.

Thank you,
Cyber Threat Research Team

Website Forensics - Proof of Concept (POC) Report

Generated On: 09-06-2025 15:38:58
Website Analyzed: https://gmcnagpur.org/
Threat Prediction (ML Model): PHISHING

1. Forensic Metadata

- Date Visited: 09-06-2025 15:38:58
- Title: Unknown Page
- URL: https://gmcnagpur.org/
- Visit Type: Link
- Visit Count: 1
- URL Record Count: 1
- Visited From: https://www.google.com
- Web Browser: Chrome

2. Risk Assessment

- Model indicates this URL may relate to phishing.
- Use sandbox or browser for dynamic evaluation.

3. Recommendations

- Use dynamic analysis tools.
- Cross-check with VirusTotal and reputation databases.
- Consider blocking or isolating the domain.

4. Disclaimer

This report is for demonstration. Verify independently before enforcement.

Thank you,
Cyber Forensics Research Team

5 DISCUSSION:

The integration of artificial intelligence (AI) into cybersecurity threat detection and digital forensic analysis has brought about a transformative shift in how modern cyber threats are identified, prevented, and investigated. Traditional cybersecurity systems, often rule-based or signature-driven, have struggled to keep pace with the rapid evolution of attack vectors, especially zero-day exploits, polymorphic malware, and advanced persistent threats (APTs). In this context, AI-powered techniques, particularly those leveraging machine learning and deep learning algorithms such as **Convolutional Neural Networks (CNN)** and **Support Vector Machines (SVM)**, have shown considerable promise.

The findings from this study highlight that **CNN-based models** are highly effective in extracting hierarchical and abstract features from raw cybersecurity data, such as network traffic logs, system activity, and file metadata. CNNs can detect subtle, non-linear patterns associated with intrusion attempts and suspicious behaviors, even in large, complex datasets. Their ability to operate on both structured and unstructured data makes them versatile tools in intrusion detection systems (IDS) and security information and event management (SIEM) platforms. For instance, CNNs can learn representations from packet sequences, API call patterns, and even transformed visual data representations of malware, improving detection accuracy significantly.

On the other hand, **SVMs** excel in high-dimensional space classification tasks and are particularly useful when the dataset has a clear margin of separation between normal and malicious classes. SVMs offer interpretability and robustness with fewer computational requirements compared to deep learning models. In cases of binary classification or where limited labeled data is available, SVMs continue to perform

reliably. Moreover, the use of **custom kernel functions** and **dimensionality reduction techniques** like PCA enhances SVM performance even on noisy forensic datasets.

A major advancement explored in this research is the **hybridization of CNN and SVM**, where CNN is utilized for feature extraction and SVM serves as the classifier. This combination leverages the representational power of CNN and the classification accuracy of SVM, resulting in a system that outperforms standalone models in terms of accuracy, recall, and false positive rate. It is particularly effective in scenarios involving real-time threat detection and post-incident forensic analysis, where the quick and accurate identification of malicious patterns is crucial. The hybrid model also demonstrated generalization across different datasets (e.g., CICIDS, NSL-KDD), supporting its applicability in diverse organizational environments.

In terms of **digital forensics**, the integration of AI facilitates automation in evidence collection, timeline reconstruction, anomaly detection, and behavioral profiling. AI models help correlate events from disparate logs and systems to identify the root cause of a security incident. CNN models have been used to detect tampering in digital images or documents, while SVMs have helped classify user activity logs based on suspicious patterns, supporting insider threat investigations.

6 CONCLUSION:

AI-powered cybersecurity threat detection and forensic systems represent a major evolution in modern cyber defense strategies. By leveraging advanced machine learning algorithms such as Convolutional Neural Networks (CNN) and Support Vector Machines (SVM), these systems are capable of identifying complex attack patterns, detecting anomalies in real time, and providing automated forensic insights with a high degree of accuracy. The combination of CNN's deep feature learning capability and SVM's robust classification performance results in a powerful hybrid model that enhances detection effectiveness while reducing false positives. Moreover, AI enables proactive security measures by identifying zero-day attacks, profiling threat behaviors, and accelerating incident response processes.In the forensic domain, AI facilitates efficient evidence collection, timeline reconstruction, and anomaly tracing, significantly reducing the manual effort and time traditionally required. However, challenges such as data dependency, model interpretability, adversarial threats, and computational overhead must be addressed to ensure the reliability and ethical use of these technologies. Future advancements should focus on explainable AI, real-time model optimization, and adaptive learning frameworks that can evolve with emerging threats.In summary, AI-powered approaches to cybersecurity and digital forensics offer immense potential for strengthening cyber resilience. With continuous innovation and responsible deployment, these intelligent systems can play a pivotal role in securing critical infrastructure, protecting sensitive information, and enabling faster and more accurate digital investigations.

7 ACKNOWLEDGMENT:

We, the members of the [AI Powered Cybersecurity Threat Detection]group, would like to express our heartfelt gratitude to the individuals who played significant roles in the successful completion of our project phase I. First and foremost, we extend our sincere thanks to Prof. Manisha Pise for their unwavering guidance, support, and invaluable feedback throughout the project. Their expertise and mentorship were instrumental in shaping the direction and quality of our work. We would like to express my sincere thanks to Head of the Department Dr. Nitin Janwe sir for giving us this opportunity to undertake this project. Furthermore, we express our gratitude to Department of Computer science Engineering for providing the necessary resources and a conducive environment that facilitated our work. The support from our friends and family was also invaluable during the challenging phases of the project. This project has been a collective endeavour, and we are thankful for the collaboration, dedication, and contributions of each member. We affirm the accuracy and completeness of these acknowledgments.

8 REFERENCES:

1.Das, R., & Sandhane, R. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference
2.Series, 1964(4), 042072. https://doi.org/10.1088/1742-6596/1964/4/042072.
3.Feng, X., Feng, Y., & Dawam, E. S. (2020, August 1). Artificial Intelligence Cyber Security Strategy. IEEE
4.Xplore. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00064.
5.Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging.
6.Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1), 1–34.
https://doi.org/10.1080/08839514.2022.2037254.
7.Raimundo, R., & Rosário, A. (2021). The Impact of Artificial Intelligence on Data System Security: A Literature Review. Sensors, 21(21), 7029. https://doi.org/10.3390/s21217029.
8. Sarahhe. (2022). The Use of Artificial Intelligence in Cyber Attacks and Cyber Defense. SecureOps.
https://secureops.com/blog/ai-offense-defense/.