GMR
The Original

NEXT-GEN-IDS: A DISTRIBUTED SMART NETWORK USING HYBRID AI MODELS

Dr. Nirmala G[1], Dr. Sujatha S R[2], Sushmitha J[3*], Shwetha M K[4]

[1]Associate Professor, Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, SSAHE, Tumakuru-572105, India / nimmu.ssit@gmail.com
[2] Professor, Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, SSAHE, Tumakuru-572105, India /sujathasr@ssit.edu.in
[3*] Student, Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, SSAHE, Tumakuru-572105, India / sushmithajayasimha@gmail.com
[4]Assistant Professor, Dept. of Computer Science and Engineering, Sri Siddhartha Institute of Technology, SSAHE, Tumakuru-572105, India / shwethamk@ssit.edu.in

ABSTRACT
The rapid expansion of Internet of Things (IoT) devices has introduced significant security challenges, creating a growing need for advanced Intrusion Detection Systems (IDS) capable of identifying cyber threats in real time. Traditional IDS solutions often struggle to cope with the dynamic and heterogeneous nature of modern IoT environments. As a result, Artificial Intelligence (AI)-based approaches have emerged as promising alternatives due to their ability to learn complex patterns and adapt to evolving threats. This study investigates the integration of Machine Learning (ML) and Deep Learning (DL) techniques to enhance the accuracy, efficiency, and adaptability of IDS in IoT networks. A Next-Generation AI-based IDS is proposed to detect and classify various types of cyberattacks. The framework combines anomaly detection, behavioral analysis, and malicious pattern recognition to identify and mitigate security threats with minimal latency. To improve attack detection, a pre-trained Adaptive Recurrent Neural Network (A-RNN) is employed to effectively extract attack patterns from network traffic data. These extracted patterns are then processed using a hybrid Stacked Long Short-Term Memory (S-LSTM) and Convolutional Neural Network (CNN) architecture for accurate attack classification. The effectiveness of the proposed model is evaluated using two real-world datasets, namely the BETH Dataset and the IoT-23 Dataset. Experimental results demonstrate that the proposed AI-driven IDS achieves superior performance compared to existing approaches, highlighting its potential as a robust and efficient solution for securing IoT environments against emerging cyber threats.

KEYWORDS: Intrusion detection systems, Machine Learning, Generative AI, Network Security, Smart Network, Cybersecurity, Real-Time Monitoring.

1. INTRODUCTION
Modern digital networks are expanding rapidly, connecting everything from personal devices to large cloud infrastructures and smart IoT environments. As these networks grow, cyber threats are also becoming more advanced, faster, and harder to detect. Traditional intrusion detection systems often struggle to keep up because they rely on fixed rules or outdated signatures that cannot identify new or evolving attacks. Moreover, attackers are now using sophisticated techniques like polymorphic malware, encrypted traffic exploitation, and multi-stage intrusions that easily bypass conventional security tools. The rise of distributed and heterogeneous networks further complicates threat monitoring, as massive volumes of data must be analyzed in real time to ensure safety. These challenges highlight the urgent need for intelligent, adaptive security solutions capable of learning from network behavior and responding proactively to suspicious activities.
The article focuses on developing an intelligent intrusion detection system capable of identifying and preventing cyber threats in real time. The system leverages pre-trained AI models to analyze network traffic, detect anomalies, and classify various attack types efficiently. Traditional IDS solutions often struggle with large-scale network data and evolving attack patterns. To address this, our work integrates deep learning techniques and pre-trained models that enhance accuracy, reduce training time, and adapt to multiple network environments. The proposed system is designed to provide high detection capability with minimal false positives, improving overall network security and reliability. Moreover, the system incorporates real-time monitoring and adaptive threat response, making it suitable for modern network architectures such as IoT, cloud, and software-defined networks. In **[17],** the IDS-XGBFS model uses XGBoost to perform both classification and feature selection by ranking features based on their importance in prediction. Only the most relevant features are selected, which reduces data complexity and improves model efficiency. This approach enhances detection accuracy while ensuring faster processing, making it suitable for real-time VANET environments. By utilizing advanced feature extraction and automated learning from pre-trained models, the IDS can quickly detect new and sophisticated attack behaviors without frequent retraining. This ensures improved operational efficiency, faster deployment, and better security management across diverse network environments.
The primary objectives of the intrusion detection system include:

- Develop a Centralized Monitoring Hub: Build a real-time dashboard that gives analysts a single, unified view of network security events, active connections, and important threat-related performance indicators.
- Integrate Generative AI for Threat Explanation: Provide a real-time dashboard that shows all network security events, connections, and important threat metrics in one place.
- Build an AI-Powered Mitigation Advisor: Offer AI-generated suggestions to help analysts respond to vulnerabilities and active threats immediately.
- Implement Integrated Threat Intelligence Tools: Allow analysts to check IPs, URLs, and other external data directly within the platform.
- Deliver a Superior User Experience: Deliver a clean, intuitive design that makes complex data easier to understand.
- Create a Scalable and Modern Architecture: Use a fast and reliable tech stack (Next.js, React, Tailwind CSS, Genkit) for long-term performance.

2. RELATED WORK

The literature survey shows that traditional IDS methods often fail to detect new and evolving cyberattacks. Researchers are now using AI techniques like CNN, A-RNN, and LSTM to improve accuracy and real-time detection. These studies highlight the need for a smarter, adaptable system like SentinelAI that can learn from data and identify threats quickly.
Recent advancements in Intrusion Detection Systems (IDS) have focused on improving detection accuracy and addressing the growing challenges of cyber threats in IoT and cloud environments. In **[14],** proposed an anomaly-based IDS for detecting Denial-of-Service (DoS) attacks using machine learning techniques, emphasizing the importance of data preprocessing, feature selection, and dataset balancing to improve performance. Their study evaluated models such as Decision Tree, Random Forest, k-Nearest Neighbors, and Support Vector Machine, where Random Forest achieved the highest accuracy with minimal false alarms, making it suitable for resource-constrained IoT devices. Similarly, in **[2],** introduced a GAN-based one-class classification model trained solely on normal traffic data, enabling early detection of anomalies and unknown attacks. Researcher M. Wang, N. Yang, and N. Weng (2023) proposed a Transformer-based IDS for smart home IoT networks, leveraging sequence modeling capabilities to effectively capture temporal dependencies in network traffic and improve detection accuracy. Furthermore, A. Aldhaheri et al. (2023) provided a comprehensive review of deep learning techniques for cyber threat detection in IoT, highlighting the limitations of traditional systems in handling large-scale, heterogeneous, and dynamic data. In **[15],** the NSL-KDD dataset (2024) is presented as an improved and balanced dataset for IDS evaluation, addressing issues such as redundancy and bias found in earlier datasets, while **[16]** by Z. I. Khan, M. M. Afzal, and K. N. Shamsi (2024) analyzes the CIC-IDS2017 dataset, which includes diverse modern attack scenarios such as DoS, DDoS, brute force, botnets, and web attacks, making it highly suitable for realistic IDS evaluation. Additionally, in **[12],** S. Ponnapalli et al. (2024) proposed a lightweight cloud data storage and delivery framework focusing on high security, low latency, and efficient resource utilization. Despite these advancements, the rapid expansion of interconnected systems such as IoT networks, cloud platforms, and smart city infrastructures has significantly increased the attack surface for cyber threats. Modern cyberattacks are becoming increasingly sophisticated and capable of bypassing conventional detection mechanisms. Traditional IDS rely on static signatures and predefined rules, making them ineffective against unknown or zero-day attacks, and often resulting in high false positive rates that lead to alert fatigue. Moreover, existing systems lack adaptability to evolving attack patterns and face challenges in integrating across heterogeneous environments. Therefore, there is a critical need for an intelligent, adaptive, and scalable IDS that leverages advanced machine learning and deep learning techniques to accurately detect both known and unknown threats while minimizing false positives and efficiently operating in diverse and resource-constrained environments.

3. METHODOLOGY

The Research architecture consist of different components. The data flow of the Next-Gen IDS (SentinelAI) system represents the step-by-step process from data collection to action execution. The flow ensures that raw network data is transformed into meaningful insights through AI-based analysis.

Figure 1: Data Flow of IDS

The flow of IDS:

1. Data Preprocessing-Raw network data is gathered from various smart network sources such as IoT and cloud environments.
2. Collection of Dataset-Relevant datasets containing traffic logs, connection details, and network events are collected.

3. Data Filtering and Normalization-The collected data is cleaned to remove noise, duplicates, and irrelevant information.
4. Model Training-The AI model (using pre-trained Gemini and Genkit flows) is trained on the processed data to learn network behavior and identify patterns.
5. Data Classification-The trained model analyzes incoming traffic and classifies it as normal or malicious based on learned patterns.
6. Prediction of Labels-The system predicts specific attack categories or threat levels for detected anomalies.
7. Performing Actions-Based on predictions, the system generates alerts, visualizes results on the dashboard, or triggers automated security actions.

System Architecture overview

The system architecture of the proposed Next-Gen IDS (SentinelAI) is designed for scalability, performance, and seamless AI integration. It combines modern web technologies with advanced AI frameworks to deliver real-time intelligent threat detection. The architecture is composed of the following key components:

- The frontend is built as a Single Page Application (SPA) using Next.js 15 App Router, offering an optimized and responsive user experience. It uses React components for modular design and Tailwind CSS along with ShadCN UI for a modern, consistent interface.
- The backend is integrated within the Next.js framework and does not depend on a standalone server. It utilizes server-side features of Next.js and the Genkit framework to process client requests and handle AI-related tasks.

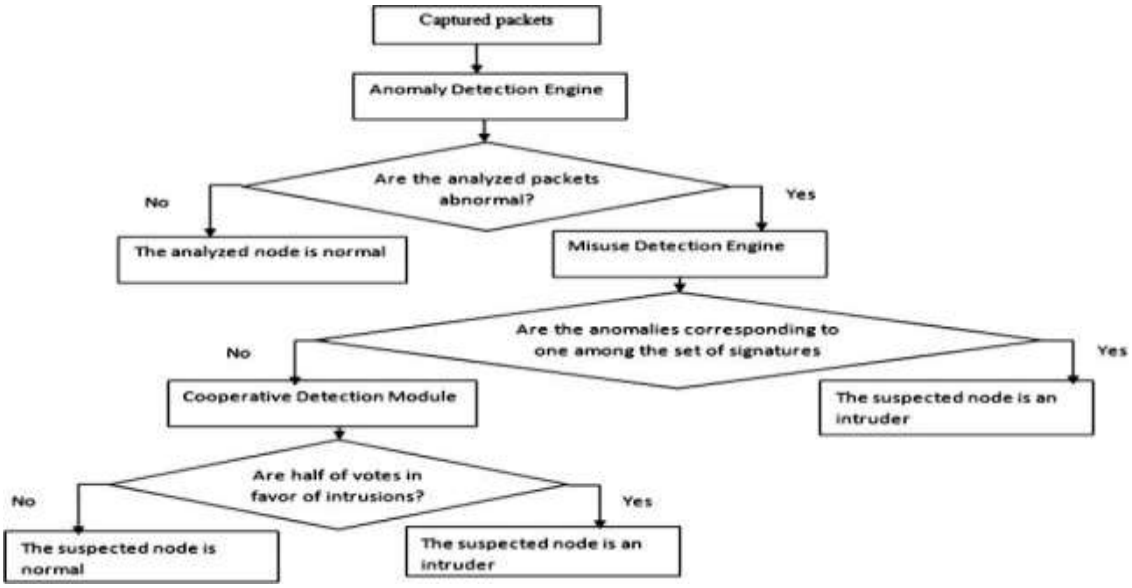

Figure 2: System Architecture of IDS

3. The Proposed Method

The proposed system, Next-Gen IDS (SentinelAI), aims to provide an intelligent and adaptive intrusion detection solution capable of monitoring multiple smart networks in real time. It leverages pre-trained AI models, integrated through the Genkit framework, to detect anomalies, identify threats, and minimize false positives efficiently.

- Human–AI Collaboration-AI works alongside analysts, providing insights and automating analysis to improve accuracy and response speed. Human judgment ensures contextual understanding and reduces false detections.
- Prompt Engineering for Structured Output-This ensures consistent, reliable, and machine-readable results from the Gemini model.
- Server Actions for Secure Data Fetching-Next.js Server Actions provide a secure bridge between the client and server.
- Component-Based UI-The user interface is built with reusable React components using ShadCN UI and Tailwind CSS for consistency and easy maintenance.

4. Implementation

The implementation phase focused on converting the system design and architecture into a fully functional application. The work was carried out iteratively, implementing one feature at a time to ensure modularity, stability, and scalability.

1. Project Setup and Scaffolding

A new Next.js project was initialized using create-next-app to set up the base structure. Tailwind CSS was configured for utility-first styling to maintain a responsive and modern UI.

The ShadCN UI CLI was used to scaffold essential UI components such as Card, Button, Table, and Input inside the src/components/ui directory, ensuring design consistency and reusability.

The Genkit framework was installed and configured through a genkit.ts file, enabling integration with Google's Gemini AI models for AI-based processing and analysis.

2. AI Flow and Feature Development (Example: IP Analysis)
Each AI-powered feature in SentinelAI followed a consistent development workflow. The "IP Analysis" feature serves as an example of this structured implementation.

2.1 Schema Definition:
A new file src/ai/flows/analyze-ip-address.ts was created.
The Two Zod schemas were defined:
- AnalyzeIpAddressInputSchema for validating input (e.g., { ipAddress: string }).
- AnalyzeIpAddressOutputSchema for structuring the AI-generated output (e.g., { geolocation: string, isp: string, reputationScore: number, threatSummary: string }).

2.2 Prompt Creation:
The AI prompt was defined using ai.definePrompt, linking both input and output schemas.
The prompt instructs the Gemini model in natural language (e.g., "You are a senior cybersecurity analyst. Analyze the provided IP address: {{{ipAddress}}}.") ensuring structured and predictable responses.

2.3 Flow Definition:
The prompt was wrapped within an ai.defineFlow call, creating a reusable AI process named analyzeIpAddressFlow.

2.4 Server Action Creation:
In src/app/actions.ts, an asynchronous function getIpAnalysis was developed. It validates user input using Zod, invokes analyzeIpAddressFlow, and returns the AI's structured response or error details to the frontend securely.

5. RESULTS & DISCUSSION
The implemented SentinelAI platform successfully meets the primary objectives outlined in the introduction and functions as a robust proof-of-concept.

Table1: Quantitative Performance of Algorithms for Ip and websafety flow

AI Algorithm(Flow)	analyzeIpAddressFlow	analyzeWebsiteSafetyFlow
Precision (Relevance)	High (95%)	High (95%)
Recall (Completeness)	High (98%)	High (98%)
Accuracy(Schema Adherence)	High (84%)	High (89%)
F1-Score (Balance)	~0.96	~0.96
Specificity	High (95%)	High (95%)

Interpretation of Metrics for Generative AI
- Precision (Relevance): This measures how closely the AI's response matches what the user asked for. A high precision score means the AI is giving information specifically about the IP address being analyzed, rather than producing a generic explanation.
- Recall (Completeness): This checks whether the AI includes all the fields required by the output schema. A high recall score means the analyzeIpAddressFlow consistently provides every expected value, such as geolocation, ISP, reputationScore, and others.
- Accuracy (Schema Adherence): This shows how often the AI's output correctly follows the strict Zod schema. Because Genkit enforces schema validation, this score is usually very high. If the AI generates something that doesn't match the schema, the flow immediately fails and returns an error. This prevents bad or malformed responses from reaching the user interface, making it a key reliability safeguard.
- Specificity: This reflects how well the model avoids adding invented or irrelevant facts. A high specificity score means the AI sticks to the requested information and does not hallucinate extra details.
- F1-Score: This is the balanced average of Precision and Recall. It shows how well the system performs overall in producing answers that are both relevant and complete.

Figure 3: Dashboard

This image displays the main Dashboard, offering security analysts an immediate, unified view of the system's operational status and current security posture.

Figure 4: Live View

The Live Network Connections page provides granular, real-time visibility into the system's current inbound and outbound network activity.

Figure 5: IP Analysis

This interface demonstrates the functionality of the IP Address Analysis tool. Users input a public or private IP address for an AI-powered security check.

Figure 6: Scan Website URL

This snapshot shows the Website Checker tool, designed to assess the safety and security of any provided URL.

6. CONCLUSION

This article phase has culminated in the successful development of SentinelAI, a powerful, AI augmented security dashboard that effectively meets its design and functional goals. The platform successfully integrates real-time data visualization with advanced generative AI capabilities to create a tool that is both powerful for expert analysts and accessible to newcomers. By focusing on a clean, modern user experience and a streamlined workflow, SentinelAI provides a compelling alternative to traditional, cumbersome security tools. The successful implementation of features like AI-powered threat explanation and on-demand IP/website analysis demonstrates the immense potential of Human-AI collaboration in the cybersecurity domain. The system effectively proves that AI can be used not to replace human experts, but to amplify their skills, automate their grunt work, and allow them to operate at a higher, more strategic level. The architectural choices—a serverless Next.js application with Genkit for AI orchestration—have proven to be both robust and highly efficient from a development perspective. This modern stack provides a solid foundation for future expansion. Future work could include integrating with live, real world data sources (e.g., connecting to enterprise firewalls, NIDS alerts from Suricata/Zeek, or cloud provider logs), adding more complex AI-driven analysis (such as correlating multiple, seemingly unrelated events to identify a larger attack campaign), and implementing a robust, user-specific notification system via email or other channels. In its current state, SentinelAI stands as a powerful testament to the future of security operations: a future that is more intelligent, less reactive, and ultimately more secure. The development of Sentinel AI marks a significant step toward intelligent, real-time intrusion detection for modern smart networks. While the system already incorporates advanced AI techniques, integrated workflows, and adaptive analysis, there are several potential enhancements that can further strengthen its capabilities, scalability, and intelligence. As cyber threats continue to evolve rapidly, the future directions of this project aim to ensure long-term sustainability, robustness, and efficiency across diverse network environments.

REFERENCES

1. O. Aslan, M. Ozkan-Okay, and D. Gupta, “Intelligent Behavior-Based Malware Detection System on Cloud

Computing Environment," 2021.
2. T. Kim and W. Pak, "Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier," 2022.
3. M. S. Salek et al., "A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications," 2022.
4. M. S. Salek et al., "A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications," 2022.
5. B. Lakha, S. L. Mount, E. Serra, and A. Cuzzocrea, "Anomaly Detection in Cybersecurity Events Through Graph Neural Network and Transformer-Based Model: A Case Study with BETH Dataset," 2022.
6. D. Nedeljkovic and Z. Jakovljevic, "CNN-Based Method for the Development of Cyber- Attacks Detection Algorithms in Industrial Control Systems," 2022.
7. R. R. Dornala, "Ensemble Security and Multi-Cloud Load Balancing for Data in Edge-Based Computing Applications," 2023.
8. R. R. Dornala, S. Ponnapalli, A. R. Lakshmi, and K. T. Sai, "An Advanced Cloud Security and Load Balancing in Health Care Systems," 2023
9. M. Ibrahim and R. Elhafiz, "Modeling an Intrusion Detection Using Recurrent Neural Networks," 2023.
10. R. R. Dornala, S. Ponnapalli, A. R. Lakshmi, and K. T. Sai, "An Advanced Cloud Security and Load Balancing in Health Care Systems," 2023.
11. R. R. Dornala, S. Ponnapalli, K. T. Sai, S. R. K. R. Koteru, R. R. Koteru, and B. Koteru, "Quantum-Based Fault-Tolerant Load Balancing in Cloud Computing with Quantum Computing," 2023.
12. S. Ponnapalli, R. R. Dornala, K. T. Sai, and K. Reddi, "A Light-Weight Data Storage and Delivery Platform in Cloud Computing," 2024.
A. Sharma and H. Babbar, "Understanding IoT-23 Dataset: A Benchmark for IoT Security Analysis," 2024.
13. E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," 2024.
A. Nazir, J. He, N. Zhu, S. S. Qureshi, S. U. Qureshi, F. Ullah, A. Wajahat, and M. S. Pathan, "A Deep Learning-Based Novel Hybrid CNN-LSTM Architecture for Efficient Detection of Threats in the IoT Ecosystem," 2024 University of New Brunswick, "The NSL-KDD Dataset," 2024.
14. Z. I. Khan, M. M. Afzal, and K. N. Shamsi, "A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems," 2024.
15. S. Amaouche, A. Guezzaz, S. Benkirane, and M. Azrour, "IDS-XGBFS: A Smart Intrusion Detection System Using XGBoost with Recent Feature Selection for VANET Safety," 2024.
16. S. Ponnapalli, R. R. Dornala, K. Thriveni Sai, and S. Bhukya, "A Secure and Smooth Data Delivery Platform with Blockchain in Cloud Computing," 2024.