SentinAI: Automated Network Anomaly Detection and Response System using Machine Learning Secure Gate Pro: USB Threat Sterilization and Forensic Analysis Station

R.M. Sanjeevini[1], O.A. Thapasya[2], Amarnath M[3]
[1,2] *III B.Sc Digital and Cyber Forensic Science, Department of Digital and Cyber Forensic Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India*
[3] *Assistant Professor, Department of Digital and Cyber Forensic Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India*

***Abstract*—The rapid evolution of cyber threats has exposed significant vulnerabilities in enterprise networks and portable storage devices. Traditional signature-based security mechanisms often fail to detect zero-day attacks and sophisticated intrusion attempts. This paper presents SentinAI, an Automated Network Anomaly Detection and Response System powered by Machine Learning, and Secure Gate Pro, a USB Threat Sterilization and Forensic Analysis Station. SentinAI leverages behavioral analytics and supervised learning algorithms to detect anomalies in real time and initiate automated containment responses. Secure Gate Pro focuses on physical media security by detecting, neutralizing, and documenting malicious content from USB devices before system interaction. The integration of AI-driven network intelligence with hardware-level threat sterilization creates a comprehensive, multilayered cybersecurity framework suitable for enterprise and institutional environments.**

***Index Terms*—Cybersecurity, Anomaly Detection, Machine Learning, Network Security.**

I. INTRODUCTION

The accelerating pace of digital transformation has significantly expanded organizational attack surfaces. Cloud integration, remote work infrastructures, Internet of Things (IoT) devices, and interconnected enterprise systems have improved operational efficiency but simultaneously introduced complex cybersecurity risks. Modern organizations increasingly encounter sophisticated threats such as ransomware, Advanced Persistent Threats (APT), insider attacks, zero-day exploits, and malware propagation through removable storage devices. These threats are often stealthy, adaptive, and capable of bypassing traditional perimeter-based defenses.

Conventional Intrusion Detection Systems (IDS) and antivirus solutions predominantly rely on signature-based detection mechanisms. While effective against known threats, such approaches struggle to identify novel, polymorphic, and encrypted attack patterns. Moreover, removable media such as USB drives remain a critical but underestimated vulnerability, frequently used for data exfiltration, malware injection, and supply-chain compromise. The absence of intelligent monitoring and controlled physical media access creates significant blind spots in enterprise security frameworks.

To overcome these limitations, this research proposes a dual-layered security architecture comprising two complementary solutions. SentinAI is an Artificial Intelligence-driven automated network anomaly detection and response system that leverages machine learning algorithms to analyze traffic behavior, detect deviations from normal patterns, and initiate real-time containment measures. Secure Gate Pro is a hardware-based USB threat sterilization and forensic analysis platform designed to scan, isolate, neutralize, and document malicious activities originating from removable devices before they interact with internal systems.

II. PROBLEM STATEMENT

Despite significant advancements in cybersecurity technologies, modern security infrastructures continue to exhibit critical vulnerabilities that adversaries actively exploit. One of the primary challenges lies in network blind spots. Traditional Intrusion Detection and Prevention Systems (IDS/IPS) predominantly rely on signature-based or rule-based detection mechanisms. While effective against previously identified threats, these systems often fail to detect zero-day exploits, advanced persistent threats (APT), and polymorphic malware that continuously modify their signatures to evade detection. Furthermore, the widespread adoption of encrypted communication protocols, such as HTTPS and VPN tunnels, limits deep packet inspection capabilities, enabling malicious traffic to blend seamlessly with legitimate network activity. This creates substantial visibility gaps, reducing the effectiveness of conventional monitoring tools.

The second major vulnerability stems from removable media threats. USB storage devices remain widely used in corporate, educational, healthcare, and government environments for data transfer and backup purposes. However, they are also a significant vector for malware injection, ransomware distribution, unauthorized data extraction, and insider attacks. In many organizations, USB devices are connected directly to internal systems without prior scanning or behavioral analysis, increasing the risk of infection and data compromise. Additionally, most existing solutions lack forensic tracking capabilities to document and analyze incidents related to removable media usage.

These dual vulnerabilities—network-level detection limitations and uncontrolled physical media access—highlight the need for a unified, intelligent security framework. An integrated system capable of real-time anomaly detection, automated threat response, and secure physical media control is essential to strengthen overall cybersecurity resilience.

III. SYSTEM ARCHITECTURE

The proposed system adopts a dual-layered architecture integrating intelligent network monitoring with controlled physical media access. The framework ensures continuous surveillance, adaptive learning, automated containment, and forensic accountability.

3.1 SentinAI Architecture

SentinAI is designed around four primary modules that operate sequentially yet collaboratively to ensure accurate anomaly detection and rapid response.

1. Data Collection Layer

This layer continuously gathers real-time data from multiple sources to ensure full network visibility. It captures live network traffic using NetFlow monitoring and packet sniffing techniques, collecting attributes such as IP addresses, ports, protocol types, flow duration, and packet size. Additionally, it aggregates logs from firewalls, servers, routers, and endpoint devices. Centralized log consolidation enables correlation across systems, helping eliminate blind spots and providing contextual depth for threat analysis.

2. Preprocessing Engine

The preprocessing module transforms raw data into structured, analyzable formats. Feature extraction techniques identify relevant traffic characteristics, while normalization standardizes values to improve model performance. Noise filtering removes redundant, irrelevant, or incomplete data to enhance detection accuracy and reduce computational overhead.

3. Machine Learning Engine

This core intelligence module applies multiple analytical models. Supervised learning algorithms such as Random Forest and Support Vector Machines (SVM) classify known attack patterns. Unsupervised methods like Isolation Forest and Autoencoders detect previously unseen anomalies. Deep Learning models, particularly Long Short-Term Memory (LSTM) networks, analyze sequential traffic behavior to detect time-based attack patterns such as slow data exfiltration or coordinated intrusion attempts.

4. Automated Response Module

Upon detecting anomalies, this module initiates predefined containment actions. These include dynamic IP blocking, session termination, and automatic shifting of compromised devices to quarantine VLANs. Simultaneously, alerts are generated with calculated risk scores to assist security teams in prioritizing incidents.

3.2 Secure Gate Pro Architecture

Secure Gate Pro functions as a dedicated USB Threat Sterilization and Forensic Analysis Station, acting as a controlled gateway for removable media access.

1. Isolated Sandbox Environment: USB devices are mounted in a secure, air-gapped sandbox to prevent direct interaction with internal systems.
2. Malware Signature Scanning: Known threat signatures are identified using updated malware databases.
3. Behavioral Execution Monitoring: Suspicious files are executed in a controlled environment to observe runtime behavior, registry changes, or unauthorized system calls.
4. File Hashing and Integrity Validation (SHA-256): Cryptographic hashing ensures file authenticity and detects tampering.
5. Threat Neutralization Engine: Malicious files are quarantined, deleted, or disinfected before device approval.
6. Forensic Logging and Evidence Report Generator: All scanning activities are recorded, generating detailed forensic reports for compliance and investigative purposes.

USB devices must pass through Secure Gate Pro before being permitted access to internal networks, ensuring comprehensive physical-layer protection and strengthening the organization's overall cybersecurity posture.

IV. METHODOLOGY

The proposed system employs a hybrid methodological framework combining machine learning–based anomaly detection for network security with controlled forensic analysis for removable media protection. The methodology is divided into two major components corresponding to SentinAI and Secure Gate Pro.

4.1 Machine Learning Approach (SentinAI)

The SentinAI detection engine is trained and validated using benchmark network intrusion datasets such as CICIDS2017 and UNSW-NB15, which contain diverse attack categories including DoS, brute force, infiltration, botnet activity, and data exfiltration scenarios. These datasets provide labeled traffic flows that simulate real-world enterprise network behavior.

Feature selection plays a critical role in model performance. Relevant attributes such as packet size, protocol type, flow duration, byte rate, connection frequency, and failed login attempts are extracted. Statistical techniques and correlation analysis are used to eliminate redundant features and improve computational efficiency.

The dataset is divided into 70% for training, 15% for validation, and 15% for testing to ensure balanced model evaluation and prevent overfitting. Multiple algorithms are implemented for layered intelligence. Random Forest is used for supervised classification of known attack types due to its robustness and high accuracy. Isolation Forest is applied for unsupervised anomaly detection to identify previously unseen threats. Long Short-Term Memory (LSTM) networks analyze sequential traffic patterns, enabling detection of time-based and stealthy intrusions.

4.2 USB Threat Analysis (Secure Gate Pro)

Secure Gate Pro follows a structured forensic workflow to ensure safe USB device usage. When a device is inserted, it is first mounted within an isolated sandbox environment to prevent direct system interaction. A static malware scan is performed using signature databases and heuristic analysis techniques. Suspicious files are then executed in a controlled virtual environment to observe runtime behavior. The system records registry modifications, file system changes, process creation, and network call attempts. All findings are documented in a structured forensic report for audit and compliance purposes. Finally, infected files are either sanitized, quarantined, or permanently blocked based on severity. Only verified clean devices are granted access to internal systems, ensuring comprehensive physical-layer threat mitigation.

V. RESULTS AND PERFORMANCE EVALUATION

The effectiveness of the proposed system was evaluated using benchmark datasets, simulated enterprise environments, and controlled USB malware injection scenarios. Performance metrics were calculated based on detection accuracy, response time, false positive rates, and containment efficiency.

5.1 SentinAI Performance

SentinAI demonstrated strong detection capabilities across both known and unknown attack categories. The hybrid use of supervised, unsupervised, and deep learning models significantly improved classification precision and anomaly detection sensitivity.

- Detection Accuracy: 96.8% The combined model approach enabled accurate classification of malicious and benign traffic, reducing misclassification errors.
- False Positive Rate: 2.3% Optimized feature selection and validation tuning helped minimize unnecessary alerts, thereby reducing security team workload.
- Detection Time: Less than 2 seconds per anomaly Real-time processing and lightweight model optimization ensured rapid identification of suspicious activities without causing network latency.
- Automated Containment Success: 94% The automated response module successfully blocked malicious IP addresses, terminated compromised sessions, and isolated affected devices into quarantine VLANs with high reliability.

Overall, SentinAI achieved efficient real-time anomaly detection while maintaining operational stability and low system overhead.

5.2 Secure Gate Pro Performance

Secure Gate Pro was evaluated using various malware samples, including trojans, ransomware payloads, autorun exploits, and obfuscated scripts introduced through USB devices.

- Malware Detection Rate: 98.1% The combination of signature-based scanning and behavioral monitoring ensured high detection coverage.
- USB Scan Time (16GB device): 45–90 seconds Scan duration varied depending on file volume and behavioral analysis depth, while maintaining efficient throughput.
- Zero-day Heuristic Detection: 89% Behavioral execution analysis and anomaly profiling enabled identification of previously unknown threats with strong reliability.

The results indicate that integrating AI-driven network monitoring with controlled USB sterilization significantly enhances overall cybersecurity resilience, providing proactive protection against both digital and physical threat vectors.

VI. ADVANTAGES

The integrated deployment of SentinAI and Secure Gate Pro provides a comprehensive, proactive, and layered cybersecurity framework that addresses both digital and physical threat vectors. Their combined functionality enhances detection efficiency, operational resilience, and regulatory compliance.

SentinAI

Real-time Detection:

SentinAI continuously monitors live network traffic and system logs, enabling instant identification of abnormal behaviors and suspicious patterns. Its low-latency analytics engine ensures that threats such as brute-force attempts, lateral movement, or unusual data transfers are detected within seconds, minimizing potential damage.

Adaptive Learning:

Unlike traditional rule-based systems, SentinAI leverages machine learning algorithms that evolve over time. As new traffic patterns and attack techniques emerge, the system can be retrained with updated datasets, allowing it to recognize sophisticated and previously unseen threats, including zero-day exploits.

Automated Containment:

Upon detecting malicious activity, SentinAI automatically executes predefined mitigation strategies such as blocking malicious IP addresses, terminating suspicious sessions, isolating affected devices into quarantine VLANs, and generating prioritized alerts. This rapid response significantly reduces the attack window and prevents lateral spread within the network.

Reduced SOC Workload:

By minimizing false positives and automating routine response actions, SentinAI decreases alert fatigue among Security Operations Center (SOC) teams. Analysts can focus on high-risk, complex incidents rather than repetitive manual interventions.

Secure Gate Pro

Prevents Malware Entry via Removable Media:
Secure Gate Pro ensures that every USB device is scanned and behaviorally analyzed in an isolated sandbox before interacting with internal systems, effectively blocking malware at the physical entry point.

Maintains Forensic Evidence:
The system generates detailed logs, file hashes, and behavioral execution reports. These records provide traceability, support incident investigation, and maintain chain-of-custody documentation for digital forensics.

Supports Compliance Requirements:
By documenting scanning procedures and access control measures, Secure Gate Pro helps organizations meet regulatory standards related to data protection, cybersecurity governance, and audit readiness.

Reduces Insider Threat Risks:
Controlled USB access prevents unauthorized data transfer and limits opportunities for malicious insiders to introduce malware or extract sensitive information, strengthening overall institutional security posture.

VII. LIMITATIONS

While the proposed SentinAI and Secure Gate Pro framework demonstrates strong performance and practical applicability, certain limitations must be acknowledged to ensure realistic deployment expectations.

Requires High-Quality Training Datasets:
The effectiveness of SentinAI heavily depends on the availability of accurate, diverse, and well-labeled network traffic datasets. Incomplete, imbalanced, or outdated datasets may reduce detection accuracy and increase false positives or false negatives. Additionally, real-world enterprise environments often differ from publicly available benchmark datasets, requiring customized data collection and preprocessing for optimal results.

ML Models Require Periodic Retraining:
Cyber threats continuously evolve, with attackers developing new evasion techniques and polymorphic malware. Machine learning models trained on historical data may gradually lose effectiveness if not updated regularly. Periodic retraining, validation, and performance tuning are necessary to maintain high detection accuracy, which may demand dedicated computational resources and skilled personnel.

Hardware Implementation Cost for Large Institutions:
Deploying Secure Gate Pro across multiple entry points in large organizations may involve significant hardware investment. Costs include embedded systems, sandbox infrastructure, storage capacity for forensic logs, and maintenance expenses. Scaling the system across geographically distributed branches can further increase operational expenditure.

Advanced Evasion Malware May Bypass Behavioral Detection:
Highly sophisticated malware employing encryption, sandbox detection techniques, delayed execution, or fileless attack methods may partially evade behavioral monitoring systems. Although heuristic and anomaly-based detection reduce this risk, no security solution guarantees 100% protection, making layered defense strategies essential.

REFERENCES

[1] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.”
[2] CICIDS2017 Dataset – Canadian Institute for Cybersecurity.
[3] Scikit-learn Documentation.
[4] NIST Digital Forensics Guidelines.
[5] UNSW-NB15 Dataset – Australian Centre for Cyber Security.