AI Powered Intelligent Framework For Detection And Prevention Of Cybersecurity Attacks Using Machine Learning Algorithms

G Gokul[1], Ms. Mahalakshimi[2]
[1]Dept of Computer Application
[2]Assistant professor
[1, 2] Dr. M.G.R Educational and Research Institute (Demmed to be University)
Chennai Tamil Nadu India

Abstract- *This paper proposes an AI-powered cybersecurity framework integrating machine learning, deep neural networks, real-time network monitoring, automated alerting, and dashboard-driven response for enterprise threat detection and prevention. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.*

Keywords: Intrusion Detection, Anomaly Detection, SOC, Threat Intelligence. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.classification, and response orchestration in operational environments.

I. INTRODUCTION

Modern organizations face ransomware, phishing, insider threats, zero-day attacks, and advanced persistent threats. Traditional signature systems struggle with evolving attacks. This work proposes an intelligent framework with real-time analytics and automated mitigation. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

2. Problem Definition

Manual monitoring, static firewall rules, and threshold alerts create delayed responses and limited visibility into sophisticated cyberattacks. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

3. Literature Survey

Review of IDS, anomaly detection, ML-based IDS, DNN methods, and automated SOC response systems. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

4. Existing System

Conventional systems rely on signatures and reactive investigation after compromise. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments..

5. Proposed System

The proposed architecture combines packet capture, telemetry ingestion, feature extraction, DNN classification, alert orchestration, dashboard monitoring, and containment automation. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and

practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

6. System Architecture

Modules: Data Collection, Preprocessing, Feature Engineering, ML Engine, Threat Scoring, Notification Engine, Dashboard, Response Controller. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

7. Methodology

Traffic logs are preprocessed, features normalized, models trained, anomalies classified, and alerts dispatched via dashboards/email/SMS. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

8. Dataset

NSL-KDD, CICIDS2017, and UNSW-NB15 datasets can be used for training and benchmarking. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

9. Algorithms

DNN, Random Forest, SVM, and anomaly detection methods support multi-class attack recognition. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

10. Implementation

Python, TensorFlow, Scikit-learn, Flask/Streamlit dashboard, alert APIs, and logging infrastructure. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

11. Results and Analysis

The framework improves detection accuracy, lowers false positives, and reduces Mean Time To Detect (MTTD). This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

12. Advantages

Automation, scalability, real-time analytics, proactive defense, reduced administrative workload. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

13. Future Work

Federated learning, explainable AI, cloud-native deployment, and adaptive self-healing networks. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

14. Conclusion

AI-driven cybersecurity frameworks provide resilient, adaptive, and scalable defense mechanisms for modern infrastructures. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports

dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.

REFERENCES

[1] IEEE IDS papers.
[2] ML for cybersecurity surveys.
[3] Deep learning intrusion detection studies. This implementation-oriented paper discusses architecture design, module interactions, workflow, deployment considerations, performance evaluation, and practical enterprise applicability. The framework supports dashboard visualization, automated SOC notification, anomaly classification, and response orchestration in operational environments.