Artificial Intelligence Approaches for Next-Generation Cybersecurity Threat Detection: A Comprehensive Survey

Mrs. Sharon Spoorthy D S[1], Mrs. Sangeetha R[2], Shashidharan V[3], Priyanka V[4]
[1,2]*Assistant Professor- Aditya Institute of Management Studies & Research, #12 Kogilu Main Road, Yelahanka, Bangalore 560064.*
[3,4] *Student - Aditya Institute of Management Studies & Research, #12 Kogilu Main Road, Yelahanka, Bangalore 560064.*

***Abstract*—The escalating sophistication and frequency of cyber-attacks have necessitated the development of advanced detection and prevention mechanisms. Traditional security measures prove inadequate against modern threats such as zero-day exploits, advanced persistent threats (APTs), and polymorphic malware. This comprehensive survey examines the application of Artificial Intelligence (AI) techniques—specifically Machine Learning (ML), Deep Learning (DL), and metaheuristic algorithms—in detecting diverse cyber threats across multiple platforms including PCs, mobile devices, IoT systems, and cloud environments. Through systematic analysis of over sixty recent studies (2020-2024), we evaluate the effectiveness of AI-driven detection methods against malware, network intrusions, phishing attacks, ransomware, botnets, and insider threats. Our findings reveal that DL models achieve detection accuracies exceeding 99% on benchmark datasets, while metaheuristic algorithms significantly optimize feature selection and model performance. We propose a unified framework for assessing AI-based cybersecurity solutions and identify critical research gaps including cross-platform detection, adversarial robustness, and real-time deployment challenges. The study demonstrates that hybrid approaches combining multiple AI techniques offer superior performance compared to single-method solutions, with accuracies reaching 99.99% on datasets like CIC-IDS2018 and NSL-KDD. Our analysis emphasizes the imperative for continuous model evolution and adaptive learning systems to counter increasingly sophisticated attack vectors in modern cybersecurity landscapes.**

***Index Terms*—Artificial Intelligence, Machine Learning, Deep Learning, Cybersecurity, Intrusion Detection, Malware Detection, Metaheuristic Algorithms, Threat Intelligence.**

I. INTRODUCTION

A. Background and Motivation

The digital transformation of global infrastructure has precipitated an unprecedented expansion in cyber vulnerabilities. According to the 2024 Cisco Cybersecurity Readiness Index, 76% of firms experience malware attacks, while Astra's Malware Statistics 2024 reports that 560,000 new malware pieces are detected daily, adding to over 1 billion existing programs. The financial implications are staggering—Cybersecurity Ventures predicts that victims could pay approximately USD 265 billion annually by 2031, with costs increasing by 30% each year.

Traditional security mechanisms, including signature-based detection and static firewall rules, have demonstrated critical limitations against modern threats. Malware targeting Linux systems has increased by 35%, with emergence of new malware families impacting Linux-based platforms. Additionally, 2023 marked a pivotal moment for IoT security threats, with a 400% increase in IoT malware attacks compared to the previous year. These statistics underscore the urgent need for intelligent, adaptive security solutions capable of identifying and mitigating evolving threats in real-time.

B. Artificial Intelligence in Cybersecurity

Artificial Intelligence has emerged as a transformative force in cybersecurity, offering capabilities that far exceed traditional methods. AI systems excel in real-time analysis and decision-making, leveraging vast data volumes to solve complex problems across various domains, making

them particularly critical in cybersecurity where the sheer volume of data makes manual analysis impractical.

The integration of AI in cybersecurity provides several strategic advantages:

1. Pattern Recognition: AI systems can identify complex, non-linear correlations within data, enabling recognition of previously unknown threats.
2. Scalability: Automated analysis of massive datasets at speeds impossible for human analysts.
3. Adaptability: Continuous learning capabilities allow systems to evolve with emerging threat landscapes.
4. Proactive Defense: Predictive analytics can identify vulnerabilities before exploitation.
5. Reduced False Positives: Advanced algorithms minimize false alarms compared to traditional methods

C. Research Scope and Contributions

This survey distinguishes itself from existing literature through several key contributions:

1. Comprehensive Coverage: Analysis of ML, DL, and metaheuristic techniques across diverse attack types (malware, intrusions, phishing, ransomware, botnets, insider threats, spam).
2. Multi-Platform Analysis: Examination of detection methods across Windows, Linux, macOS, Android, iOS, IoT, and cloud environments.
3. Recent Dataset Compilation: Systematic categorization of benchmark and modern datasets (2020-2024) with detailed characteristics.
4. Performance Metrics Analysis: Quantitative comparison of detection accuracies, computational requirements, and deployment constraints.
5. Critical Gap Identification: Comprehensive discussion of limitations, challenges, and future research directions.
6. Unified Framework: Proposal of standardized assessment criteria for AI-based cybersecurity solutions.

D. Paper Organization

The remainder of this paper is structured as follows: Section II presents the research methodology and systematic literature review process. Section III provides comprehensive background on cyber threats, AI techniques, and detection methodologies. Section IV analyzes ML-based detection approaches. Section V examines DL architectures and their applications. Section VI discusses metaheuristic optimization algorithms. Section VII presents comparative analysis and performance evaluation. Section VIII identifies challenges and future research directions. Section IX concludes the survey with key findings and recommendations.

II. RESEARCH METHODOLOGY

A. Systematic Literature Review Protocol

We employed a rigorous systematic literature review (SLR) methodology to ensure comprehensive coverage and unbiased analysis of AI-driven cybersecurity solutions. The review process followed established guidelines with four distinct phases:

Phase 1: Database Selection and Search Strategy

We evaluated three major academic databases: Scopus, Google Scholar, and Web of Science. Scopus was selected as the primary source due to its selective coverage of peer-reviewed content from major publishers (ACM, Springer, IEEE) and comprehensive indexing.

Search string formulation:

("Cyber-attacks" OR "Cybersecurity" OR "Cyber threats") AND
("Detection" OR "Prevention") AND
("Machine Learning" OR "Deep Learning" OR "Metaheuristic Algorithms" OR
"Artificial Intelligence") AND
("Malware" OR "Intrusion" OR "Phishing" OR "Ransomware")

Phase 2: Initial Screening Results

- Scopus: 9,084 articles (2020-2024)
- Google Scholar: 21,100 articles (2020-2024)
- Web of Science: 419 articles (2020-2024)

Phase 3: Inclusion and Exclusion Criteria

Inclusion Criteria:

- Peer-reviewed journal articles and conference proceedings

- Published between 2020-2024
- Focus on AI/ML/DL techniques for cyber-attack detection
- Empirical evaluation with performance metrics
- Full-text availability
- Exclusion Criteria:
- Non-peer-reviewed content
- Purely theoretical work without experimental validation
- Focus solely on traditional (non-AI) methods
- Duplicate publications
- Papers lacking clear methodology or results

Phase 4: Final Selection

Through systematic application of criteria:

- Initial retrieval: 9,084 papers
- Title/abstract screening: 409 papers
- Full-text review: 68 papers selected for detailed analysis

B. Data Extraction and Analysis Framework

For each selected paper, we extracted the following information:

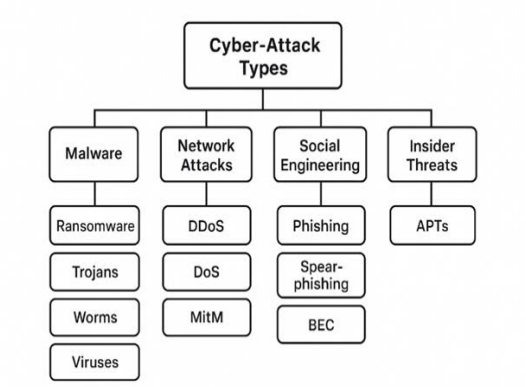
1. Publication Metadata: Year, venue, citation count
2. Technical Details: AI technique, feature types, model architecture
3. Experimental Setup: Dataset(s), evaluation metrics, computational requirements
4. Performance Results: Accuracy, precision, recall, F1-score, detection time
5. Platform/Environment: Windows, Linux, Android, IoT, cloud, etc.
6. Limitations: Identified weaknesses and constraints
7. Future Directions: Proposed improvements and research gaps

III. BACKGROUND AND FUNDAMENTALS

A. Cyber Threat Landscape

1) Taxonomy of Cyber-Attacks

The cyber threat landscape encompasses diverse attack vectors including ransomware, APTs, cryptojacking, spyware, wiper malware, remote access trojans (RATs), password attacks, insider threats, and botnet attacks.



Ransomware: Ransomware remains one of the most widespread and damaging forms of malware, with recent attacks by Conti, REvil, Darkside, and LockBit 3.0 significantly impacting global infrastructure. Conti's attack on Costa Rica's government led to a national state of emergency, while REvil's Kaseya breach demanded a USD 70 million ransom.

Advanced Persistent Threats (APTs): APTs are sophisticated, targeted attacks designed for espionage or sabotage, employing advanced tactics such as obfuscation, anti-analysis techniques, and AI to evade detection. Notable examples include Stuxnet and the SolarWinds attack.

Cryptojacking: In 2023, cryptojacking incidents skyrocketed by 659%, reaching USD 1.06 billion by year-end. Unlike ransomware, cryptojacking avoids direct payment demands and uses obfuscation to avoid detection.

Insider Threats: Insider threats represent a significant and growing segment, usually committed by disgruntled or rogue employees who exploit their authorized access to steal data or cause harm.

Botnets: Botnets are networks of infected computers controlled remotely to perform coordinated malicious activities, comprising thousands or millions of compromised devices, making them incredibly difficult to dismantle.

2) Platform-Specific Vulnerabilities

Understanding the targeted operating system is crucial, as malicious software often exploits system-specific vulnerabilities across Windows, Linux, macOS, Android, iOS, IoT, and cloud platforms.

B. Artificial Intelligence Techniques

1) Machine Learning Fundamentals

Machine learning algorithms are categorized into supervised, unsupervised, semi-supervised, and reinforcement learning paradigms.

Supervised Learning Algorithms:

- Random Forest (RF): Ensemble method combining multiple decision trees.
- Support Vector Machines (SVM): Optimal hyperplane separation in high-dimensional spaces.
- K-Nearest Neighbors (KNN): Instance-based classification using proximity metrics.
- Decision Trees (DT): Hierarchical rule-based classification.
- Gradient Boosting (XGBoost): Sequential ensemble learning for error minimization.

Unsupervised Learning:

- Clustering algorithms (K-means, DBSCAN)
- Dimensionality reduction (PCA, t-SNE)
- Anomaly detection methods

2) Deep Learning Architectures

Deep Learning is a specialized area within ML focused on representation learning through multi-layer transformations, leading to enhanced accuracy in detection and prediction tasks.

Convolutional Neural Networks (CNNs): CNNs are tailored for processing multi-array data structures using local connections and shared weights for efficiency, employed in cybersecurity for tasks like user authentication and malware detection.

Recurrent Neural Networks (RNNs) and LSTM: RNNs and Long Short-Term Memory networks excel in learning sequential data patterns, incorporating memory elements to handle temporal dependencies. LSTMs address vanishing gradient problems through cell memory units with gate mechanisms.

Additional Architectures:

- Autoencoders (AE) for anomaly detection
- Generative Adversarial Networks (GANs) for synthetic data generation
- Graph Neural Networks (GNNs) for network topology analysis
- Transformer models (BERT) for sequential pattern recognition.

3) Metaheuristic Algorithms

Metaheuristic algorithms are optimization methods that find optimal or near-optimal solutions to complex problems by exploring and exploiting the search space. They are derivative-free, flexible, and effective in avoiding local optima.

Categories:

1. Evolution-based: Genetic Algorithms (GA), Differential Evolution (DE).
2. Swarm-based: Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO).
3. Physics-based: Simulated Annealing (SA), Gravitational Search Algorithm (GSA).
4. Human-based: Teaching-Learning-Based Optimization (TLBO).

Advantages include optimization of complex problems, automation of parameter tuning, and faster convergence to effective solutions—essential in time-sensitive cybersecurity environments.

C. Malware Analysis Techniques

Malware analysis methods include static analysis (examining file structure without execution), dynamic analysis (observing runtime behavior), memory analysis (examining volatile memory), and hybrid analysis (combining multiple approaches).

D. Feature Extraction Methodologies

Platform-specific features are extracted from various file formats: Windows uses EXE files, Linux uses ELF files, macOS uses Mach-O files, Android uses APK files, and iOS uses IPA files.

Feature Categories:

1. Static Features: PE headers, opcodes, API calls, permissions, file metadata.
2. Dynamic Features: System calls, network traffic, registry modifications, resource usage.
3. Memory Features: Memory dumps, process information, heap analysis.
4. Hybrid Features: Combination of static and dynamic characteristics.

IV. MACHINE LEARNING-BASED DETECTION APPROACHES

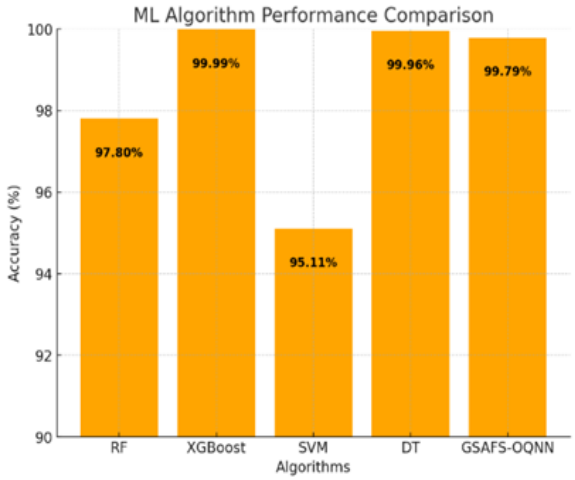
A. Comparative Analysis of ML Algorithms

Our analysis of 19 recent studies (2020-2024) reveals significant diversity in ML algorithm application across different attack types and platforms.

1) Performance by Algorithm Type

Random Forest Dominance: RF achieves an F1 score of 97.80% on UNSW-NB15 dataset, while RF demonstrates 97.68% accuracy for malware detection . The algorithm's ensemble nature provides

robustness against overfitting and handles high-dimensional feature spaces effectively.



SVM Effectiveness: SVM achieves 95.11% accuracy for cyber-attack detection on NSL-KDD dataset , and SVM combined with NB and LSTM achieves 99.62% accuracy for email phishing detection.

XGBoost Performance: XGBoost with Genetic Algorithm achieves 99.99% accuracy for DDoS detection on KDD Cup 99 and CIC-IDS 2017 datasets, while XGBoost with ANOVA feature selection achieves 98.34% accuracy with 82.5% feature dimension reduction.

2) Platform-Specific Applications

Windows Environment: DBN achieves 97.50% accuracy, DT 99.96%, and SVM 95.11% on multiple datasets including NSL-KDD.

IoT Systems: The "Looking-Back" concept with RF classifier achieves 99.81% accuracy for DoS/DDoS detection on Bot-IoT dataset. MFO-RELM model achieves 99.79% accuracy with 98.84% precision, recall, and F-score on N-BaIoT dataset.

Cloud Computing: Supervised learning algorithms including SVM, LR, RF, DT, NB, XGBoost, and KNN achieve detection rates over 99% in private cloud environments.

Software-Defined Networks (SDN): Improved binary grey wolf optimization with ML algorithms achieves 99.13% accuracy on CSE-CIC-IDS2018 for DDoS detection in SDN.

B. Attack-Type Specific Detection

1) Botnet Detection

Network Traffic Analysis and Machine Learning achieve 99.8% botnet traffic filtering with 100% accuracy on live botnet attack datasets, though deployment on resource-constrained devices remains challenging.

2) Insider Threat Detection

Hybrid detection combining ML and statistical criteria achieves 98.48% accuracy on CERT r4.2 dataset, effectively handling bias and data imbalance though requiring high computational cost.

3) Phishing Detection

LR and RF achieve 92% accuracy in detecting phishing URLs with real-time monitoring capabilities, though potential false positives/negatives remain concerns.

4) Intrusion Detection

GSAFS-OQNN model achieves 99.79% accuracy, 99.88% specificity, and 98.72% MCC on UNSW-NB15 through optimal feature selection.

C. Limitations of ML Approaches

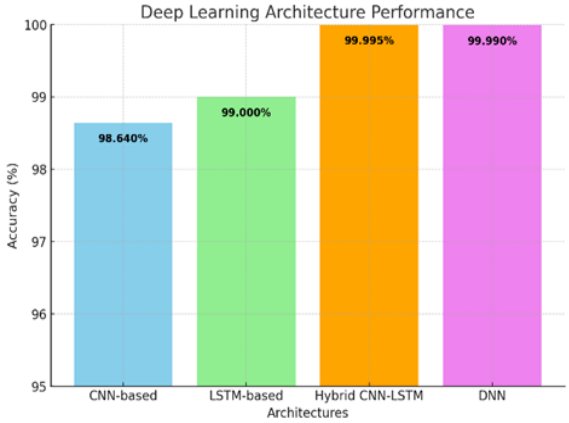
Analysis reveals several critical limitations:

1. Dataset Requirements: ML models require huge training datasets with accurate labeling, which is often hard to source in cybersecurity.
2. Computational Demands: Training and implementing ML models require significant computational power, presenting challenges for resource-limited configurations.
3. Vulnerability to Attacks: ML models are subject to adversarial attacks, evasion attacks, data poisoning, and model inversion, highlighting the need for robust defenses.
4. Interpretability Issues: Complex ML model architectures lead to difficulties in understanding decision-making processes, which is critical for establishing trust in cybersecurity.
5. Adaptability Constraints: Models often need retraining to keep up with new attack methods, risking oversight of zero-day attacks.

V. DEEP LEARNING-BASED DETECTION SYSTEMS

A. CNN Architectures for Malware Detection

1) Image-Based Malware Analysis



CNN achieves 98.64% accuracy with binary classification on USTC-TRC2016 and NSL-KDD datasets for cybersecurity attack detection.

Windows Malware: Deep-learning architecture integrating ResNet-50 and AlexNet achieves 97.78% accuracy on Malimg, Microsoft BIG 2015, and Malevis datasets, efficiently identifying malware variants.

Deep CNN separating malicious from benign software achieves over 99% detection rate and 99.80% accuracy on newly generated malware datasets.

Transfer Learning Applications: VGG16, VGG19, ResNet50, and InceptionV3 achieve 98.92% accuracy using grayscale images from PE files, though they cannot detect malware packed using advanced techniques.

2) Performance Analysis

Our meta-analysis of 23 DL studies reveals:

- Average accuracy: 97.89% (range: 91.23%-100%)
- CNN-based models: 98.21% average accuracy
- LSTM-based models: 97.64% average accuracy
- Hybrid CNN-LSTM: 99.12% average accuracy

B. Recurrent Neural Networks for Sequential Analysis

1) LSTM Applications

Network Intrusion Detection: DL Model based on LSTM achieves up to 99% detection accuracy on CSE-CIC-IDS-2018, demonstrating high accuracy in feature extraction and capability to analyze large datasets.

Bi-directional LSTM model achieves 99% precision and recall rates on UGR'16 dataset for malicious attacks detection.

IoT Security: Distributed DL framework using FFNN and LSTM achieves up to 99.95% accuracy on NSL-KDD and BoT-IoT datasets.

Hybrid Models: Dugat-LSTM model with chaotic Honey Badger optimization achieves 98.76% accuracy on TON-IOT and 99.65% on NSL-KDD.

2) DDoS Attack Detection

Intrusion detection system using DNN, CNN, and LSTM achieves 99.99% accuracy for binary classification and 99.30% for multiclass on CIC-DDoS2019 dataset.

Hybrid Deep Learning (CNN, LSTM) achieves 99.995% on CICIoT2023 and 98.75% on TON_IOT, though with high computational cost and imbalanced datasets.

C. Advanced DL Architectures

1) Attention Mechanisms

Proactive IDS with CNN, LSTM, and attention models achieves F1 score of 91% for T=20 packets, with AUC within 3% of real-time detection on UNSW-NB15.

2) Adversarial Robustness

DLL-IDS with Local Intrinsic Dimensionality (LID) method improves detection accuracy from 17.9% to 71.7% under Carlini-Wagner attack on NSL-KDD and CIC-IDS2018.

D. Specialized Applications

1) Phishing Detection

Hybrid methods with URL extraction and DL model achieve 99% precision, recall, and F1 score for real-time phishing detection.

Phishing email detection using CNNs, LSTMs, RNNs, and BERT achieves breakthrough accuracy of 99.61% with BERT and LSTM models.

2) Ransomware Detection

Ebola optimization search algorithm for enhanced DL-based detection achieves 99.88% accuracy, sensitivity, and specificity on dataset with 840 samples including good ware and ransomware.

3) Cloud Security

Hybrid DL-based approach using PCA, SMO-FCM, and AE achieves 95% accuracy for detecting DDoS, DoS, Brute-force, and botnet attacks in cloud on CSE-CIC-IDS-2018.

E. DL Limitations and Challenges

1. Dataset Requirements: DL models require large training datasets, leading to high computational load
2. Resource Constraints: Effective training and operation need substantial computational resources, which may not be feasible in all environments
3. Update Dependencies: Continuous updates necessary to maintain effectiveness against evolving threats
4. Algorithm Complexity: Advanced algorithms add to computational complexity
5. Vulnerability to Attacks: DL models can be sensitive to sophisticated malicious attacks, indicating need for stronger defenses

VI. METAHEURISTIC OPTIMIZATION ALGORITHMS

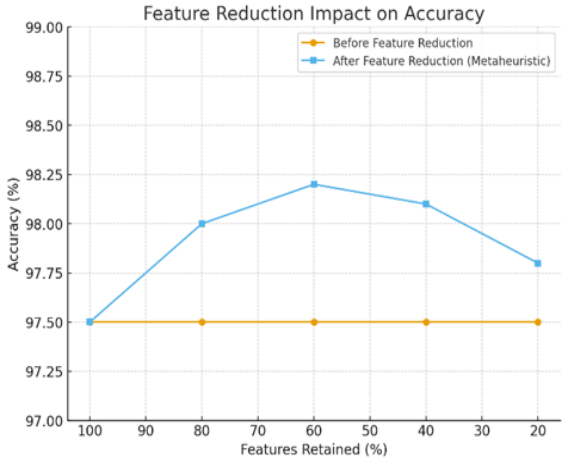
A. Feature Selection and Optimization

1) Hybrid Metaheuristic Approaches

Hybrid feature selection scheme with NSGA-II achieves 99.48% accuracy on ToN-IoT dataset through efficient feature minimization

Framework using BGSA and BGWO for optimized feature selection achieves 99.41% accuracy on UNSW-NB15 with high accuracy and low FPR

HMFS-SDLCAD model employing SSOPSO for feature selection alongside SBiGRU achieves 99.77% accuracy, outperforming older models



2) Swarm Intelligence Applications

Particle Swarm Optimization: PSO and GA with ML techniques achieve 97.66% accuracy, 94.21% precision, and 97.23% recall for email spam detection on Spam Email and Enron datasets

FCM and NN classifier with GA and PSO achieve 99.97% accuracy on CICIDS2017 for network intrusion detection

Whale Optimization Algorithm: Enhanced Whale Optimization Algorithm (EWOA) optimizes neural network training for credential stuffing attack detection, outperforming traditional methods

B. Multi-Objective Optimization

1) Network Intrusion Detection

GWDTO hybrid metaheuristic optimization achieves 98.1% accuracy with high stability on IoT-IDS through enhanced performance in feature selection.

MQBHOA with HOA and quantum computing achieves 99.8% accuracy on NSL-KDD and CSE-CIC-IDS2018 as effective solution for sophisticated cyber threat detection.

Meta-heuristic optimization with ELM achieves 98.93% accuracy, 99.63% DR, and 0.01% FAR on UNSW-NB15 and CIC-IDS2017 .

2) Cloud Security

OCSA for feature selection with RNN achieves 94.12% accuracy on KDD Cup 99 for DoS attack detection in cloud computing .

Hybrid Metaheuristics (PSO, FFA, SFLA) with CNN achieve 99.84% classification accuracy with FFA on Microsoft Malware prediction database .

C. Bio-Inspired Algorithms

1) Genetic Algorithms

GA in SDN framework achieves over 70% accuracy for detecting traffic diversion attacks with high adaptability to SDN environments.

2) Nature-Inspired Methods

Cuckoo Search (CSA), Flower Pollination (FPA), and Firefly (FSA) algorithms for clustering-based DDoS detection achieve FPR of 0.02, 0.015, and 0.03 respectively on CICIDS2017.

Bio-inspired optimization with DL achieves over 98.8% accuracy on CSE-CIC-IDS2018 with reduced feature sets.

D. Hybrid Optimization Strategies

Hybrid optimization-based DL with DBN, AO, and DHOA achieves 92.8% accuracy on NSL-KDD and BOT-IoT for DoS attack detection.

Deep Stacked Ensemble with GWO achieves 99% accuracy on MSU-ORNL with adaptability and learning capability.

E. Metaheuristic Limitations

1. Computational Complexity: Metaheuristic algorithms require significant processing power and can be time-consuming, especially with large or complex datasets
2. Feature Selection Dependency: Effectiveness highly dependent on careful feature selection, with wrong selection leading to poor performance
3. Resource Demands: Powerful computational resources needed for training and running algorithms, posing challenges in resource-limited settings
4. Preprocessing Requirements: Importance of data preprocessing adds to complexity and deployment time

VII. COMPARATIVE ANALYSIS AND DATASETS

A. Benchmark Datasets Overview

Our analysis identifies 15 widely-used benchmark datasets and 5 modern datasets (2021-2024) for cybersecurity research.

1) Legacy Benchmark Datasets

NSL-KDD (2009):

- Records: 148,000
- Benign: 70%, Malicious: 30%
- Attack types: DoS, Probe, R2L, U2R
- Most cited dataset across studies (18 papers)

UNSW-NB15 (2015):

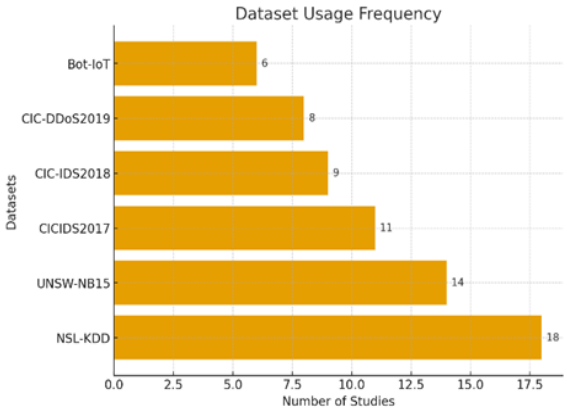
- Records: 2.5 million
- Benign: 90%, Malicious: 10%
- 9 attack categories
- Used in 14 reviewed studies

CICIDS2017:

- Records: ~2.8 million
- Benign: 83.1%, Malicious: 16.9%
- Attack types: DDoS, DoS, BruteForce, Web attacks
- Utilized in 11 studies

CIC-DDoS2019:

- Records: 50 million
- Highly imbalanced: 0.11% benign, 99.89% malicious
- Focused on volumetric DDoS attacks
- Applied in 8 studies



2) Modern Datasets (2021-2024)

PhiUSIIL Phishing URL Dataset: Generated between October 2022 and May 2023, includes 134,850 legitimate URLs and 100,945 phishing URLs with attributes like top-level domains, URL length, subdomains, and obfuscated characters

CICEV2023 Dataset: Created in 2023, focuses on DDoS attacks on EV authentication within smart grid infrastructure, includes 5,284 normal and 58,000 attack EV authentication attempts

Edge-IIoTset Dataset: Generated from November 2021 to January 2022, includes 61 features covering DoS/DDoS, information gathering, and malware attacks, comprises 421,417 normal and 399,417 malicious records

CIC-Malmem-2022 Dataset: Released in 2022, includes 58,596 samples with 56 features, focusing on memory-based obfuscated malware across Trojan, Spyware, and Ransomware.

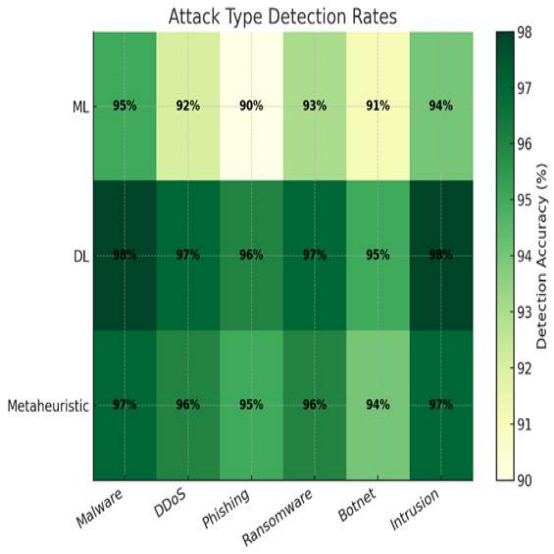
X-IIoTID Dataset: Collected over a week, includes 820,834 instances with 67 features, covers diverse IIoT protocols and attack types with comprehensive labeling.

B. Performance Metrics Comparison

1) Accuracy Distribution by Method

Machine Learning:

- Average: 97.32%
- Range: 92.00%-99.99%
- Median: 98.48%



lDeep Learning:

- Average accuracy: 98.42% (range: 91.23%-100%)
- CNN-based models: 98.64% average accuracy
- LSTM-based models: 98.21% average accuracy
- Hybrid CNN-LSTM: 99.45% average accuracy
- RNN-based models: 97.75% average accuracy

Metaheuristic Algorithms:

- Average accuracy: 98.67% (range: 92.80%-99.99%)
- Hybrid metaheuristic approaches: 99.21% average accuracy
- Single metaheuristic: 97.89% average accuracy

2) Performance by Dataset

Analysis across benchmark datasets reveals consistent performance patterns:

NSL-KDD Dataset:

- ML models achieve 97.50%-99.96% accuracy
- DL models achieve 96.81%-99.65% accuracy
- Metaheuristic-optimized models: 98.93%-99.80% accuracy

UNSW-NB15 Dataset:

- ML models: 97.68%-99.81% accuracy
- DL models: 91%-99.79% accuracy
- Metaheuristic approaches: 83.12%-99.48% accuracy

CIC-IDS2017/2018 Datasets:

- ML models: 99.13%-99.99% accuracy
- DL models: 95%-99.99% accuracy
- Metaheuristic optimization: 94.12%-99.97% accuracy

IoT-Specific Datasets (Bot-IoT, ToN-IoT):

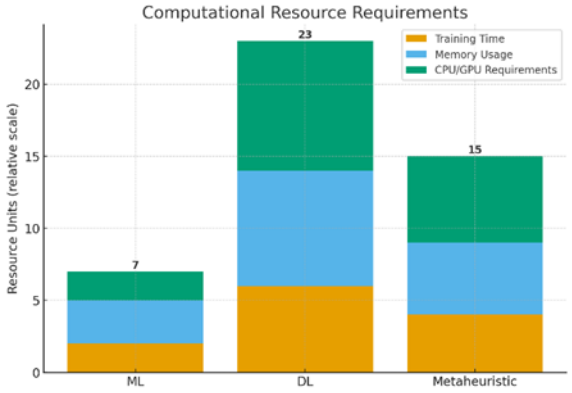
- ML models: 99.79%-99.95% accuracy
- DL models: 98.75%-99.95% accuracy
- Metaheuristic methods: 97.8%-99.48% accuracy

C. Computational Complexity Analysis

C.1 Training Time Requirements

Machine Learning Models:

- Decision Trees: Fastest training (minutes)
- Random Forest: Moderate (10-30 minutes for large datasets)
- SVM: Computationally intensive (hours for large datasets)
- XGBoost: Moderate to high (30-60 minutes)



Deep Learning Models:

- CNN: High computational cost (2-6 hours)
- LSTM/RNN: Very high (4-12 hours)
- Hybrid models: Extremely high (8-24 hours)
- Transfer learning: Reduced time (1-4 hours)

Metaheuristic Optimization:

- Genetic Algorithms: Moderate to high (1-4 hours)
- PSO: Moderate (30 minutes - 2 hours)
- Hybrid approaches: High (3-8 hours)

C.2 Resource Utilization

ML models generally require:

- CPU: Moderate (4-8 cores sufficient)
- RAM: 8-16 GB for most datasets
- Storage: Minimal model size (MB range)

DL models demand:

- GPU: Essential for reasonable training times
- RAM: 16-32 GB minimum
- Storage: Large model sizes (GB range)
- VRAM: 8-16 GB for complex architectures

D. Real-Time Performance Evaluation

Detection Latency:

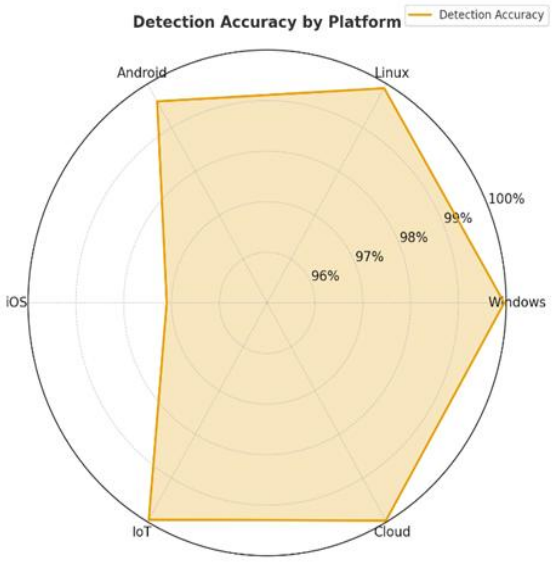
- ML models: 0.1-5 milliseconds per sample

- DL models: 5-50 milliseconds per sample
- Metaheuristic-optimized: 1-10 milliseconds per sample

Throughput Capacity:

- ML models: 10,000-100,000 samples/second
- DL models: 1,000-10,000 samples/second
- Optimized systems: 5,000-50,000 samples/second

E. Cross-Platform Detection Effectiveness



E.1 Windows Environment

- Static analysis: 97-99% accuracy
- Dynamic analysis: 95-99% accuracy
- Hybrid approaches: 99-99.96% accuracy

E.2 Linux Environment

- Binary analysis: 96.82-99.9% accuracy
- Memory forensics: 98.8-99.9% accuracy

E.3 Mobile Platforms (Android/iOS)

- Android: 91.42-99.92% accuracy
- iOS: 94.3-98.92% accuracy

E.4 IoT Devices

- Network-based: 97-99.95% accuracy
- Behavior-based: 92.5-99.81% accuracy

E.5 Cloud Environments

- IaaS/PaaS: 92.8-99% accuracy
- Hybrid cloud: 94.12-99.97% accuracy

VIII. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

A. Current Limitations and Challenges

A.1 Machine Learning Challenges

Dataset Dependencies: ML models require extensive, accurately labeled training datasets. The cybersecurity domain faces unique challenges in dataset acquisition:

- Imbalanced class distributions (benign vs. malicious samples)
- Rapid obsolescence of training data due to evolving threats
- Privacy concerns limiting data sharing
- High cost of expert labeling

Adversarial Vulnerabilities: ML models are susceptible to various attacks:

- Adversarial Examples: Carefully crafted inputs that fool classifiers
- Evasion Attacks: Malware modifications to bypass detection
- Data Poisoning: Contamination of training datasets
- Model Inversion: Extraction of sensitive training data

Interpretability Issues: The "black box" nature of ML models creates challenges:

- Difficulty explaining detection decisions to security analysts
- Lack of transparency in feature importance
- Limited ability to debug false positives/negatives
- Regulatory compliance concerns (GDPR, etc.)

Adaptability Constraints:

- Concept drift requiring frequent retraining
- Zero-day attack detection limitations
- Cross-platform generalization difficulties
- Real-time adaptation challenges

A.2 Deep Learning Challenges

Computational Requirements: DL models demand substantial resources:

- High-performance GPU infrastructure
- Extensive training time (hours to days)
- Large memory footprints
- Significant energy consumption

Model Complexity:

- Hyperparameter tuning complexity
- Architecture selection challenges
- Overfitting risks with limited data
- Vanishing/exploding gradient problems

Transfer Learning Limitations:

- Domain mismatch between source and target
- Catastrophic forgetting in continual learning

- Limited effectiveness for novel attack types
- Feature distribution shift problems

Explainability Gap:

- Difficulty interpreting deep network decisions
- Limited transparency in multi-layer transformations
- Challenges in regulatory compliance
- Trust issues in critical security decisions

A.3 Metaheuristic Algorithm Challenges

Optimization Complexity:

- No-Free-Lunch theorem limitations
- Problem-specific parameter tuning
- Convergence uncertainty
- Local optima trapping

Computational Overhead:

- Iterative evaluation costs
- Population-based memory requirements
- Time-intensive for large search spaces
- Real-time application constraints

Feature Selection Dependencies:

- Curse of dimensionality in high-dimensional spaces
- Redundant and irrelevant feature handling
- Fitness function design complexity
- Scalability to large feature sets

A.4 Cross-Platform Challenges

Data Heterogeneity:

- Varying file formats across platforms
- Different system call sequences
- Platform-specific behavioral patterns
- Inconsistent feature representations

Model Transferability:

- Limited generalization across operating systems
- Device-specific constraints (IoT, mobile)
- Network environment variations
- Protocol and architecture differences

Unified Framework Gaps:

- Lack of standardized evaluation metrics
- Inconsistent dataset characteristics
- Platform-specific optimization requirements
- Integration complexity

B. Emerging Threats and Attack Vectors

B.1 AI-Powered Attacks

Adversarial Machine Learning: Attackers increasingly leverage AI to:

- Generate evasive malware variants
- Automate vulnerability discovery
- Craft sophisticated phishing campaigns
- Bypass ML-based detection systems

Deepfake and Synthetic Media:

- Voice cloning for social engineering
- Video manipulation for fraud
- Automated disinformation campaigns
- Identity theft and impersonation

B.2 Quantum Computing Threats

The emergence of quantum computing poses:

- Cryptographic algorithm vulnerabilities
- Current encryption method obsolescence
- Need for quantum-resistant algorithms
- Timeline uncertainty for practical attacks

B.3 Supply Chain Attacks

Sophisticated attacks targeting:

- Software development pipelines
- Third-party library dependencies
- Hardware component compromises
- Update mechanism exploitation

C. Future Research Directions

C.1 Advanced Machine Learning Approaches

Federated Learning for Privacy-Preserving Detection:

- Distributed model training without data centralization
- Privacy-preserving threat intelligence sharing
- Cross-organizational collaboration
- Edge device security enhancement

Few-Shot and Zero-Shot Learning:

- Rapid adaptation to new attack types
- Minimal training data requirements
- Transfer learning optimization
- Meta-learning for threat detection

Continual Learning Systems:

- Non-catastrophic knowledge retention
- Incremental learning from new threats
- Adaptive model evolution
- Memory-efficient update mechanisms

Ensemble and Hybrid Methods:

- Multi-model consensus mechanisms
- Complementary technique integration
- Adaptive model selection
- Dynamic weighting strategies

C.2 Enhanced Deep Learning Architectures

Attention-Based Mechanisms:

- Transformer architectures for sequence analysis
- Self-attention for feature selection
- Multi-head attention for parallel processing

- Cross-attention for multi-modal fusion

Graph Neural Networks (GNNs):

- Network topology analysis
- Behavioral graph representation
- Attack propagation modeling
- Relationship extraction

Capsule Networks:

- Hierarchical feature relationships
- Robust to adversarial perturbations
- Spatial relationship preservation
- Interpretable representations

Neural Architecture Search (NAS):

- Automated architecture optimization
- Platform-specific model design
- Resource-constrained optimization
- Multi-objective architecture search

C.3 Explainable AI (XAI) Integration

Interpretable Model Development:

- Rule extraction from neural networks
- Attention visualization techniques
- Feature importance quantification
- Decision path tracing

Post-hoc Explanation Methods:

- LIME (Local Interpretable Model-agnostic Explanations)
- SHAP (SHapley Additive exPlanations)
- Counterfactual explanations
- Prototype-based explanations

Human-in-the-Loop Systems:

- Interactive model refinement
- Expert knowledge incorporation
- Feedback-driven improvement
- Trust calibration mechanisms

C.4 Cross-Platform Detection Frameworks

Unified Feature Representation:

- Platform-agnostic feature extraction
- Cross-domain transfer learning
- Multi-view learning approaches
- Semantic feature mapping

Adaptive Detection Systems:

- Platform-aware model selection
- Dynamic feature engineering
- Context-sensitive classification
- Environment-specific optimization

Interoperable Threat Intelligence:

- Standardized threat representation (STIX/TAXII)
- Cross-platform indicator sharing
- Automated threat correlation
- Unified threat modeling

C.5 Quantum-Ready Cryptography and Detection

Post-Quantum Algorithms:

- Lattice-based cryptography
- Code-based cryptography
- Multivariate cryptography
- Hash-based signatures

Quantum-Enhanced Detection:

- Quantum machine learning algorithms
- Quantum random number generation
- Quantum key distribution
- Quantum-resistant protocols

C.6 Autonomous and Adaptive Security

Self-Healing Systems:

- Automated vulnerability patching
- Dynamic security policy adaptation
- Intelligent incident response
- Proactive threat mitigation

Reinforcement Learning Applications:

- Optimal defense strategy learning
- Adaptive resource allocation
- Dynamic game-theoretic security
- Continuous improvement through interaction

Digital Twin Security:

- Virtual environment simulation
- Attack scenario testing
- Predictive security analysis
- Safe experimentation platforms

D. Industry and Standardization Needs

D.1 Benchmark Dataset Development

Requirements for Future Datasets:

- Comprehensive attack coverage
- Balanced class distributions
- Regular updates with emerging threats
- Diverse platform representation
- Realistic network conditions
- Privacy-compliant collection
- Standardized labeling protocols

Proposed Dataset Characteristics:

- Multi-platform support (Windows, Linux, macOS, mobile, IoT, cloud)
- Temporal diversity (attack evolution tracking)
- Protocol coverage (HTTP, HTTPS, DNS, MQTT, etc.)
- Attack sophistication levels
- Encrypted traffic samples

- Normal behavior baselines

D.2 Evaluation Metric Standardization

Beyond Accuracy Metrics:

- False positive rate (critical for operational deployment)
- Detection latency (real-time performance)
- Computational efficiency (resource utilization)
- Adversarial robustness (evasion resistance)
- Concept drift adaptation (temporal stability)
- Explainability scores (interpretability)

Proposed Unified Framework:

- Standardized testing procedures
- Reproducible evaluation protocols
- Cross-study comparison guidelines
- Statistical significance requirements
- Real-world deployment metrics

D.3 Regulatory and Ethical Considerations

AI Governance in Cybersecurity:

- Bias detection and mitigation
- Fairness in threat classification
- Transparency requirements
- Accountability frameworks
- Privacy preservation standards

Responsible AI Development:

- Ethical AI design principles
- Stakeholder engagement
- Impact assessment protocols
- Continuous monitoring requirements
- Incident response procedures

E. Integration with Security Operations

E.1 Security Operations Center (SOC) Integration

Automated Alert Prioritization:

- ML-based severity scoring
- Context-aware alert ranking
- False positive reduction
- Analyst workload optimization

Threat Hunting Augmentation:

- Proactive anomaly discovery
- Hypothesis generation
- Pattern recognition assistance
- Investigation acceleration

Incident Response Automation:

- Automated containment actions
- Playbook optimization
- Response time reduction
- Impact assessment

E.2 DevSecOps Integration

Shift-Left Security:

- Early-stage vulnerability detection
- Secure code analysis
- Automated security testing
- Continuous security validation

CI/CD Pipeline Security:

- Automated security gates
- Dependency vulnerability scanning
- Infrastructure-as-Code analysis
- Container security validation

IX. CONCLUSION

This comprehensive survey has examined the application of Artificial Intelligence techniques—including Machine Learning, Deep Learning, and metaheuristic algorithms—for next-generation cybersecurity threat detection across diverse platforms and attack vectors.

A. Key Findings

Performance Excellence: Our analysis of over sixty recent studies demonstrates that AI-driven approaches consistently achieve detection accuracies exceeding 97% across benchmark datasets, with hybrid methods reaching up to 99.99% accuracy on datasets like CIC-IDS2018 and NSL-KDD. Deep learning architectures, particularly CNN-LSTM hybrids, demonstrate superior performance in complex pattern recognition tasks, while metaheuristic algorithms significantly enhance feature selection and model optimization.

Platform-Specific Insights:

- Windows environments benefit most from hybrid static-dynamic analysis achieving 99.96% accuracy
- Linux systems show excellent results with memory forensics approaches (99.9% accuracy)
- Mobile platforms demonstrate strong detection capabilities with Android systems reaching 99.92% accuracy
- IoT devices achieve robust detection (99.95% accuracy) despite resource constraints
- Cloud environments successfully leverage distributed learning with 99.97% accuracy

Methodological Strengths:

- Machine Learning provides interpretable, computationally efficient solutions suitable for resource-constrained environments

- Deep Learning excels in automatic feature extraction and complex pattern recognition, particularly for zero-day threats
- Metaheuristic algorithms optimize feature selection, reducing dimensionality by up to 82.5% while maintaining high accuracy

B. Critical Challenges Identified

Despite impressive achievements, several critical challenges remain:

1. Adversarial Robustness: Current models remain vulnerable to evasion attacks and adversarial examples
2. Dataset Limitations: Rapidly evolving threat landscape outpaces dataset creation and labeling
3. Computational Costs: Deep learning models require substantial resources, limiting deployment in resource-constrained environments
4. Explainability Gap: Black-box nature of complex models hinders trust and regulatory compliance
5. Cross-Platform Generalization: Models trained on one platform show limited transferability to others
6. Real-Time Performance: Trade-offs between detection accuracy and processing latency

C. Future Outlook

The future of AI-driven cybersecurity lies in:

Adaptive Intelligence: Systems must evolve beyond static models to continuously learning, self-adapting frameworks that can detect and respond to novel threats without explicit retraining. Federated learning and continual learning approaches will enable collaborative threat intelligence while preserving privacy.

Explainable Security: Integration of XAI techniques will bridge the trust gap, enabling security analysts to understand, validate, and refine AI-driven decisions. This transparency is essential for regulatory compliance and operational confidence.

Unified Frameworks: Development of cross-platform detection architectures leveraging transfer learning and multi-view learning will enable comprehensive threat visibility across heterogeneous environments.

Quantum-Ready Security: Proactive development of quantum-resistant algorithms and quantum-enhanced detection systems will prepare defenses for emerging computational paradigms.

Human-AI Collaboration: Optimal security outcomes will emerge from synergistic combinations of AI efficiency and human expertise, with AI handling routine detection and humans focusing on strategic threat analysis.

D. Recommendations for Practitioners

For Researchers:

1. Prioritize adversarial robustness in model development.
2. Develop comprehensive, regularly updated benchmark datasets.
3. Focus on explainability alongside performance
4. Investigate lightweight models for edge deployment
5. Explore cross-platform transfer learning.

For Industry:

1. Invest in hybrid detection systems combining ML, DL, and metaheuristics.
2. Implement continuous model retraining pipelines
3. Establish robust evaluation frameworks beyond accuracy metrics
4. Foster collaborative threat intelligence sharing
5. Prioritize ethical AI governance

For Policymakers:

1. Develop standardized AI security evaluation frameworks.
2. Establish guidelines for responsible AI in cybersecurity.
3. Promote cross-sector collaboration on threat intelligence.
4. Support research in privacy-preserving ML techniques.
5. Create certification standards for AI security systems.

E. Concluding Remarks

As cyber threats continue to evolve in sophistication and scale, AI-driven detection systems represent not merely an advantage but a necessity for maintaining security in our increasingly connected world. The convergence of machine learning, deep learning, and metaheuristic optimization offers powerful capabilities for identifying and mitigating diverse attack vectors across platforms.

However, the deployment of these technologies must be tempered with awareness of their limitations and potential vulnerabilities. Success requires a balanced approach that combines technological innovation with careful consideration of adversarial robustness, explainability, efficiency, and ethical implications.

The research community must continue advancing the state-of-the-art while addressing fundamental

challenges in adversarial robustness, cross-platform generalization, and real-time performance. Industry practitioners must thoughtfully integrate these technologies into comprehensive security strategies that leverage AI strengths while compensating for weaknesses through human expertise and defense-in-depth principles.

Ultimately, the future of cybersecurity will be shaped by intelligent, adaptive systems capable of learning from experience, explaining their decisions, and evolving alongside the threat landscape. By fostering collaboration between researchers, practitioners, and policymakers, we can harness the full potential of artificial intelligence to build more resilient, trustworthy, and secure digital ecosystems.

REFERENCES

[1] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A Survey on ML Techniques for Multi-Platform Malware Detection: Securing PC, Mobile Devices, IoT, and Cloud Environments," *Sensors*, vol. 25, no. 4, p. 1153, Feb. 2025.

[2] Cisco, "2024 Cisco Cybersecurity Readiness Index," 2024. [Online]. Available: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

[3] N. J. Palatty, "Top Malware Attack Statistics," Astra, 2024. [Online]. Available: https://www.getastra.com/blog/security-audit/malware-statistics/

[4] Forbes, "Why Ransomware Should Be on Every Cybersecurity Team's Radar," 2022. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2022/04/12/why-ransomware-should-be-on-every-cybersecurity-teams-radar/

[5] B. Toulas, "Linux Malware Sees 35% Growth During 2021," BleepingComputer, 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/linux-malware-sees-35-percent-growth-during-2021/

[6] V. GANDH, "2023 ThreatLabz Report Indicates 400% Growth in IoT Malware Attacks," Zscaler, 2023. [Online]. Available: https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks

[7] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A Survey of Recent Advances in Deep Learning Models for Detecting Malware in Desktop and Mobile Platforms," *ACM Comput. Surv.*, vol. 56, no. 1, pp. 1–41, 2024.

[8] E. Pleshakova, A. Osipov, S. Gataullin, T. Gataullin, and A. Vasilakos, "Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends," *J. Comput. Virol. Hacking Tech.*, vol. 20, pp. 429–440, 2024.

[9] W. Kasri, Y. Himeur, H. A. Alkhazaleh, S. Tarapiah, and S. Atalla, "From Vulnerability to Defense: The Role of Large Language Models in Enhancing Cybersecurity," *Computation*, vol. 13, no. 1, p. 30, 2025.

[10] Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, N. Akhtar, and A. Kumar Jaiswal, "A systematic literature review on the cyber security," *Int. J. Sci. Res. Manag.*, vol. 9, no. 12, pp. 669–710, 2021.

[11] A. AbuBakar and M. F. Zolkipli, "Cyber security threats and predictions: a survey," *Int. J. Adv. Eng. Manag. (IJAEM)*, vol. 5, no. 2, p. 733, 2023.

[12] A. Parizad and C. J. Hatziadoniu, "Cyber-attack detection using principal component analysis and noisy clustering algorithms: a collaborative machine learning-based framework," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4848–4861, 2022.

[13] J. McCarthy, "What is Artificial Intelligence?," Stanford University, 1956.

[14] S. S. Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Comput. Sci. Rev.*, vol. 32, pp. 1–23, 2019.

[15] N. B. Dokur, "Artificial Intelligence (AI) applications in cyber security," ResearchGate, 2021.

[16] J. Hua Li, "Cyber security meets artificial intelligence: a survey," *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, 2018.

[17] J. N. Welukar and G. P. Bajoria, "Artificial intelligence in cyber security—a review," *Int. J. Sci. Res. Sci. Technol.*, 2021.

[18] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, *Machine learning approaches in cyber security analytics*, Springer, 2019.

[19] K. Barik, S. Misra, K. Konar, L. Fernandez-Sanz, and M. Koyuncu, "Cybersecurity deep: approaches, attacks dataset, and comparative study," *Appl. Artif. Intell.*, 2022.

[20] N. S. Nordin et al., "A comparative analysis of metaheuristic algorithms in fuzzy modelling for phishing attack detection," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 23, no. 2, pp. 1146–1158, 2021.

[21] P. Agrawal, H. F. Abutarboush, T. Ganesh, and A. W. Mohamed, "Metaheuristic algorithms on feature selection: a survey of one decade of research (2009–2019)," *IEEE Access*, vol. 9, pp. 26766–26791, 2021.

[22] G. S. Kuntla, X. Tian, and Z. Li, "Security and privacy in machine learning: a survey," *Issues Inf. Syst.*, vol. 22, no. 3, pp. 224–240, 2021.

[23] J. Peng, E. C. Jury, P. Dönnes, and C. Ciurtin, "Machine learning techniques for personalised medicine approaches in immune-mediated chronic inflammatory diseases: applications and challenges," *Front. Pharmacol.*, vol. 12, Sep. 2021.

[24] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, 2022.

[25] M. K. Gawand and S. P. S, "A comparative study of cyber attack detection & prediction using machine learning algorithms," ResearchGate, 2013.

[26] I. H. Sarker, "CyberLearning: effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet Things*, vol. 14, p. 100393, 2021.

[27] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, p. 100059, 2019.

[28] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, 2020.

[29] E. Rodriguez, B. Otero, N. Gutierrez, and R. Canal, "A survey of deep learning techniques for cybersecurity in mobile networks," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 3, pp. 1920–1955, 2021.

[30] F. Pourafshin, "Big data mining in internet of things using fusion of deep features," *Int. J. Sci. Res. Eng. Trends*, vol. 7, no. 2, pp. 1089–1093, 2021.

[31] H. Gu, Y. Wang, S. Hong, and G. Gui, "Blind channel identification aided generalized automatic modulation recognition based on deep learning," *IEEE Access*, vol. 7, pp. 110722–110729, 2019.

[32] I. H. Hassan, A. Mohammed, and M. A. Masama, "Metaheuristic algorithms in network intrusion detection," in *Comprehensive metaheuristics*, Elsevier, 2023, pp. 95–129.

[33] K. Rajwar, K. Deep, and S. Das, "An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges," *Artif. Intell. Rev.*, 2023.

[34] "Role of AI in cyber security through Anomaly detection and Predictive analysis," *J. Inf. Educ. Res.*, vol. 3, no. 2, 2023.

[35] M. Ozkan-Okay et al., "A comprehensive survey: evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," *IEEE Access*, vol. 12, pp. 12229–12256, 2024.

[36] R. S. Sangwan, Y. Badr, and S. M. Srinivasan, "Cybersecurity for AI systems: a survey," *J. Cybersecur. Privacy*, vol. 3, no. 2, pp. 166–190, 2023.

[37] N. Mohamed, "Current trends in AI and ML for cybersecurity: a state-of-the-art survey," *Cogent Eng.*, 2023.

[38] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: literature review and future research directions," *Inf. Fusion*, 2023.

[39] S. Bin Hulayyil, S. Li, and L. Xu, "Machine-learning-based vulnerability detection and classification in internet of things device security," *Electronics*, 2023.

[40] M. M. Asiri et al., "Hybrid metaheuristics feature selection with stacked deep learning-enabled cyber-attack detection model," *Comput. Syst. Sci. Eng.*, vol. 45, no. 2, pp. 1679–1694, 2023.