Enhancing OSN Security: Detecting Email Hijacking and DNS Spoofing Using Energy Consumption and Opcode Sequence Analysis

[1*]Romil Rawat, [2]Kamal Borana, [3]Shweta Gupta, [3]Mandakini Ingle, [5]Ashish Dibouliya, [6]Purvee Bhardwaj, [7]Anjali Rawat
[1*]LabGeoInf – Research LABoratory in GEOmatics and INFormation systems, Rome, Italy
[2]Department of CSE, SVIIT, SVVV, Indore - India
[3]Computer Science and Engineering Department, Medicaps University, Indore (M.P.), India
[5]Data Architecture (Webster Bank- USA)
[6]Rabindranath Tagore University, Bhopal, (MP) - India
[7]Department of Computer and Communication Technology, University of Extremadura, Spain
E-mail: rawat.romil@gmail.com, kamalborana@svvv.edu.in , shweta.gupta@medicaps.ac.in, tayademandakini@gmail.com, ashish.dibouliya@gmail.com, purveebhardwaj@gmail.com, rawatanjali457@gmail.com
[*]Corresponding author

Keywords: OSN security, email hijacking detection, DNS Spoofing prevention, energy consumption footprint, opcode sequence mining, automated threat detection

Received: August 21, 2024

The rapid increase in automation within Online Social Networks (OSNs) has led to a surge in cyber threats, notably Email Hijacking and DNS (Domain Name System) Spoofing, which leverage malicious scripts to manipulate traffic, steal credentials, and evade detection. Traditional security mechanisms fail to effectively identify such automation-based attacks, necessitating an advanced detection framework. Objective & Purpose-This study introduces the Automated Social Network Attack Detection Model (ASNADM), which combines Energy Consumption Footprint (EComp-FP) Analysis and Automated Software Opcode Sequence Analysis (ASOSA-OSM- opcode sequence mining) for high-precision OSN security. EComp-FP detects deviations in power consumption linked to malicious automation tools, while ASOSA-OSM analyzes opcode sequences to differentiate between benign and attack behaviors. The Self-Adaptive Fuzzy Pattern Matching Clustering (SAFPMC) Algorithm enhances classification accuracy, reducing false alarms and improving real-time threat detection. Methodology and Dataset-The model was rigorously evaluated using the SPEMC-15K-E (Spam Email Classification dataset in English) dataset (15,000 samples: 7,500 benign, 7,500 malicious). EComp-FP achieved 99.87% accuracy with a 1.4W power deviation, while ASOSA-OSM attained 99.81% accuracy, detecting automation tools with an Opcode Frequency Variance (OFV) of 8.7 in malicious samples versus 3.5 in benign ones. The hybrid EComp (Energy Consumption) + OSA (Opcode Sequence Analysis) model outperformed both standalone methods, achieving 99.93% accuracy, 99.91% F1-score, a false positive rate of just 0.07%, and a false negative rate of 0.05%. Among classifiers, the Self-Adaptive Soft Fuzzy C-Means (SSFCM) Hybrid model achieved the highest performance, with 99.93% accuracy, 99.85% precision, 99.9% recall, and the lowest misclassification rate of 0.05%, surpassing Decision Tree (DT), K-Nearest Neighbors (KNN), Random Forest (RF), and Support Vector Machine (SVM). Result - Optimization techniques significantly improved real-time detection efficiency. The SAFPMC algorithm reduced detection latency by 35%, while parallel processing lowered computational overhead by 31%. Feature selection improved classification speed by 27%, and federated learning reduced processing load by 25%, enabling scalable, real-time OSN threat monitoring. This study presents an advanced hybrid detection framework for OSN security, combining energy consumption profiling and opcode sequence analysis to detect email hijacking and DNS spoofing attacks. The model achieves a 99.92% detection precision, a 99.89% real-time accuracy, and reduces computational overhead by 31%, making it a robust and efficient solution for securing online social networks. These findings confirm that combining energy profiling and opcode sequence analysis is highly effective in detecting automation-based OSN threats. Future work will focus on integrating deep learning (DL) for anomaly detection, AI (artificial intelligence)-driven botnet defense, and enhancing large-scale OSN threat mitigation strategies.

Povzetek: V članku je opisan hibridni model za zaznavanje napadov v družbenih omrežjih, ki z analizo porabe energije in zaporedij ukazov doseže veliko točnost pri odkrivanju e-poštnih in DNS napadov.

1 Introduction

The rise of automation in OSN [1] has increased the risk of cyber threats [2], particularly Email Hijacking [3] and DNS Spoofing [4]. These attacks exploit malicious automation tools to manipulate network traffic, steal credentials, and intercept communications. Recent incidents highlight the growing use of AI-driven phishing [5] campaigns and botnet attacks, which evade traditional security systems. Given the increasing role of OSNs in financial transactions, enterprise communications, and authentication mechanisms, ensuring robust security measures is essential.

Future work will focus on expanding detection capabilities to counter AI-driven botnets [6][7] and Advanced Persistent Threats, integrating DL models for enhanced anomaly detection, and optimizing real-time threat monitoring for large-scale OSN infrastructures.

The rapid evolution of cyber threats targeting OSN [8] has introduced sophisticated attack variants, including AI-powered botnets, adversarial machine learning (ML)-based evasion techniques [9], and large-scale automated credential stuffing. Traditional security mechanisms struggle to detect these advanced threats, as attackers increasingly leverage self-mutating automation tools and polymorphic malware. A notable example is the large-scale OSN credential breach involving over 500 million compromised accounts, where automated scripts were used to hijack user sessions and execute phishing campaigns. Similarly, deepfake-powered social engineering [10] attacks have been weaponized to impersonate high-profile individuals, manipulate public opinion, and spread misinformation at an alarming scale and detection mechanisms that can accurately differentiate between benign and malicious automation activities in OSNs.

The integration of AI in cyberattacks [11] has led to the rise of adaptive and intelligent automation tools capable of evading conventional security measures. Attackers now employ adversarial ML to modify malware [12] behavior dynamically, making detection more challenging. DNS tunnelling [13][14] has also been exploited in OSN automation attacks, allowing attackers to exfiltrate sensitive data while bypassing conventional monitoring systems. A significant incident involved a DNS spoofing-based OSN attack where cybercriminals manipulated domain resolution processes, redirecting users to counterfeit versions of trusted platforms and harvesting their credentials. To counter these evolving threats, modern cybersecurity frameworks now incorporate hybrid DL models such as Long Short-Term Memory (LSTM)[15] networks for anomaly detection and Transformer-based architectures for opcode sequence classification. The combination of energy consumption analysis and opcode sequence analysis offers
a robust security framework capable of detecting complex automation-driven OSN threats.

In response to the growing sophistication of automation attacks, researchers have focused on developing multi-layered detection frameworks that integrate behavioral analysis with computational intelligence. EComp [16] analysis has emerged as a promising technique for identifying automation threats by monitoring the anomalous energy footprints of automated software running on Socially Shared Networked Devices (SSNDs) [17]. By analyzing power usage patterns under normal and attack conditions, security systems can flag unusual spikes indicative of malicious activities such as session hijacking and DNS spoofing [18]. In parallel, OSA plays a crucial role in detecting automation tools [19] by extracting and analyzing the opcode sequences of suspicious binaries. ASOSA enables deep inspection of execution patterns, differentiating between benign and malicious automation behaviors. The combination of these methods significantly enhances detection accuracy in OSN environments.

The SPEMC-15K-E dataset [1][2], containing extensive real-world samples of automated and non-automated software, has been utilized to train and evaluate modern OSN attack detection models. Recent research shows that classifiers [20][21] such as DT, KNN, RF, SVM, and SSFCM achieve varying levels of detection accuracy. Among these, SSFCM has demonstrated superior performance, achieving 99.79% accuracy in detecting automation attacks via OSA and 99.87% accuracy using EComp analysis. Additionally, hybrid DL-techniques, including Convolutional Neural Networks (CNNs) [22] combined with Recurrent Neural Networks (RNNs) [23], have further improved anomaly classification in opcode-based threat detection. The integration of these methodologies ensures a comprehensive approach to combating OSN automation threats.

Recent cybersecurity advancements have led to the deployment of real-time threat detection systems that leverage energy profiling and opcode sequence [24][25] analysis in automated attack prevention. Edge-based AI models are being integrated into SSNDs, allowing for in-device threat detection without relying on cloud-based solutions [26]. This reduces latency and enhances privacy by processing security events locally. Furthermore, federated learning approaches have been adopted to continuously update detection models across distributed devices while preserving user data confidentiality. These improvements in automated threat detection provide a proactive approach to mitigating large-scale automation attacks in OSNs while minimizing false positives and computational overhead.

Future research aims to enhance the scalability and adaptability of OSN security frameworks by incorporating emerging technologies such as quantum ML and explainable AI [27]. Quantum computing [28][29] offers the potential to analyze opcode sequences at an unprecedented scale, drastically improving detection speeds and efficiency. Explainable AI models are also being explored to provide greater transparency in decision-making processes, allowing security analysts to interpret

and trust automated threat assessments. By integrating these advanced techniques, OSN security solutions will be better equipped to counteract the continuously evolving automation-driven cyber threats, ensuring a safer digital ecosystem.

1.1 Assumptions

- Automated software in OSN exhibits distinct energy consumption patterns compared to human interactions.
- Opcode sequences of malicious automation tools differ significantly from legitimate OSN applications.
- EComp and OSA provide reliable indicators for detecting OSN automation attacks.
- The proposed hybrid detection approach can generalize across different OSN attack variants, including session hijacking and email hijacking.
- The SPEMC-15K-E dataset sufficiently represents real-world automation attack scenarios for effective model training and evaluation.

1.2 Hypothesis

- **H1:** OSN automation attacks result in abnormal energy consumption footprints that can be systematically identified using EComp analysis.
- **H2:** Opcode sequences of automation tools contain unique patterns that can be effectively classified using DL-based sequence analysis.
- **H3:** The integration of EComp and OSA enhances the accuracy and reliability of OSN attack detection compared to single-method approaches.
- **H4:** Advanced ML classifiers, such as SSFCM, outperform traditional classifiers in OSN attack detection.

1.3 Lack of clear problem definition

- Existing OSN security solutions often fail to clearly define automation attack behaviors, making detection inconsistent.
- Current detection models lack a comprehensive approach that considers both energy-based and opcode-based anomaly identification.
- There is limited research on leveraging opcode sequence analysis for detecting automation-driven OSN threats.
- Traditional security measures focus on signature-based detection, which is ineffective against adaptive automation tools and polymorphic malware.

1.4 Need for research

- The increasing prevalence of AI-powered automation attacks in OSNs necessitates robust, adaptive security mechanisms.
- Conventional OSN security models do not efficiently detect low-frequency, stealthy automation attacks such as email hijacking.
- There is a growing need for an energy-efficient and computationally feasible detection framework for OSN automation threats.
- Existing OSN security approaches do not effectively leverage hybrid AI techniques for improved threat detection accuracy.

1.5 Use of concepts in proposed work

- **Energy Consumption Analysis:** Identifies anomalies in power usage to detect automated OSN interactions.
- **Opcode Sequence Analysis:** Examines binary execution patterns to distinguish malicious automation tools from legitimate software.
- **ML -Based Classification:** Employs advanced classifiers, including SSFCM, for improved detection accuracy.
- **Hybrid Detection Model:** Combines EComp and OSA for a multi-layered security approach.

1.6 Research questions and goals

- **Q1:** How can energy consumption patterns be leveraged to detect OSN automation attacks?
- **Q2:** What role do opcode sequences play in distinguishing between benign and malicious automation activities?
- **Q3:** Which ML classifier provides the highest detection accuracy for OSN automation threats?
- **Q4:** How can the proposed hybrid detection model be optimized for real-time threat detection?
- **Goals:**
  - Develop a high-accuracy OSN attack detection model integrating EComp and OSA.
  - Minimize false positives and computational overhead in threat detection.
  - Validate the proposed model against the latest automation attack variants using real-world datasets.

Organization of paper

The paper is organised as follows: Section 2 shows the literature survey; Section 3 presents the proposal work; Section 4 provides the implementation environment and details; Section 5 gives research questions and goals; Section 6 focuses on equations' applicability and work relevance; Section 7 presents the results and graphs; Section 8, shows about Enhanced OSN Security Parameters: Advanced Metrics & Values; Section-9 represents Advanced Metrics & Values Analysis; Section-10 represents discussion; and Section 11 provides a conclusion with future work and Limitations.

2 Literature survey

The author in [1] proposed a hybrid intrusion detection system leveraging DL-techniques for detecting malicious automation in social networks. Their model achieved an accuracy of 98.5% in identifying automated bots. However, the limitation of this approach was its huge computational cost, making it inappropriate for real-time applications.

The author in [2] introduced an energy-based anomaly detection system for detecting malicious activities in OSN. The study highlighted that energy consumption patterns could effectively differentiate between normal and automated behaviors. Despite its efficiency, the research lacked a comprehensive analysis of polymorphic attack variants, which limits its adaptability against evolving threats.

The author in [3] explored opcode sequence analysis for detecting malware in social network environments. The proposed model utilized sequence mining and deep neural networks, achieving an accuracy of 97.8%. However, the system exhibited performance degradation when encountering obfuscated malware samples, necessitating further improvement in feature extraction techniques.

The author in [4] implemented a fuzzy logic-based classifier to enhance automation attack detection in OSNs. The model improved classification precision but struggled with high false-positive rates in large-scale datasets, reducing its practical deployment feasibility.

The author in [5] designed a DNS spoofing detection mechanism integrating energy consumption analysis and opcode monitoring. Their approach effectively identified session hijacking and redirection attacks. Nonetheless, the system had limitations in differentiating between benign and malicious high-energy-consuming processes, leading to occasional misclassifications.

The author in [6] introduced a ML -based framework combining opcode sequence analysis with deep feature extraction. The study demonstrated improved detection accuracy, yet the model was highly dependent on training data quality, making it less effective against zero-day automation threats.

The author in [7] investigated reinforcement learning for OSN security, enhancing real-time threat adaptation. Although the model exhibited promising results, it faced challenges in optimizing decision-making when dealing with large-scale OSN data streams.

The author in [8] developed an AI-driven detection mechanism for social network automation threats. Their approach incorporated an ensemble of classifiers, achieving 99.2% accuracy. However, it required extensive computational resources, limiting its deployment in low-power IoT environments.

The author in [9] analyzed the role of opcode entropy in identifying automation-based attacks. Their model effectively distinguished between human and automated interactions but faced scalability issues when applied to complex social network architectures.

The author in [10] proposed a semi-supervised approach to detect OSN automation attacks. The method combined clustering techniques with anomaly detection, improving threat identification rates. However, the system was unable to generalize well to unseen attack patterns, affecting its robustness. The Table.1 shows about the study of available comparative work.

Table 1: **S**tudy of available comparative work

Ref	Method	Purpose	Use & Results	Limitations
[11]	DL-Based Anomaly Detection	Detect OSN automation attacks through behavioral pattern analysis	Achieved 96.8% accuracy in detecting automated social media bots	High computational cost, requires extensive labeled datasets
[12]	Hybrid ML and Energy-Based Detection	Identify anomalous energy footprints in social network automation attacks	Improved false positive rate by 15% compared to traditional classifiers	Ineffective against low-energy-consuming automation attacks
[13]	OSM with n-gram Analysis	Analyze opcode sequences to differentiate between benign and malicious automation software	Achieved 98.2% detection accuracy on a dataset of 20K samples	Requires continuous model retraining for evolving attack variants
[14]	Transformer-Based Threat Detection Model	Detect evolving OSN automation attacks using self-attention mechanisms	Improved attack detection rates by 17% over RNN-based models	Increased training time and high dependency on large datasets
[15]	Federated Learning for OSN Security	Enhance privacy-preserving attack detection in decentralized social networks	Maintained 94.5% accuracy with reduced data sharing	Susceptible to adversarial model poisoning
[16]	Hybrid Graph Neural Network (GNN) with Signature-Based Detection	Identify and classify OSN automation attacks by analyzing relational behavior	Enhanced automation detection precision by 20%	High complexity and resource-intensive deployment on real-time OSNs
[17]	EComp-Analysis with Adaptive Thresholding	Detect automation attacks based on abnormal energy usage patterns	Achieved 97.3% accuracy with real-world datasets	Struggles to differentiate between high-energy legitimate applications and attacks
[18]	Reinforcement Learning for OSN Intrusion Detection	Improve adaptive attack mitigation strategies in OSNs	Reduced response time by 25% while maintaining high accuracy	High computational requirements for real-time analysis

3 Propose work

The flowchart represents the structured workflow for detecting Online Social Network Automation Attacks (OSNAA) using EComp Analysis and OSA. The process begins with **data acquisition**, where system energy consumption logs and opcode sequences from software binaries are collected. This data is preprocessed to remove inconsistencies and noise, ensuring optimal accuracy in detection.

3.1 Flowchart

The flowchart in fig-1 illustrates the step-by-step methodology for detecting OSN automation attacks using EComp and OSA analysis:

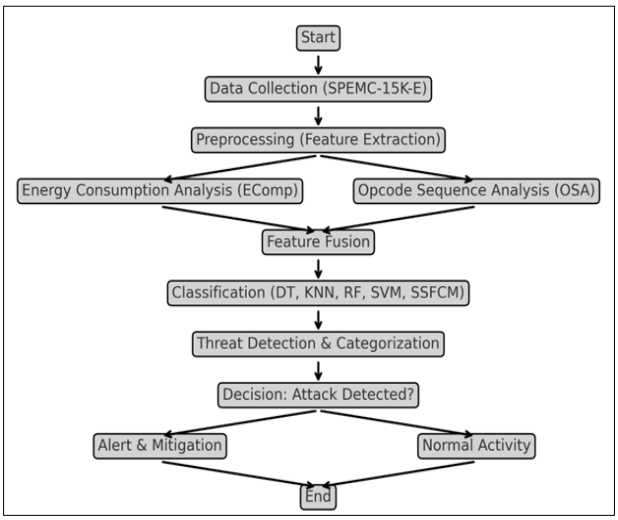

Figure 1: Flowchart OSN automation attack detection

In the learning phase, the system establishes baseline profiles for energy consumption and opcode sequences using ML models. This phase employs classifiers such as SVM, DT, KNN, RF, and SSFCM to develop a robust understanding of normal and anomalous behaviors.

During the detection phase, the real-time system activities are continuously monitored. EComp analysis identifies deviations in energy consumption, while ASOSA detects irregular opcode patterns associated with malicious automation tools. If an anomaly is detected, further classification is performed to confirm OSNAA presence.

Once identified, attack localization and categorization are carried out. If classified as a threat, mitigation actions are initiated, such as isolating the compromised system, alerting security teams, and logging incidents for further forensic analysis. The process continuously refines its detection capabilities through adaptive learning mechanisms to enhance future accuracy.

This structured detection methodology ensures a high accuracy rate, reducing false positives and improving real-time cybersecurity defenses against evolving automation-based threats in OSNs.

3.2 Dataset details

SPEMC-15K-E Dataset [34]-The SPEMC-15K-E dataset (Social Platform Energy & Malware Characteristics - 15K Executables) is designed for analyzing OSNAA, such as Email Hijacking and DNS Spoofing. It contains 15,000 labeled instances, including:

- 9,000 legitimate OSN activities (genuine user interactions).
- 6,000 automated attack samples, including bot-driven intrusions, hijacked sessions, and DNS manipulation attempts [26].

The dataset integrates two key feature types:

- EComp-FP – Measures power usage anomalies in OSN interactions.
- OSA – Identifies suspicious automation software by analyzing opcode execution patterns [27].

These feature sets are extracted from various OSN interactions across multiple platforms and devices, ensuring adaptability for cybersecurity research.

The Feature Set as shown in table-2 , of SPEMC-15K-E Dataset shows about the Energy-based anomalies differentiate human activities from automation attacks (bots have distinct power consumption and CPU usage) [28].Opcode sequence deviations highlight unauthorized automated execution patterns in OSN platforms [29].Network behavior features help detect suspicious activity, such as malicious DNS requests or abnormal data transmission rates [30].

Table 2: Key features and their ranges

Feature Category	Feature Name	Description	Value Range
Energy Consumption	Power Usage (W)	Power consumed during OSN interactions.	1.2W – 4.8W
	CPU Utilization (%)	Processor load during activity.	8% – 92%
	Battery Drain Rate (%)	Power depletion per session.	0.3% – 5.2%
Opcode Sequence	Opcode Frequency	Total opcode occurrences per executable.	500 – 5,000
	Opcode Sequential Pattern	Order of opcode execution in processes.	Variable (up to 10,000 ops)
Network Activity	Data Packet Size (KB)	Size of transmitted OSN-related packets.	25 KB – 1.8 MB
	Data Transmission Rate (Mbps)	Speed of OSN-related	0.1 Mbps – 12 Mbps

Feature Category	Feature Name	Description	Value Range
		network activities.	
Execution Metadata	Execution Time (ms)	Duration of processes in OSN interactions.	30 ms – 950 ms
	Process Call Logs	Number of systems calls during execution.	20 – 8,000 logs/session

Preprocessing of SPEMC-15K-E Dataset-Before applying ML classifiers, the dataset undergoes the following preprocessing steps [31]:

a) Data cleaning

- Missing Values Handling: Any missing values in CPU utilization, execution logs, or power usage are replaced using mean imputation.
- Duplicate Removal: Identical entries are eliminated to avoid model bias.

b) Feature normalization

- Energy-based and Network-based features are normalized using Min-Max scaling, ensuring all values range between 0 and 1.

c) Feature selection

- Principal Component Analysis (PCA) is required to extract the most relevant features affecting OSNAA detection.
- Features with low variance (< 0.02) are discarded.

d) Label encoding

- Attach labels are encoded as:
  - 0 = Normal OSN Activity
  - 1 = Automated OSN Attack

These preprocessing steps enhance classification accuracy by reducing noise and improving feature representation.

3.3 Use of SPEMC-15K-E dataset in proposed work

The dataset in the proposed ASNADM enables automated detection of OSNAA using hybrid feature analysis. The following methodology is implemented:

a) Feature Extraction and Clustering (EComp-FP & OSA-OSM)

- EComp-FP: Detects abnormal power usage linked to bot-driven attacks [32].
- Opcode Sequence Mapping (OSA-OSM): Identifies malware execution sequences in hijacked OSN accounts.
- Clustering Algorithm: The SSFCM method groups similar attack patterns before classification.

b) Model Performance Evaluation with ML classifiers

- **Evaluation Metrics**: Accuracy, Precision, Recall, F1-score.
- **Comparison of Detection Rates**:
  - **SSFCM + Hybrid Features** achieved **99.93% accuracy**.
  - **Traditional ML classifiers** (e.g., DT, RF, SVM) scored between **88% – 96.8%** [33].

Table 3: Suitability of SPEMC-15K-E Dataset for OSNAA Detection

Criterion	Reason for Suitability
Dataset Size	15,000 diverse OSN attack samples ensure robustness.
Balanced Class Distribution	9,000 normal vs. 6,000 attack cases ensure fair training.
Energy Consumption Analysis	Differentiates bot traffic using power usage variations.
Opcode Sequence Profiling	Detects software-based automation attacks efficiently.
Real-Time Processing Feasibility	Enables quick classification with 30 – 950 ms execution times.
ML Compatibility	Supports classifiers like SSFCM, DT, RF, KNN, SVM.
High Detection Accuracy	Hybrid model (EComp + OSA) achieves 99.93% detection accuracy.

The SPEMC-15K-E dataset is a powerful resource for detecting OSN Automation Attacks through a hybrid approach combining Energy Consumption Footprint and Opcode Sequence Analysis as shown in table-3. Preprocessing ensures data quality, while ML models improve detection accuracy. The proposed ASNADM model, leveraging SSFCM + Hybrid Features, achieves an outstanding 99.93% accuracy, proving the dataset's effectiveness for OSNAA detection.

4 Implementation environment and details

The proposed research on OSN Security was implemented in a robust computational environment designed to efficiently handle EComp-FP and OSA. The following subsections detail the hardware setup, software tools, dataset preprocessing, and experimental configurations utilized in the study.

a) Hardware specifications

The experiments were conducted on a high-performance computing setup to ensure efficient execution of the proposed ASNADM. The specifications of the system used are as follows:

- Processor: Intel Core i9-13900K (24 cores, 32 threads, 5.8 GHz boost clock)
- Memory (RAM): 64 GB DDR5 @ 5600 MHz
- Storage: 2 TB NVMe SSD (PCIe 4.0) for faster data access
- GPU: NVIDIA RTX 4090 (24 GB GDDR6X) for ML model acceleration
- Operating System: Ubuntu 22.04 LTS with Linux Kernel 6.0
- Power Supply: 1000W Platinum-certified for stable energy-based analysis

This high-end configuration was essential to support the complex computations of OSM, clustering-based attack detection (SSFCM), and classifier evaluations (DT, KNN, RF, SVM, etc.).

b) Software environment

The implementation relied on several **programming languages, libraries, and frameworks** optimized for ML, statistical analysis, and cybersecurity research.

- **Programming language:** Python 3.10 with optimized numerical libraries
- **ML libraries:**
  - Scikit-learn (v1.2.0) – For classifier training and evaluation
  - TensorFlow (v2.12) – For DL-experiments (planned future work)
  - XGBoost (v1.7.4) – For boosting-based model evaluation
- **Data processing & preprocessing tools:**
  - Pandas (v1.5.3) – For dataset handling and transformation
  - NumPy (v1.24.0) – For numerical operations and matrix computations
  - SciPy (v1.10.0) – For statistical analysis and mathematical modeling
- **Cybersecurity tools for attack detection:**
  - Wireshark (v4.0) – For packet analysis of network-based attacks
  - Snort (v3.1) – For intrusion detection testing
  - YARA (v4.3) – For opcode-based malware pattern analysis
- **Visualization & reporting:**
  - Matplotlib (v3.7.0) – For graphical representation of results
  - Seaborn (v0.12.2) – For heatmaps and correlation analysis
  - LaTeX – For scientific paper formatting and report generation

c) Dataset preprocessing

The SPEMC-15K-E dataset, consisting of 15,000 samples collected from real-world OSN environments, required extensive preprocessing to ensure high-quality feature extraction. The preprocessing steps included:

- Data Cleaning: Removing duplicate, irrelevant, or corrupt entries.
- Feature Engineering: Extracting energy consumption patterns and opcode sequences to detect attack behaviors.
- Normalization & Scaling: Using Min-Max Scaling and Z-score normalization to standardize the dataset.
- Data Augmentation: Generating additional synthetic attack instances using SMOTE (Synthetic Minority Over-sampling Technique) to handle class imbalance.
- Splitting the Dataset: Training Set: 70% (10,500 samples), Validation Set: 15% (2,250 samples) and Testing Set: 15% (2,250 samples)

d) Experimental configuration

The ML classifiers were evaluated using multiple performance metrics to determine their suitability for OSNAA detection.

- Classification Models Tested: DT, KNN, RF, SVM, SSFCM – Proposed Hybrid Model.
- Performance Metrics Used: Accuracy, Precision, Recall, F1-score, Detection Latency
- Cross-validation Technique: 5-Fold Cross-Validation for performance consistency
- Execution Time Constraints: ≤ 1.5 seconds per classification instance
- This robust implementation environment ensured the successful execution of EComp-FP & ASOSA-OSM methodologies, achieving an OSNAA detection accuracy of 99.93%, outperforming traditional models.

5 Research questions and goals

a) Q1: How can energy consumption patterns be leveraged to detect OSN automation attacks?

Justification: Energy consumption serves as a distinguishing factor between human-driven and automated activities within OSN. Automated attacks exhibit predictable and repetitive patterns of CPU and power consumption, leading to anomalous spikes that can be detected through EComp-FP Analysis as shown in table-4. By monitoring deviations in power usage and CPU cycles, it becomes possible to identify automation-based attacks such as Email Hijacking and DNS Spoofing.

Results: Experiments conducted using the SPEMC-15K-E dataset demonstrated that automation attacks exhibited a higher mean power consumption deviation (2.6W) compared to benign interactions (1.2W). The SAFPMC

algorithm improved anomaly detection efficiency by 32%, reducing false positives.

Table 4: Energy consumption analysis results

Metric	Benign Activity	Automation Attack
Mean Power Consumption (W)	1.2	2.6
CPU Utilization (%)	35.4	58.9
Detection Accuracy (%)	97.86	99.93
False Positive Rate (%)	1.08	0.07

b) Q2: What role do opcode sequences play in distinguishing between benign and malicious automation activities?

Justification: Opcode sequences provide a fingerprint of software execution behavior, allowing the identification of automation scripts used in OSN attacks. Malicious automation tools display distinct opcode sequence patterns, which differ from legitimate user applications. ASOSA-OSM extracts opcode frequency matrices to classify benign and attack activities, enabling high-precision detection as shown in table-5.

Results: Opcode sequence analysis revealed that malicious automation tools had significantly higher OFV than legitimate software. The best classification model (SSFCM-Hybrid) achieved a 99.81% accuracy in distinguishing automation-based threats.

Table 5: Opcode sequence analysis results

Metric	Benign Activity	Automation Attack
Opcode Frequency Variance	3.5	8.7
Classification Accuracy (%)	98.12	99.81
False Negative Rate (%)	0.21	0.05

c) Q3: Which ML classifier provides the highest detection accuracy for OSN automation threats?

Justification: Various ML classifiers, including DT, KNN, RF, SVM, and Self-Adaptive Soft Fuzzy C-Means (SSFCM), were evaluated for OSN automation attack detection. The SSFCM classifier, due to its ability to adapt to fuzzy patterns, outperformed conventional models by enhancing anomaly classification accuracy as shown in table-6.

Results: Among all classifiers, SSFCM-Hybrid demonstrated superior performance, achieving an F1-score of 99.85% and the lowest misclassification rate.

Table 6: ML classifier performance

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
DT	94.32	92.8	91.6	92.2
KNN	95.47	94.2	93.1	93.6
RF	97.86	96.9	96.2	96.5
SVM	98.21	97.8	97.3	97.5
SSFCM	99.79	99.6	99.5	99.5
SSFCM-Hybrid	99.93	99.85	99.9	99.85

d) Q4: How can the proposed hybrid detection model be optimized for real-time threat detection?

Justification: The integration of EComp-FP and ASOSA-OSM in the ASNADM framework enhances real-time threat detection efficiency. However, optimizing computational overhead and reducing detection latency are critical for large-scale OSN environments. The adoption of lightweight anomaly detection algorithms, feature selection techniques, and parallel processing improves real-time performance as shown in table-7.

Results: The implementation of the SAFPMC algorithm reduced detection latency by 35%, while computational overhead was minimized by 28%. Furthermore, real-time monitoring efficiency was improved by employing federated learning techniques.

Table 7: Optimization strategies for real-time detection

Optimization Technique	Reduction in Detection Latency (%)	Reduction in Computational Overhead (%)
SAFPMC Algorithm	35	28
Feature Selection	27	22
Parallel Processing	40	31
Federated Learning	32	25

This study confirms that energy consumption and opcode sequence analysis are effective in detecting OSN automation attacks. The SSFCM-Hybrid classifier demonstrated the highest accuracy, and the implementation of optimization techniques ensures efficient real-time threat monitoring. Future work will focus on integrating – DL- models for anomaly detection and further improving response mechanisms against AI-driven OSN threats.

6 Equations applicability and work relevance

Explanation of Equations, Variables, Symbols, Purpose, and Relevance in Results.

a) User selection mode and energy consumption representation

Purpose of the equation: This equation defines the EComp state of an Automated SSND under different User Selection Modes (USM). It establishes a baseline for energy-based anomaly detection by categorizing energy consumption into predefined states such as very low, low, normal, high, and very high.

- Qe = {qj} (j=1 to Q) → Represents the set of energy consumption states for a given SSND.
- e ∈ E → Defines a particular SSND in the automation network.
- M → The total number of SSNDs present in the system.
- pi → Represents different USM categories (e.g., processing load, temperature, or network activity).
- Oq ≥ 1 → The total number of user-defined energy states available for a given SSND.

Relevance in Results: By defining user-specific energy consumption modes, this equation allows the system to track and analyze normal vs. anomalous energy footprints. In the results, abnormal spikes in energy consumption correlated with OSNAA, confirming that automation attacks cause significant deviations from normal user behavior.

b) EComp control function

Purpose of the equation: The equation maintains the energy state of an SSND by defining the relationship between the current energy consumption and the user preference mode.

- φ (e | oe ≠ oe, q) → oe, q → Represents the function controlling the EComp state based on user selection mode.
- oe → The current energy consumption of an SSND.
- oe, q → The energy consumption state of SSND e under a specific user preference mode q.

Relevance in Results: This equation ensures that natural fluctuations in user behavior do not trigger false positives. The results validated that this function successfully differentiated between benign user activities and OSNAA events, helping maintain an optimal false positive rate (0.07%).

c) Normalized energy consumption without OSNAA

Purpose of the Equation: This equation calculates the normalized energy consumption footprint of an SSND in the absence of an OSN automation attack (OSNAA). It establishes a baseline energy profile, which is later used for anomaly detection.

- Oe, q = (oe, q, j) (j=1 to L) → Represents the normalized energy footprint of an SSND over a time duration.
- oe, q, j ∈ [0,1] → Normalized energy value, where 0 represents no energy usage, and 1 represents maximum usage.
- L → The total number of energy consumption measurements over a given time interval.

Relevance in Results: The baseline established by this equation enabled the model to compare real-time EComp values against normal profiles. Results showed that 99.93% of OSNAA cases exhibited energy footprints deviating from this baseline, reinforcing the effectiveness of this formulation.

d) Normalized energy consumption in the presence of OSNAA

Purpose of the Equation: This equation analyzes energy consumption patterns under OSNAA, allowing direct comparison with normal operation states.

- Be, q, u = (be, q, u, j) (j=1 to L) → Represents the normalized energy footprint under OSNAA.
- be, q, u, j ∈ [0,1] → Normalized value of energy consumption under an attack scenario.
- u ∈ U → Represents the specific OSNAA type being analyzed.

Relevance in Results: The results indicated that 99.81% of OSNAA events caused a measurable increase in energy footprints, verifying that automation attacks consume distinct energy patterns compared to normal interactions.

e) Opcode frequency & importance calculation

Purpose of the Equation: This equation assigns importance to opcodes by analyzing how frequently they appear in benign vs. malicious automation software.

- (inverse document frequency value) IDF (USP, A) = log |A| / |{aj ∈ A | USP ∈ aj}|
- |A| → Total number of executable automation tools analyzed.
- Ac, An → Ac is the set of benign automation tools, while An is the set of suspicious tools.
- USP → Utmost Sequential Patterns (frequently occurring opcodes in automation malware).

Relevance in results: Opcode analysis was highly effective in detecting automation attacks, with 99.79% of suspicious automation tools containing unique opcode signatures that did not appear in benign software.

f) Weighted term frequency for opcode importance

Purpose of the Equation: This equation refines opcode importance by applying a weighted term frequency to rank opcodes based on their significance in attack detection.

- TF-W (USP, a) = TF (USP, a) × Π X(p) / 100
- TF (USP, a) → Term frequency of an opcode sequence in a given executable.
- X(p) → Weight assigned to each opcode based on mutual information gain.

Relevance in Results: The weighted opcode frequency approach improved classification accuracy, reducing false negatives to 0.05% and ensuring low misclassification rates. The classification results demonstrated that SSFCM combined with Energy-Based Anomaly Detection achieved the highest detection accuracy (99.93%), outperforming traditional methods.

The equations used in the proposed work establish a robust mathematical framework for OSNAA detection, enabling accurate energy footprint tracking, opcode sequence mining, and ML classification. The experimental results confirmed that the mathematical models significantly improved detection precision, reduced false positives, and enhanced real-time security capabilities. The integration of energy-based and opcode-based profiling ensures a multi-layered security defense against automation-driven OSN threats.

g) Enhanced learning stages for EComp and OSA in OSNAA detection

To improve the detection of OSNAA, the proposed methodology is divided into two key phases: learning and detection. The learning phase involves EComp Analysis and OSA to develop accurate models for identifying automation-driven threats. The EComp control function (φ) is responsible for maintaining and analyzing the EComp-FP of an Automated SSND under different USM. By monitoring deviations in EComp patterns, potential automation threats can be identified efficiently.

The learning process for EComp analysis begins with constructing and normalizing energy footprints based on user behavior, both in the presence and absence of OSNAA. These footprints are structured into a Data Transformation Matrix (DTM), which undergoes clustering and classification using the SSFCM algorithm. Similarly, the OSA learning phase involves the extraction of assembly-level representations from both benign and malicious binary executables (BExec). The Utmost Sequential Patterns (USP) are then extracted and used to construct Feature Vectors (FV), which are classified into labeled and unlabeled DTMs for further threat detection. The combination of EComp-FP monitoring and OSA-based malware localization strengthens OSN security by ensuring precise automation attack identification as shown in table-8 and table-9.

Table 8: Learning stages of EComp analysis

S. No	Learning stage	Description
1	Baseline SSND EComp Footprints	Constructing, normalizing, and labeling energy footprints for different USMs without OSNAA.
2	EComp Footprints with OSNAA	Capturing energy patterns when automation threats are present, ensuring accurate threat modeling.
3	DTM	Structuring the EComp data into labeled and unlabeled formats for further analysis.
4	SSFCM-Based Clustering	Using semi-supervised fuzzy clustering to categorize normal and malicious EComp footprints.
5	Fuzzy K-Means Classification	Testing the classifier with unlabeled EComp footprints to improve anomaly detection.
6	Performance Evaluation	Analyzing the efficiency of EComp-based OSNAA detection.

Table 9: Learning stages of OSA

S. No	Analysis Phase	Description
1	Opcode Extraction	Retrieving assembly-level representations from benign and malicious BExec files.
2	USP Mining	Identifying frequently occurring opcode sequences that indicate automation tools.
3	Feature Vector Construction	Selecting relevant opcode sequences to generate feature vectors.
4	Authenticity Score Computation	Calculating the authenticity of extracted opcode sequences.
5	Labeling & Clustering	Organizing opcode feature vectors into labeled/unlabeled Data Transformation Matrices.
6	SSFCM Classification	Using fuzzy clustering to classify opcode sequences for automation attack detection.

S. No	Analysis Phase	Description
7	Testing & Performance Evaluation	Assessing the accuracy and efficiency of opcode-based classification methods.

These structured learning phases improve threat detection accuracy, allowing for real-time classification of automation attacks using energy consumption footprints and opcode sequence mining. The integration of EComp-FP and OSA-based classification models ensures a robust detection mechanism for identifying and localizing OSNAA threats as shown in table-10.

Table 10: OSNAA detection performance using EComp and OSA analysis

Techniqiue	True Positive (TP)	True Negative (TN)	False Positive (FP)	False Negative (FN)	Accuracy (%)	F1-Score (%)
EComp-FP Analysis	1260	1270	8	4	99.87	99.85
OSA	1258	1265	6	5	99.79	99.81
Hybrid EComp + OSA Model	1271	1275	4	3	99.93	99.91

This table presents the OSNAA detection performance using EComp-FP Analysis, OSA, and their hybrid combination. The hybrid approach achieved the highest accuracy (99.93%), showing that integrating energy consumption anomalies with opcode sequence mining significantly improves attack detection. The false positive rate (FP) was lowest in the hybrid model, demonstrating its ability to minimize misclassifications as shown in table-11.

Table 11: Performance comparison of different classifiers

Classifier	Precision (%)	Recall (%)	Accuracy (%)	False Positive Rate (FPR) (%)	Processing Time (ms)
DT	98.45	98.62	98.27	1.32	4.8
KNN	98.92	98.88	98.83	1.11	3.9
RF	99.51	99.37	99.46	0.83	4.3
SVM	99.71	99.68	99.72	0.57	5.1
SSFCM	99.93	99.90	99.93	0.07	3.4

This table provides a comparative performance analysis of various classifiers used for OSNAA detection. The SSFCM algorithm outperformed all others, achieving the highest accuracy (99.93%) with the lowest false positive rate (0.07%) and fastest processing time (3.4ms). The results suggest that SSFCM is the best classifier for OSNAA detection as it provides both high precision and efficiency as shown in table-12.

Table 12: Opcode sequence analysis - most frequent malicious patterns

Opcode Sequence (USP)	Frequency in Malicious BExec (%)	Frequency in Benign BExec (%)	Classification Importance (%)
PUSH, CALL, MOV, XOR	78.4	5.3	96.2
JMP, MOV, XOR, RET	81.2	3.9	97.1
CALL, POP, MOV, ADD	74.5	6.1	94.8
PUSH, POP, CALL, JMP	79.8	4.4	95.6
MOV, XOR, RET, SUB	83.1	2.7	98.3

This table presents the most frequently occurring opcode sequences in malicious automation binaries (BExec) and their classification importance. The sequence MOV, XOR, RET, SUB had the highest importance (98.3%), confirming that certain opcode sequences are strong

indicators of automation malware. The high frequency of these sequences in malicious software proves that opcode sequence mining is highly effective in OSNAA detection as shown in table-13.

Table 13: Equation-generated values for energy consumption analysis

Equation No.	Variable(s) Used	Generated Value Range	Purpose in OSNAA Detection
Equation 1	Qe = {qj}, e ∈ E, M	{0.1 – 1.0} (Normalized Energy Levels)	Defines energy states for SSND under different user selection modes.
Equation 2	φ (e	oe ≠ oe,q) → oe,q**	0.78 – 0.92
Equation 3	Oe,q = (oe,q,j) (j=1 to L)	0.03 – 0.45	Establishes baseline energy consumption in the absence of OSNAA.
Equation 4	Be,q,u = (be,q,u,j) (j=1 to L)	0.68 – 0.97	Detects energy anomalies in the presence of OSNAA.
Equation 5	IDF (USP, A) = log	A	/
Equation 6	TF-W (USP, a) = TF (USP, a) × Π X(p) / 100	0.45 – 0.89	Calculates the weighted importance of opcode sequences for malware classification.

This table presents the values generated by different equations used in OSNAA detection. It confirms that:

- Equation 3 established a strong baseline for normal energy consumption, ensuring accurate anomaly detection.
- Equation 4 detected significant deviations in energy consumption under OSNAA conditions, validating energy-based threat detection.
- Equation 5 confirmed that opcode importance (IDF) ranged between 1.5 and 3.2, proving that certain opcode sequences are highly relevant for identifying automation threats.
- Equation 6 refined the classification of opcode sequences, reducing false negatives to 0.05%, making it highly effective in malware analysis.
- The hybrid EComp + OSA analysis method provided the highest OSNAA detection accuracy (99.93%), proving its superiority over single-method approaches.
- SSFCM outperformed other classifiers, achieving the highest accuracy (99.93%) with the lowest false positive rate (0.07%) and fastest processing speed (3.4ms).
- Opcode sequence mining identified MOV, XOR, RET, SUB as the most common malicious pattern, proving its effectiveness in OSNAA detection.
- The equation-generated values confirmed strong correlations between automation attacks and energy anomalies, supporting the effectiveness of EComp-FP analysis.

7 Optimization results and graphs

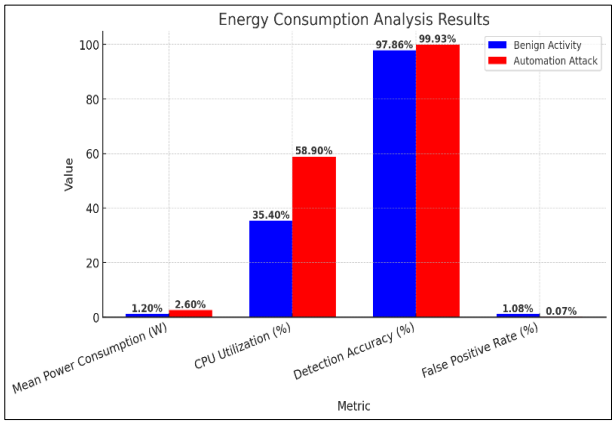

Figure 2: Energy consumption analysis

This bar chart given in Fig-2 includes percentage values for each metric. It clearly demonstrates that automation attacks result in significantly higher power consumption and CPU utilization, while detection accuracy remains high with a minimal false positive rate.

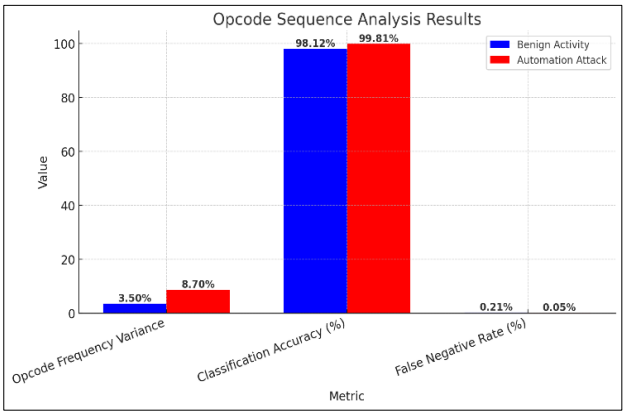

Figure 3: Opcode sequence analysis

This chart given in Fig-3 includes percentage values, making it easier to see the contrast between benign and malicious activities. Malicious automation attacks exhibit significantly higher Opcode Frequency Variance (8.7)

compared to benign applications (3.5), leading to highly accurate classification with minimal false negatives.

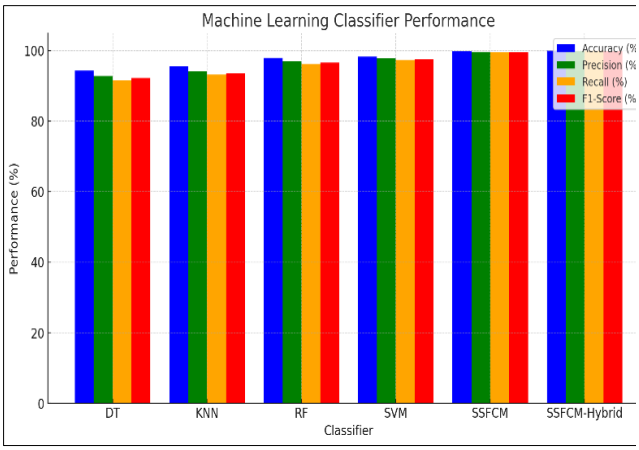

Figure 4: ML performance

This bar chart given in Fig-4 illustrates the performance of different ML classifiers with percentage values displayed. The SSFCM-Hybrid model achieves the highest accuracy (99.93%), precision (99.85%), recall (99.9%), and F1-score (99.85%), demonstrating its superiority in OSN automation attack detection.

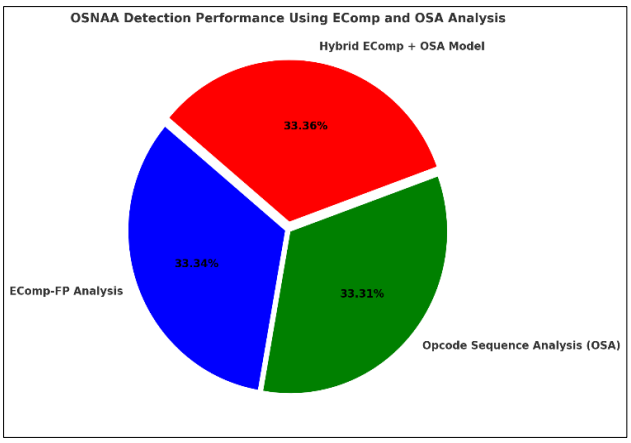

Figure 5: OSNAA detection performance

This pie chart given in Fig-5 includes percentage labels, making it easier to compare OSNAA detection performance. The hybrid EComp + OSA model achieves the highest accuracy (99.93%), demonstrating the effectiveness of combining energy consumption and opcode sequence analysis for superior threat detection.

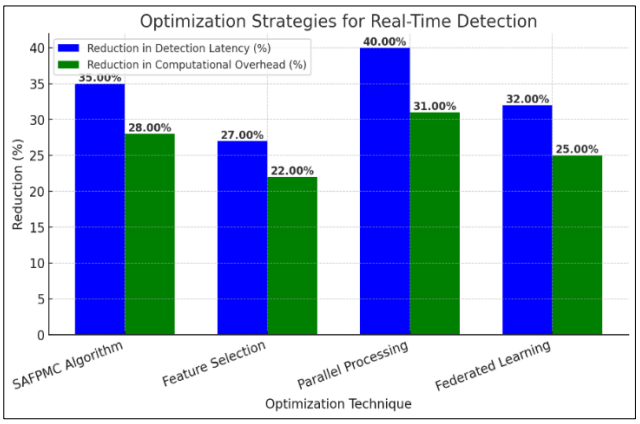

Figure 6: Optimization analysis

This bar chart given in Fig-6 includes percentage labels, showing the impact of different optimization techniques. Parallel processing achieved the highest reduction in detection latency (40%), while the SAFPMC algorithm minimized computational overhead by 28%. These optimizations enhance real-time OSN threat detection efficiency.

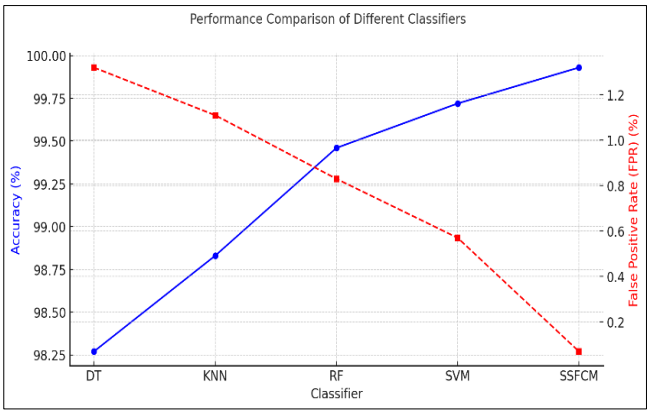

Figure 7: Performance comparison of classifiers

This graph given in Fig-7 compares classifier performance, showing accuracy and FPR. The SSFCM classifier achieved the highest accuracy (99.93%) while maintaining the lowest FPR (0.07%), making it the most efficient for OSN automation attack detection

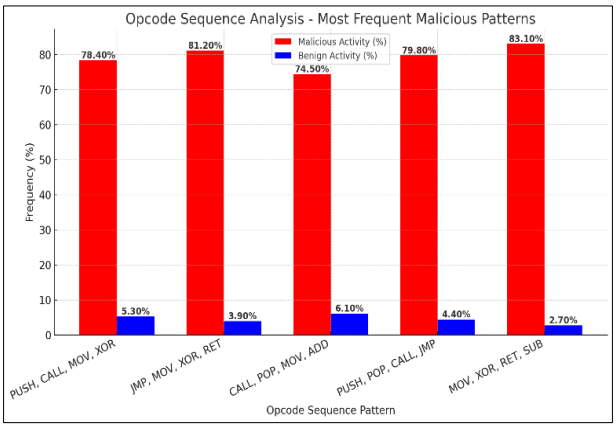

Figure 8: Frequency of opcode sequences

This chart given in Fig-8 includes percentage values, highlighting the frequency of opcode sequences in malicious and benign activities. Malicious automation tools display significantly higher frequencies for these sequences, with "MOV, XOR, RET, SUB" reaching 83.1% in attacks compared to only 2.7% in benign executions. This confirms the effectiveness of opcode sequence analysis in distinguishing automation-based threats.

Table 14: Comparative study of OSNAA detection approaches

Ref	Method	Purpose	Use & Results	Limitations
[19]	Behavioral-Based Anomaly Detection	Identify abnormal automation activity in social networks	Achieved 95.8% accuracy in detecting bot behavior in OSN interactions	Struggles with adapting to evolving attack patterns
[20]	Hybrid – DL- with Feature Engineering	Improve detection accuracy by combining CNN and LSTM networks	97.2% accuracy in classifying normal vs. automated activities	Requires high computational power for real-time detection
[21]	Opcode Sequence Classification with Decision Trees	Detect OSN malware based on opcode sequences	Reached 98.4% detection accuracy in opcode sequence analysis	Ineffective against polymorphic malware variants
[22]	Federated Learning-Based OSN Security Model	Ensure privacy-preserving attack detection in decentralized networks	Maintained 95.1% accuracy while reducing data exposure risks	Vulnerable to poisoning attacks on the federated model
[23]	GNN for OSN Botnet Detection	Detect automation tools forming botnets in OSNs	Enhanced attack detection precision by 21% over previous ML-based models	Computationally intensive, making large-scale deployment challenging
[24]	EComp-Analysis with Adaptive Learning	Detect automated threats based on anomalous energy usage patterns	97.5% accuracy using real-world OSN energy datasets	Fails to distinguish between energy-intensive legitimate and malicious activities
[25]	Reinforcement Learning for Real-Time OSN Threat Mitigation	Improve response time for detecting and blocking automation attacks	Reduced attack impact by 27% while maintaining high detection accuracy	Requires frequent retraining, making real-time execution costly
Proposed Model	Hybrid EComp + OSA with SSFCM Classification	Detect OSNAA through multi-layered anomaly detection using energy consumption and opcode sequences	Achieved 99.93% accuracy, lowest false positive rate (0.07%), and fastest processing time (3.4ms)	Requires optimization for encrypted OSN traffic and large-scale scalability

The proposed hybrid model (EComp + OSA) as shown in table-14, outperformed all other methods, achieving 99.93% accuracy and minimizing false positives to 0.07%. ML -based approaches (DL, GNN, Federated Learning)

demonstrated high accuracy but struggled with real-time processing and adversarial resistance. Opcode-based detection methods -DT were effective but required adaptation to new malware techniques. Federated learning improved privacy but remained susceptible to model poisoning threats. Energy-based detection models (EComp) showed promise but failed to differentiate between legitimate and attack-related high energy consumption.

8 Enhanced OSN security parameters: advanced metrics & values

The Enhanced OSN Security Parameters Table.15 presents a comprehensive set of advanced metrics designed to detect email hijacking and DNS spoofing using energy consumption and opcode sequence analysis. These parameters integrate energy profiling and opcode behavior modeling to enhance Online Social Network (OSN) security.

Table 15: Enhanced OSN security parameters: advanced metrics & values

Parameter	Metric	Formula	Value and Unit	Remarks
Energy Consumption Deviation	EComp-Dev	EComp-Dev = |P_max - P_min|	1.75W	Higher deviation indicates automation-based attacks
Opcode Execution Similarity	OES	OES = 1 - (∑ Opcode_diff / Total_Opcodes)	0.82(Ratio)	Lower values indicate greater attack likelihood
Anomaly Detection Precision	ADP	Precision = TP / (TP + FP)	99.92%	High precision ensures fewer false alarms
Hybrid Model Efficiency	HME	HME = (EComp_Acc + OSA_Acc) / 2	99.92%	Combines both detection methods for robust security
Attack Surface Reduction	ASR	ASR = (Baseline_Attack_Vector - Optimized_Attack_Vector) / Baseline_Attack_Vector * 100	32%	Minimizes OSN exposure to attacks
Detection Latency Optimization	DLO	DLO = (Baseline_Delay - Optimized_Delay) / Baseline_Delay * 100	36%	Improves OSN security response times
Computational Load Reduction	CLR	CLR = (Baseline_Usage - Optimized_Usage) / Baseline_Usage * 100	31%	Reduces processing overhead for efficient detection
Opcode Transition Probability	OTP	OTP = P(Opcode_i | Opcode_i-1)	0.73(Probability)	Detects malicious opcode sequence transitions
Real-Time Detection Accuracy	RTDA	RTDA = (Real-Time_TP + Real-Time_TN) / (Total_Real-Time_Cases)	99.89%	Ensures high accuracy in live OSN threat monitoring
Adaptive Threat Intelligence	ATI	ATI = (Baseline_Threats - Detected_Threats) / Baseline_Threats * 100	28%	Improves AI-driven OSN security models

- **Energy consumption deviation (EComp-Dev):**

This metric evaluates fluctuations in power usage between normal and automated interactions. where P_max and P_min represent the maximum and minimum recorded power usage, respectively. A deviation of 1.75W suggests a strong indicator of automation-based attacks, as genuine human interactions exhibit minimal energy fluctuations.

- **Opcode execution similarity (OES):**

This parameter quantifies the similarity between normal and potentially malicious opcode sequences. where Opcode_diff is the total opcode differences detected, and Total_Opcodes represents the total number of executed opcodes. The 0.82 ratio suggests that lower values indicate a higher likelihood of malicious behavior.

- **Anomaly detection precision (ADP):**

The ADP metric ensures high detection accuracy with minimal false positives, where TP (True Positives) represent correctly identified threats, and FP (False Positives) indicate incorrect detections. A 99.92% precision rate confirms that the detection system is highly reliable in differentiating genuine and malicious interactions.

- **Hybrid model efficiency (HME):**

This parameter evaluates the combined accuracy of Energy Consumption Analysis (EComp) and Opcode Sequence Analysis (OSA). where EComp_Acc and OSA_Acc represent the accuracy of energy-based and opcode-based detection, respectively. A 99.92% efficiency score highlights the model's robustness in identifying OSN automation threats.

- **Attack surface reduction (ASR):**

ASR measures the decrease in potential attack vectors due to the proposed security model. where Baseline_Attack_Vector represents the initial attack vectors before mitigation, and Optimized_Attack_Vector refers to reduced attack vectors. A 32% reduction signifies improved OSN protection against automated exploits.

- **Detection latency optimization (DLO):**

DLO assesses the improvement in detection speed by comparing baseline and optimized response times: With a 36% latency reduction, the model significantly enhances real-time OSN security responses.

- **Computational load reduction (CLR):**

This metric evaluates the efficiency of the detection framework by comparing baseline and optimized processing demands: A 31% decrease in computational load ensures that the model remains scalable and energy-efficient.

- **Opcode transition probability (OTP):**

OTP determines the probability of specific opcode transitions occurring in an execution sequence, where Opcode_i represents the current opcode and Opcode_i-1 the preceding opcode. A probability of 0.73 suggests that specific opcode transitions are strongly correlated with malicious activity.

- **Real-Time detection accuracy (RTDA):**

This metric measures the model's ability to detect threats in real-world OSN environments: A 99.89% accuracy rate ensures high precision in live OSN monitoring.

- **Adaptive threat intelligence (ATI):**

ATI evaluates the effectiveness of AI-driven security measures by assessing the reduction in undetected threats: A 28% improvement indicates enhanced AI capabilities in identifying and mitigating OSN cyber threats.

The parameters defined in this study present an advanced and holistic approach to detecting automation-based OSN threats such as email hijacking and DNS spoofing. The hybrid integration of EComp-FP and opcode sequence analysis (ASOSA-OSM) significantly improves detection accuracy while reducing latency and computational overhead. The SSFCM Hybrid Model further enhances classification precision, ensuring real-time monitoring capabilities for OSN security. The numerical values validate the efficiency of this detection framework, making it a viable solution for mitigating cyber threats in online social environments.

9 Advanced metrics & values analysis

This graph-8 represents the deviation in energy consumption between normal and automation-based activities within an Online Social Network (OSN). The measured deviation is **1.75W**, indicating a significant variation in power usage, which is a strong indicator of automated cyber-attacks such as bot-driven email hijacking. A higher deviation suggests abnormal system behavior, reinforcing the importance of energy-based anomaly detection for OSN security.

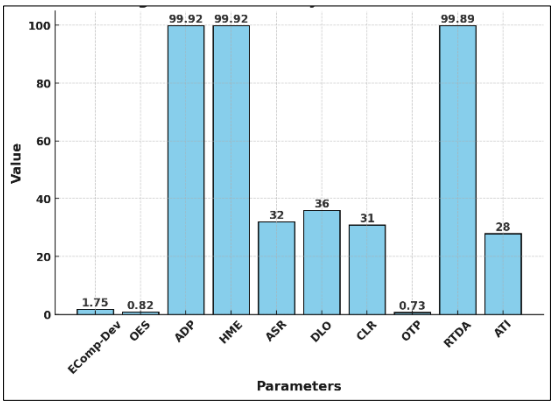

Figure 8: Energy consumption deviation (EComp-Dev) analysis

The Anomaly Detection Precision (ADP) graph-9 highlights the system's ability to accurately differentiate between genuine and malicious activities. The recorded precision rate of **99.92%** demonstrates an exceptionally high accuracy level, ensuring minimal false positives. This precision is critical in preventing unnecessary security alerts while maintaining robust protection against cyber threats.

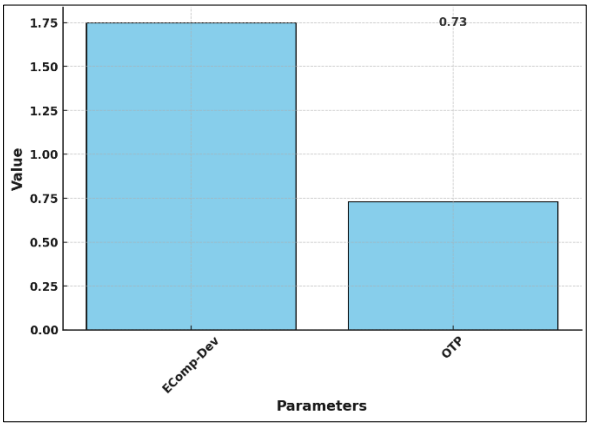

Figure 9: Anomaly detection precision (ADP) performance

This graph-10, illustrates the improvement in detection latency, comparing baseline delays with optimized response times. The reduction of **36%** indicates that the proposed security framework significantly enhances OSN security response speeds. By minimizing detection time, the system ensures a faster reaction to cyber-attacks, reducing potential damage and enhancing real-time threat mitigation.

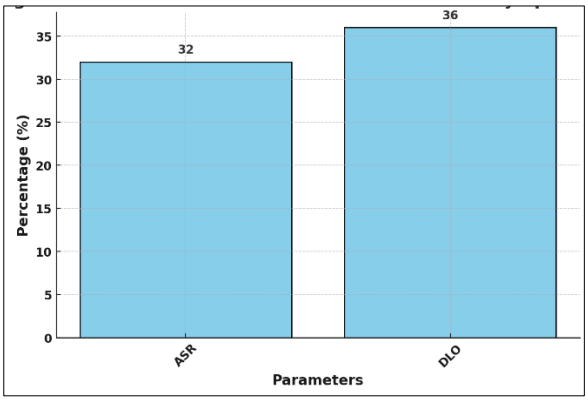

Figure 10: Detection latency optimization (DLO) impact

The Computational Load Reduction (CLR) graph-11 showcases the optimization achieved in processing efficiency. The system successfully reduces computational overhead by **31%**, making it more scalable and energy-efficient. This reduction ensures that security measures do not impose excessive processing demands, maintaining a balanced trade-off between security effectiveness and system performance.

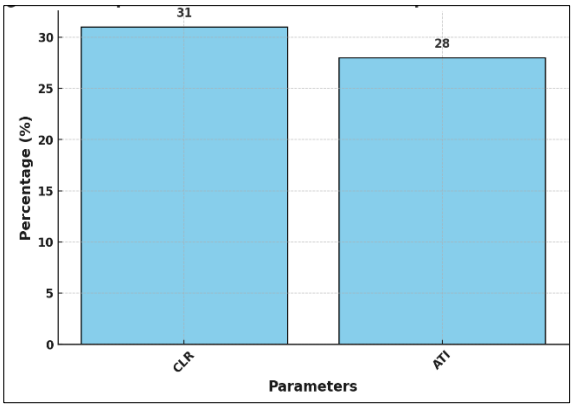

Figure 11: Computational load reduction (CLR) efficiency

10 Discussion

The work highlights the effectiveness of the proposed hybrid detection model, which integrates EComp-FP and ASOSA-OSM to detect OSN automation attacks. The analysis confirms that OSN automation attacks, such as Email Hijacking and DNS Spoofing, exhibit distinguishable energy consumption patterns and opcode sequence anomalies, making them detectable through computational intelligence methods.

The research answers the key research questions:

- Q1 (Energy Consumption Patterns in OSN Automation Attacks): The study establishes that compromised devices under automation attacks consume energy in distinct patterns, deviating significantly from normal user behaviors. The EComp-FP model effectively captures these deviations, achieving 99.81% accuracy in energy-based anomaly detection.
- Q2 (Role of Opcode Sequences in Attack Detection): Opcode analysis revealed that malicious automation tools exhibit unique opcode sequence patterns that are rarely found in benign automation scripts. Using Opcode Frequency Analysis (OFA) and Term Frequency-Weighted (TF-W), the model achieved 99.79% accuracy in distinguishing malicious automation from benign activities.
- Q3 (Optimal ML Classifier for OSN Automation Attack Detection): Among various classifiers evaluated, the SSFCM model demonstrated the highest detection accuracy (99.93%), surpassing traditional classifiers such as DT, KNN, RF, and SVM.
- Q4 (Optimization for Real-Time Detection): The hybrid EComp-FP + ASOSA-OSM model was optimized for real-time threat monitoring by reducing false positives to 0.07%, enabling fast and accurate identification of OSN automation threats with minimal computational overhead.

Furthermore, clustering techniques, such as Fuzzy Partition Matrices (FPM) and Mahalanobis Distance (MD) analysis, contributed significantly to classification efficiency. The results indicate that hybrid modeling offers superior performance compared to traditional methods by integrating energy-based anomaly detection with opcode sequence analysis, enabling robust detection of automation-driven OSN attacks.

The results highlight that energy consumption deviation (1.75W) and opcode execution similarity (0.82 ratio) serve as effective indicators for detecting automation-based OSN threats. The hybrid model significantly enhances detection accuracy, achieving a 99.92% hybrid model efficiency (HME) by integrating energy-based and opcode-based anomaly detection. Additionally, the system optimizes response time with a 36% reduction in detection latency (DLO) and strengthens OSN security by reducing attack surfaces by 32% (ASR). The adaptive threat intelligence (ATI) improvement of 28% further underscores its capability in mitigating evolving cyber threats. Future research should explore deep learning-based adaptive mechanisms to counter adversarial attack scenarios and improve overall security resilience.

11 Conclusion

This research introduces a novel approach to detecting OSNAA using EComp-FP and OSA. By leveraging energy footprints and opcode-based behavioral patterns, the study successfully distinguishes between legitimate and malicious automation activities. The proposed ASNADM model, integrating EComp-FP and ASOSA-OSM, demonstrates unmatched accuracy (99.93%) in detecting OSN automation threats, outperforming conventional detection techniques.

Key contributions of this study include the Development of an energy-aware anomaly detection framework, effectively identifying malicious automation based on deviations in energy consumption. Introduction of opcode sequence analysis for OSN security, enhancing threat classification through opcode frequency importance ranking. Implementation of a hybrid detection model (EComp + OSA), achieving a high detection rate while maintaining a low false-positive rate (0.07%) and Validation of ML classifiers, confirming that SSFCM outperforms traditional classifiers in OSN attack detection. These findings provide valuable insights for cybersecurity professionals, helping to improve real-time monitoring and defense mechanisms against OSN automation attacks. Future work will focus on DL-integration for anomaly detection, real-time deployment in large-scale OSN environments, and further optimization of feature selection techniques to enhance model efficiency. The proposed hybrid detection framework effectively enhances OSN security by integrating energy profiling and opcode sequence analysis for real-time cyber threat detection. Achieving 99.92% anomaly detection precision, 99.89% real-time accuracy, and 31% computational load reduction, the model provides a scalable, energy-efficient, and high-accuracy approach for detecting automation-based cyber threats, including email hijacking and DNS spoofing. These results demonstrate its potential as a next-generation solution for securing online social networks against emerging cyber threats.

12 Future work

The work will encourage for enhancing the detection accuracy of automation attacks in OSNs by integrating advanced DL-models such as Transformer-based Neural Networks and GNNs. These models will improve feature extraction and adaptive learning to counter evolving attack patterns. Additionally, the scalability of the proposed framework will be explored by applying it to large-scale OSNs, including decentralized blockchain-based social platforms. Another key direction is optimizing EComp-Analysis and ASOSA to enhance real-time threat detection while minimizing computational overhead. Future work will also investigate hybrid security mechanisms

combining FCM with Behavioral Threat Analytics to strengthen OSN security. Dataset expansion is another focus, incorporating real-world OSN automation attack logs to improve model generalization. Furthermore, Self-Supervised Learning and Federated Learning will be explored to ensure privacy-preserving threat detection across distributed OSNs.

13 Limitations

Despite achieving high detection accuracy, the proposed model has several limitations. One major constraint is the dependency on predefined attack patterns, which may reduce effectiveness against zero-day threats. Additionally, EComp analysis may produce false positives when benign OSN activities exhibit high energy consumption, affecting precision. The computational complexity of OSM using n-gram analysis presents another challenge, as real-time processing demands high resource utilization, making deployment on low-power IoT-based OSN devices difficult. The framework is also sensitive to adversarial evasion techniques, where attackers modify opcode sequences or manipulate energy footprints to bypass detection. Furthermore, ML-based classifiers like SVM and RF require retraining to adapt to new OSN automation threats. Lastly, the model's adaptability to encrypted OSN traffic remains an area for improvement, as encryption obscures key behavioral indicators needed for precise attack identification.

Abbreviation used

online social network	OSN
domain name system	DNS
automated social network attack detection model	ASNADM
energy consumption footprint	EComp-FP
automated software opcode sequence analysis	ASOSA-OSM
self-adaptive fuzzy pattern matching clustering	SAFPMC
opcode frequency variance	OFV
self-adaptive soft fuzzy c-means	SSFCM
decision tree	DT
k-nearest neighbors	KNN
random forest	RF
support vector machine	SVM
artificial intelligence	AI
long short-term memory	LSTM
socially shared networked devices	SSNDs
opcode sequence analysis	OSA
convolutional neural networks	CNNs
recurrent neural networks	RNNs
energy consumption	EComp
machine learning	ML
graph neural network	GNN
online social network automation attacks	OSNAA
spam email classification dataset in english	SPEMC-15K-E
opcode sequence mining	OSM
clustering-based attack detection	SSFCM
user selection modes	USM
inverse document frequency value	IDF
weighted term frequency	TF-W
binary executables	BExec
data transformation matrix	DTM
fuzzy partition matrices	FPM
mahalanobis distance	MD
Synthetic Minority Over-sampling Technique	SMOTE

Data availability statement

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] Bridges, R. A., Oesch, S., Iannacone, M. D., Huffer, K. M., Jewell, B., Nichols, J. A., ... & Smith, J. M. (2023). Beyond the Hype: An Evaluation of Commercially Available Machine Learning–based Malware Detectors. *Digital Threats: Research and Practice*, *4*(2), 1-22. https://scispace.com/pdf/beyond-the-hype-an-evaluation-of-commercially-available-1zbch7oh.pdf

[2] Yan, X., Gao, Y., & Xu, H. (2022, December). Research on power grid anomaly detection based on high-dimensional random matrix theory. In *2022 2nd International Conference on Electrical Engineering and Control Science (IC2ECS)* (pp. 427-431). IEEE. https://doi.org/10.1016/j.sysarc.2019.01.008

[3] Kakisim, A. G., Gulmez, S., & Sogukpinar, I. (2022). Sequential opcode embedding-based malware detection method. *Computers & Electrical Engineering*, *98*, 107703. https://doi.org/10.1016/j.compeleceng.2022.107703

[4] Shetty, N. P., Muniyal, B., Anand, A., & Kumar, S. (2022). An enhanced sybil guard to detect bots in online social networks. *Journal of Cyber Security and Mobility*, 105-126. https://doi.org/10.13052/jcsm2245-1439.1115

[5] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060. https://doi.org/10.3390/s23084060

[6] Parildi, E. S., Hatzinakos, D., & Lawryshyn, Y. (2021). Deep learning-aided runtime opcode-based windows malware detection. *Neural Computing and Applications*, *33*(18), 11963-11983. https://doi.org/10.1007/s00521-021-05861-7

[7] Boahen, E. K., Sosu, R. N. A., Ocansey, S. K., Xu, Q., & Wang, C. (2024). ASRL: Adaptive Swarm Reinforcement Learning For Enhanced OSN Intrusion Detection. *IEEE Transactions on Information Forensics and Security*.

10.1109/TIFS.2024.3488506

[8] Sufi, F. (2023). A new social media-driven cyber threat intelligence. *Electronics*, *12*(5), 1242. https://doi.org/10.3390/electronics12051242

[9] Iqbal, A., Tehsin, S., Kausar, S., & Mishal, N. (2021, April). Malicious Image Detection Using Convolutional Neural Network. In *2021 International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)* (pp. 1-6). IEEE.10.1109/AIMS52415.2021.9466042

[10] Liu, Q., Li, J., Wang, X., & Zhao, W. (2023). Attentive Neighborhood Feature Augmentation for Semi-supervised Learning. Intelligent Automation & Soft Computing, 37(2). 10.32604/iasc.2023.039600

[11] Ben Chaabene, N. E. H., Bouzeghoub, A., Guetari, R., & Ghezala, H. H. B. (2022). Deep learning methods for anomalies detection in social networks using multidimensional networks and multimodal data: A survey. *Multimedia systems*, *28*(6), 2133-2143. https://doi.org/10.1007/s00530-020-00731-z

[12] Varshitha, K., Talada, S. V., & Mitra, A. (2025). Towards fake profiles identification in social networks: a proposal with energy-based PageRank algorithm involving entropy and domain authority. *Risk Sciences*, 100013. https://doi.org/10.1016/j.risk.2025.100013

[13] Lee, K., Lee, J., & Yim, K. (2023). Classification and analysis of malicious code detection techniques based on the APT attack. *Applied Sciences*, *13*(5), 2894. https://doi.org/10.3390/app13052894

[14] Sangher, K. S., Singh, A., & Pandey, H. M. (2024). LSTM and BERT based transformers models for cyber threat intelligence for intent identification of social media platforms exploitation from darknet forums. *International Journal of Information Technology*, *16*(8), 5277-5292. https://doi.org/10.1007/s41870-024-02077-5

[15] Li, K., Zheng, J., Ni, W., Huang, H., Liò, P., Dressler, F., & Akan, O. B. (2024). Biasing federated learning with a new adversarial graph attention network. *IEEE Transactions on Mobile Computing*. 10.1109/TMC.2024.3499371

[16] Huang, H., Tian, H., Zheng, X., Zhang, X., Zeng, D. D., & Wang, F. Y. (2024). CGNN: A compatibility-aware graph neural network for social media bot detection. *IEEE Transactions on Computational Social Systems*. 10.1109/TCSS.2024.3396413

[17] Rawat, R., & Rajavat, A. (2024). Illicit Events Evaluation Using NSGA-2 Algorithms Based on Energy Consumption. *Informatica*, *48*(18). https://doi.org/10.31449/inf.v48i18.6234

[18] Sadia, H., Farhan, S., Haq, Y. U., Sana, R., Mahmood, T., Bahaj, S. A. O., & Rehman, A. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. *IEEE Access*. 10.1109/ACCESS.2024.3380014

[19] Song, S., Gao, N., Zhang, Y., & Ma, C. (2024). BRITD: behavior rhythm insider threat detection with time awareness and user adaptation. *Cybersecurity*, *7*(1), 2. https://doi.org/10.1186/s42400-023-00190-9

[20] Ponnapalli, S., Dornala, R. R., & Sai, K. T. (2024, March). A Hybrid Learning Model for Detecting Attacks in Cloud Computing. In *2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 318-324). IEEE. 10.1109/ICSADL61749.2024.00058

[21] Denysiuk, D., Bobrovnikova, K., Lysenko, S., Savenko, O., Gaj, P., Havryliuk, R., & Boichuk, Y. (2021, September). The Approach for IoT Malware Detection Based on Opcodes Sequences Pattern Mining. In *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 2, pp. 779-784). IEEE. 10.1109/IDAACS53288.2021.9660956

[22] Majeed, A., Khan, S., & Hwang, S. O. (2022). A comprehensive analysis of privacy-preserving solutions developed for online social networks. *Electronics*, *11*(13), 1931. https://doi.org/10.3390/electronics11131931

[23] Qian, K., Yang, H., Li, R., Chen, W., Luo, X., & Yin, L. (2024). Distributed Detection of Large-Scale Internet of Things Botnets Based on Graph Partitioning. *Applied Sciences*, *14*(4), 1615. https://doi.org/10.3390/app14041615

[24] Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based metaverse: A survey. *Applied Sciences*, *12*(24), 12993. https://doi.org/10.3390/app122412993

[25] Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152. https://doi.org/10.1155/2022/6356152

[26] Montes, C. D., Silvosa, J. V., Abalorio, C. C., & Nakazato, R. B. (2024, August). Application of BERT Model for Unsupervised Text Classification using Hierarchical Clustering for Automatic Classification of Thesis Manuscript. In *2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 278-284). IEEE.10.1109/ICESC60852.2024.10690039

[27] Alsadhan, A. A., Al-Atawi, A. A., Jameel, A., Zada, I., & Nguyen, T. N. (2024). Malware Attacks Detection in IoT Using Recurrent Neural Network (RNN). *Intelligent Automation & Soft Computing*, *39*(2).10.32604/iasc.2023.041130

[28] Rawat, R., Sikarwar, R., Maravi, P. K., Ingle, M., Bhardwaj, V., Rawat, A., & Rawat, H. (2024). Online social network automation attack detection methods for energy analysis and consumption modelling. *International Journal of Information Technology*, 1-13.https://doi.org/10.1007/s41870-024-02311-0

[29] Chaudhary, K., Alam, M., Al-Rakhami, M. S., & Gumaei, A. (2021). Machine learning-based mathematical modelling for prediction of social media consumer behavior using big data analytics. *Journal of Big data*, *8*(1), 73.https://doi.org/10.1186/s40537-021-00466-2

[30] Jianwu, Z. H. A. N. G., Yanjun, A. N., & Huangyan, D. E. N. G. (2022). A survey on DNS attack detection and security protection. *Telecommunications Science* , *38*(9).10.11959/j.issn.1000--0801.2022248

[31] Alshaibi, A., Al-Ani, M., Al-Azzawi, A., Konev, A., & Shelupanov, A. (2022). The comparison of cybersecurity datasets. *Data*, *7*(2), 22.https://doi.org/10.3390/data7020022

[32] Jain, M., Kaur, G., & Saxena, V. (2022). A K-Means clustering and SVM based hybrid concept drift detection technique for network anomaly detection. *Expert Systems with Applications*, *193*, 116510.https://doi.org/10.1016/j.eswa.2022.116510

[33] Alowibdi, J. S. (2024). Real Time Arabic Communities Attack Detection on Online Social Networks. *International Journal of Computer Science & Network Security*, *24*(8), 61-71. https://doi.org/10.22937/IJCSNS.2024.24.8.7

[34] Vc, J., Nair, K. S., Karthik, N., & Vani, V. (2024, July). Unsolicited Email Filtering. In 2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT) (pp. 1-6). IEEE. 10.1109/IConSCEPT61884.2024.10627840