CHAPTER: 1

INTRODUCTION

1.1 Basic Overview

With cyber threats evolving at an unprecedented pace—ransomware, zero-day exploits, social engineering attacks—traditional cybersecurity systems are failing to keep up. Most existing tools are reactive, siloed, and require manual intervention. CyberSentinel AI aims to change that by building a self-healing, AI-driven cybersecurity framework that continuously learns, adapts, and defends in real time. This system will detect anomalies, analyze threat patterns, and automatically initiate mitigation protocols using reinforcement learning and anomaly detection. The architecture integrates user profiling, real-time log monitoring, and threat intelligence feeds to create a unified, autonomous defense mechanism.

Key pillars:

- AI-powered Threat Detection
- Reinforcement Learning-based Auto-Mitigation
- Real-time Log & Behavior Analysis
- Cross-platform Dashboard & Reporting System

1.2 Objectives of the Project

- Build an intelligent, autonomous cybersecurity framework.
- Detect anomalies in system/network/application behavior.
- Apply reinforcement learning for self-mitigation.
- Integrate with SIEM tools, firewall logs, and system-level data.
- Provide a real-time, centralized dashboard for monitoring & control.

1.3 Scope of the Project

CyberSentinel AI is a next-gen cybersecurity solution engineered to **autonomously detect, analyze, and respond to threats** across modern IT infrastructures—cloud, on-prem, and hybrid. The project focuses on creating a **self-healing, AI-powered cybersecurity system** that evolves with threat patterns and adapts in real-time using reinforcement learning and anomaly detection. This project encompasses the **development of an end-to-end intelligent threat defense platform** with the following capabilities:

- **Anomaly Detection:** Real-time identification of abnormal system and network behaviors using unsupervised and supervised ML models (Isolation Forest, LSTM-AE, Random Forests).
- **Reinforcement Learning Engine:** A self-optimizing module that learns the best mitigation actions (block IP, isolate endpoint, revoke privileges) based on feedback loops.
- **Natural Language Log Interpretation:** Convert unstructured syslogs, firewall logs, and alerts into actionable insights using NLP.
- **Threat Classification & Clustering:** Detect and group similar cyberattack patterns to streamline mitigation and avoid false positives.
- **Cross-Platform Threat Monitoring Dashboard:** A responsive frontend (Streamlit or React) that visualizes alerts, responses, system health, and feedback analytics.

The system is designed with modularity and future expansion in mind. The long-term scope includes:

- **Deception Techniques:** Integration with honeypots to actively bait and study intruders.
- **Threat Intelligence Feeds:** Ingesting third-party intel (MISP, OpenCTI, AbuseIPDB) to proactively defend against known vulnerabilities and IPs.
- **Compliance Auditing:** Extend functionality to auto-verify conformance with standards like ISO 27001, NIST, and GDPR.
- **Self-Retraining Models:** Periodically update the AI model with user feedback and live data for continuous learning.
- **Multi-Tenant Support:** Enable deployment across multiple enterprise environments with tenant-level isolation and policy enforcement.
- **Mobile and CLI Access:** Access alerts and respond to incidents via mobile or terminal-based interfaces.

CHAPTER: 2

LITERATURE REVIEW

2.1 Background History

- The paper titled "**Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification**" explores the significant impact of Artificial Intelligence (AI) on cybersecurity. It highlights how AI brings about the **automation of responses, detection of network threats, and enhanced security awareness**.The research examines various modern AI techniques, including **deep learning, machine learning, and behavior analysis**, used to counter the increasing complexity of cyber threats. Specific AI applications discussed for threat detection include Machine Learning for Anomaly Detection, Deep Learning for Malware Classification, and Reinforcement Learning for Adaptive Defense. Deep learning architectures like Deep Belief Networks (DBNs), Recurrent Neural Networks (RNNs), and Convolutional Neural Networks (CNNs) are presented for their ability to capture complex relationships in data for threat detection. Classical machine learning algorithms like Support Vector Machines (SVMs) and Random Forests are also noted for their use in cybersecurity tasks. However, the paper acknowledges challenges in implementing these AI solutions, such as **adversarial attacks, data scarcity, interpretability, and the need to adapt to evolving threats**. Future directions involve developing hybrid approaches and integrating AI with emerging technologies for more robust systems. [1]

- The paper titled "**The Role of Machine Learning in Cybersecurity**" provides a **holistic and comprehensive overview** of how Machine Learning (ML) is used in the cybersecurity domain. It aims to make the topic understandable to a wide audience, including decision-makers, security professionals, and researchers.The article discusses the **benefits** of ML, particularly highlighting its applications in **cyberthreat detection**, covering areas like network intrusion, malware, and phishing detection. It also explores additional tasks ML can address, such as alert management, raw-data analysis, risk assessment, and threat intelligence. However, the paper emphasizes the **intrinsic problems** of deploying ML in cybersecurity due to the dynamic and adversarial nature of the domain, including issues like **concept drift and adversarial attacks**. It concludes by

outlining future challenges and recommendations for stakeholders to bridge the gap between research and practice. Two real industrial case studies are also presented. [2]

- The paper proposes an **adaptive self-healing mechanism** for Cyber-Physical Systems (CPS) security using **Long Short-Term Memory (LSTM) networks**. Recognizing that traditional static security methods struggle against dynamic cyber threats, this research introduces a system that **autonomously detects, responds to, and recovers** from cyber-physical attacks in real-time. The LSTM model analyzes system data to identify anomalies and initiate corrective actions. The proposed model achieved **exceptional performance**, demonstrating **99% accuracy** and **100% precision** in anomaly detection, significantly outperforming traditional methods. This work offers a robust, neural network-driven approach to enhance CPS resilience. [3]

- The paper investigates the **ethical integration of Artificial Intelligence (AI) in cybersecurity** within the Philippine context. It highlights the growing importance of AI as digital threats escalate, emphasizing the need for AI adoption that prioritizes **fairness, accountability, and transparency**. The study identifies key ethical risks, including **algorithmic biases and data privacy concerns**. While advocating for AI's potential to enhance threat detection and national security, the paper stresses the necessity of **comprehensive ethical frameworks, legal safeguards, and responsible practices** to ensure AI benefits Filipinos while safeguarding personal data and human rights.[4]

- The paper explores using **generative AI for automated security operations in cloud computing**. It highlights how generative AI offers significant benefits like **automating threat detection, real-time incident addressing, and vulnerability management** in dynamic cloud environments. The study examines integrating generative AI with cloud security tools such as AWS GuardDuty and Google Cloud Security Command Center, and applications in SOAR systems. Key outcomes include **increased response time, enhanced detection accuracy, and a shift towards proactive security**. The paper also acknowledges challenges like over-dependence and adversarial risks but emphasizes generative AI's importance in strengthening cloud defense. [5]

- The paper highlights that **traditional security methods are struggling** against the extreme growth and complexity of cyber threats. It proposes that **Artificial Intelligence (AI)** offers a promising solution to enhance **threat identification, response, and mitigation**. The paper provides a blueprint of AI-based strategies, including **anomaly detection, behavior analysis, and predictive modeling**, utilizing techniques like machine learning and natural language processing. AI's benefits include processing massive data, detecting intricate patterns, automating tasks, and

speeding up response times. However, challenges such as **data quality, interpretability, and adversarial attacks** are also addressed. The paper emphasizes the significance of AI in strengthening cybersecurity defenses. [6]

- The paper explores the significant role of **Machine Learning (ML) in enhancing cybersecurity defenses**. It emphasizes ML's ability to **automate threat detection**, analyze large data volumes, and **adapt to evolving threats**. Key opportunities discussed include improved **anomaly detection**, behavioral analysis, and automated incident response. The paper also highlights significant challenges, such as **data privacy concerns, model bias, interpretability, and adversarial attacks**. It stresses the importance of **ethical considerations** and **continuous learning** to address the dynamic nature of cyber threats. [7]

- The paper proposes a novel **AI-based cybersecurity model** designed to **optimize threat identification and response in critical infrastructure (CI)** sectors such as energy, transport, and healthcare. The system employs **advanced AI methods**, including artificial neural networks, machine learning, probabilistic models, and genetic algorithms, to analyze data and detect threats. Through simulations, it achieved a **94% classification accuracy** and **4% false positive rate**, significantly reducing threat mitigation time. The model showed enhanced scalability and performance compared to traditional methods. Challenges discussed include data variety, integration with legacy systems, and ethical considerations. [8]

- This paper provides a survey on the **use of Machine Learning (ML) and Artificial Intelligence (AI) in cybersecurity**. It investigates the critical function of ML in **strengthening cyber defenses**, highlighting how ML enables systems to **recognize and neutralize cyber threats autonomously**. The paper explores ML applications, particularly in **threat detection**, and examines challenges such as **data dependence** and **ethical choices**. It emphasizes ML's potential in cybersecurity for **protecting digital infrastructure**. [9]

- The paper evaluates the **relevance and applicability of Machine Learning (ML) and Artificial Intelligence (AI) in cybersecurity**. It highlights their potential to significantly **enhance cyber threat detection**, improve **Intrusion Detection Systems (IDS)**, and contribute to **predictive analytics and threat intelligence**. ML/AI can process vast data, learn new attacks, and automate tasks. However, the paper identifies challenges like **data privacy, false positives, and adversarial attacks**, **data quality**, **model interpretability (XAI)**, and **ethical/legal concerns**, stressing the need for **interdisciplinary collaboration** to overcome them. [10]

2.2 Existing System

Currently available cybersecurity platforms such as CrowdStrike, Splunk, and Darktrace offer threat detection, monitoring, and response automation. While these systems provide robust analytics, most still rely on signature-based detection or pre-configured rules. They struggle to detect zero-day exploits, insider threats, and novel behavior-based attacks. Moreover, these tools require constant manual configuration and lack true autonomous decision-making. Their responses are often reactive, not proactive, and most do not adapt based on evolving attack patterns or real-time context, leaving networks vulnerable in high-speed threat environments.

2.2.1 Smart Modules in Existing Systems

In existing cybersecurity systems, threat handling is often divided into isolated components—log monitoring, signature matching, alert triggering, rule-based actions—akin to "smart modules." These modules operate independently without deeply correlating multi-dimensional signals. For instance, if a user logs in from an unusual location and simultaneously attempts privilege escalation, most systems raise separate alerts but fail to recognize them as a coordinated attack. **CyberSentinel AI** bridges this gap by fusing behavioral analysis, contextual awareness, and machine learning to correlate seemingly disparate signals and respond holistically in real time.

2.3 Issues and Challenges of Existing System

- **Lack of Adaptability**: Most tools don't learn from past incidents or adjust to new threat patterns autonomously.
- **Fragmented Detection**: No deep correlation between events, leaving sophisticated multi-stage attacks undetected.
- **High False Positives**: Traditional systems flood dashboards with noisy alerts that require manual filtering.
- **Delayed Mitigation**: Human intervention is often needed to initiate a response, causing critical delays.
- **Static Intelligence**: Most systems depend on outdated rule sets or signatures, making them ineffective against zero-day threats.
- **Limited Self-Healing Capability**: Once compromised, systems rarely initiate corrective actions or isolate affected components.

2.4 Problem Statement

Modern cybersecurity systems are predominantly reactive, siloed, and reliant on manual intervention, making them inadequate against evolving threats like zero-day exploits, insider attacks, and advanced persistent threats (APTs). Traditional tools lack contextual awareness, adaptive learning, and real-time mitigation capabilities. This leads to delayed threat detection, ineffective responses, and increased vulnerability to breaches. **CyberSentinel AI** addresses this gap by introducing an intelligent, autonomous cybersecurity framework that leverages machine learning, anomaly detection, and reinforcement learning to detect, analyze, and autonomously respond to threats in real-time — transforming static defense into a self-healing, adaptive security ecosystem.

2.5 Proposed System

The proposed system, **CyberSentinel AI**, overcomes these limitations by introducing an intelligent, autonomous, and self-adaptive cybersecurity platform. It leverages advanced machine learning models—including anomaly detection, clustering, and reinforcement learning—to detect threats in real time and respond without human intervention. The system can interpret unstructured log data using NLP, detect patterns of suspicious behavior, and trigger auto-mitigation workflows.

Key features include:

- Cross-platform threat monitoring dashboard using Streamlit or React.
- Real-time log ingestion via system agents or APIs.
- Self-adaptive AI engine capable of anomaly detection and auto-response.
- Scalable, secure cloud-based backend (Firebase / MongoDB).
- Integration with system logs, firewalls, and threat intel APIs.
- Feedback loop for continuous learning and reduced false positives.

CyberSentinel AI sets a new standard in autonomous defense by shifting from reactive monitoring to proactive, intelligent threat neutralization—delivering speed, accuracy, and resilience in one cohesive system.

CHAPTER: 3

SYSTEM REQUIREMENTS

3.1 Software Requirements

- **Backend Development**:
  - **Python** (Core programming language for system logic and AI models)
  - **FastAPI / Flask** (For RESTful API services that connect the dashboard and AI engine)
- **Log & Data Ingestion:**
  - **Syslog Parsers / Logstash / Filebeat** (To collect and forward logs from endpoints)
  - **APIs** for firewall, server, and application log integration.
- **AI/ML Model Development:**
  - **Scikit-learn**, **TensorFlow**, **PyTorch** (For anomaly detection and classification models)
  - **Hugging Face Transformers** (For NLP-based log parsing and command pattern analysis).
  - **OpenAI/Groq APIs** *(Optional for large model inference during POC)*
- **Database:**
  - **MongoDB / Firebase Firestore** (To store logs, threat records, and user metadata)
- **Frontend Dashboard (Monitoring UI):**
  - **Streamlit** (Rapid prototyping dashboard for real-time alerts and analytics)
  - **ReactJS + Tailwind CSS** *(For scalable web interface in later phases)*
- **Authentication & Role Management:**
  - **Firebase Authentication** or **JWT-based OAuth** (For secure role-based access control)
- **Cloud Deployment:**
  - **AWS EC2 / Google Cloud Functions / Firebase** (To deploy APIs, AI services, and serve logs from a centralized platform)

3.2Hardware Requirements

- **Development Machine (For Training & Local Testing):**
  - **Processor**: Intel i7+ or Apple M1/M2
  - **RAM**: 16 GB or higher
  - **Storage**: Minimum 512 GB SSD

- **GPU** (Optional but ideal): NVIDIA RTX 3060+ for training complex models

- **Cloud Infrastructure (For Hosting Models and Services):**
  - **AWS EC2 / GCP VMs / Firebase Functions** for AI inference and real-time APIs.
  - Scalable resources based on network size and log volume
- **Test Devices / Environments:**
  - Virtual machines running **Linux, Windows**, and **Metasploitable** for generating synthetic attack logs.
  - Simulated environments with **Firewall logs**, **Web server logs**, and **Syslogs** for testing

3.3 Functional and Non-Functional Requirements

Functional Requirements:

1. **User Authentication & Access Control:**
   Admins securely log in to access the monitoring dashboard and system settings.
2. **Log Collection & Parsing:**
   System receives logs from endpoints, servers, and network devices in real time.
3. **Threat Detection Engine:**
   ML-based models analyze logs and detect anomalies or known threat patterns.
4. **Automated Mitigation Response:**
   Based on threat severity, the system performs actions like blocking IPs, revoking access, or sending alerts.
5. **Real-Time Monitoring Dashboard:**
   Web-based interface to display alerts, system health, and user actions.
6. **Feedback Loop for AI Models:**
   Admins can flag false positives/negatives, helping models improve over time.
7. **Threat History & Analytics:**
   Stores past threats, actions taken, and allows report generation.
8. **Cloud Sync & Data Backup:**
   All logs, threats, and configurations are securely stored in the cloud for redundancy.

Non-Functional Requirements:

1. **Scalability:**
   System should scale with increasing log volume and support multi-device integration.

2. **Security & Privacy:**

   End-to-end encryption, secure authentication, and access logs must be maintained.

3. **Performance:**

   Threat detection latency must be <2 seconds for real-time responsiveness.

4. **Reliability:**

   System must maintain >99.9% uptime with auto-restart and failover handling.

5. **Cross-Platform Compatibility:**

   Dashboard should work across devices and browsers with responsive design.

6. **Maintainability:**

   Modular codebase with separate layers for log ingestion, detection, and UI.

7. **Usability:**

   Intuitive UI/UX suitable for both technical admins and non-cybersecurity users.

3.4 Description of Tools

Tool/Framework	Purpose
FastAPI / Flask	Backend APIs for detection, response, and admin actions
Scikit-learn / TensorFlow	ML models for anomaly detection, classification, and behavior analysis
Hugging Face Transformers	NLP for parsing unstructured logs and threat commands
MongoDB / Firebase	Store logs, user actions, threat records, model outputs
Streamlit / ReactJS	Frontend dashboard for real-time alerts, history, and analytics
Firebase Authentication	Role-based access control and secure login
AWS / GCP / Firebase Cloud	Hosting for backend, database, and AI APIs
Logstash / Filebeat	Log ingestion pipeline for system and firewall logs

CHAPTER: 4

SYSTEM DESIGN

4.1 System Architecture

The architecture of **CyberSentinel AI** is modular and scalable, built to enable real-time cybersecurity threat detection, analysis, and autonomous response. The system consists of a **Streamlit-based web dashboard** for admins, a **Python-based backend** hosting the AI models, and a **cloud-based database** for log storage and threat metadata.The system collects logs from endpoints, servers, or network devices via agents or APIs. These logs are processed in real time by the AI engine to detect anomalies or known threats. Upon detection, the **Threat Response Module** can initiate automated mitigation actions such as blocking IPs or isolating services.Key cloud services (Firebase, AWS, GCP) provide authentication, model hosting, and reliable data storage.

Key Components:

- **Web Dashboard (Streamlit):**
  UI for viewing alerts, system activity, and triggering manual actions.
- **AI Backend (Python + ML):**
  Uses machine learning models (Isolation Forest, Decision Trees, etc.) for anomaly detection and auto-response logic.
- **Firebase Authentication:**
  Handles secure admin login, session control, and role-based access.
- **Database (MongoDB / Firebase Firestore):**
  Stores logs, user actions, threat classifications, and model outputs.
- **Cloud Hosting (GCP / AWS / Firebase):**
  Deploys AI services and backend APIs with reliability and global access.
- **Log Sources:**
  System logs, firewall logs, application logs, and behavioral signals from connected machines.

This architecture decouples concerns—Streamlit handles UI, Firebase manages auth/storage, and the AI backend focuses on real-time analysis and response.

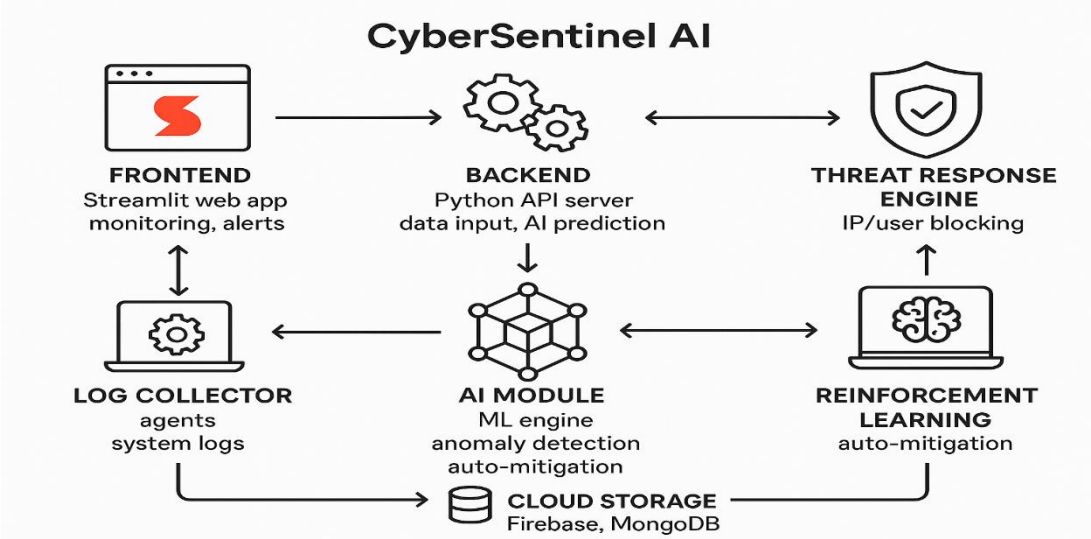


Fig 4.1: System Architecture of CyberSentinel AI

4.2 Context Analysis Diagram

4.2.1 Class Diagram

Key classes in the system include **AdminUser**, **LogEvent**, **Threat**, **ResponseAction**, and **AIModel**. Each class is designed to manage one major part of the system.

Class Overview:

- **AdminUser:** `(userId, username, email, password)`
  – Methods: `login()`, `triggerResponse()`, `reviewThreat()`
  – Each AdminUser has access to all logs and threat data.
- **LogEvent:** `(eventId, timestamp, sourceIP, eventType, status)`
  – Collected from system agents or APIs.
- **Threat:** `(threatId, threatType, confidenceScore, detectedBy, mitigationStatus)`
  – Detected by the AIModel and linked to a LogEvent.
- **ResponseAction:** `(actionId, actionType, timestamp, successFlag)`
  – Connected to a Threat, stores mitigation results.
- **AIModel:** `(modelName, version)`
  – Method: `detectThreat(LogEvent)`
  – Performs classification, anomaly detection, and scoring.

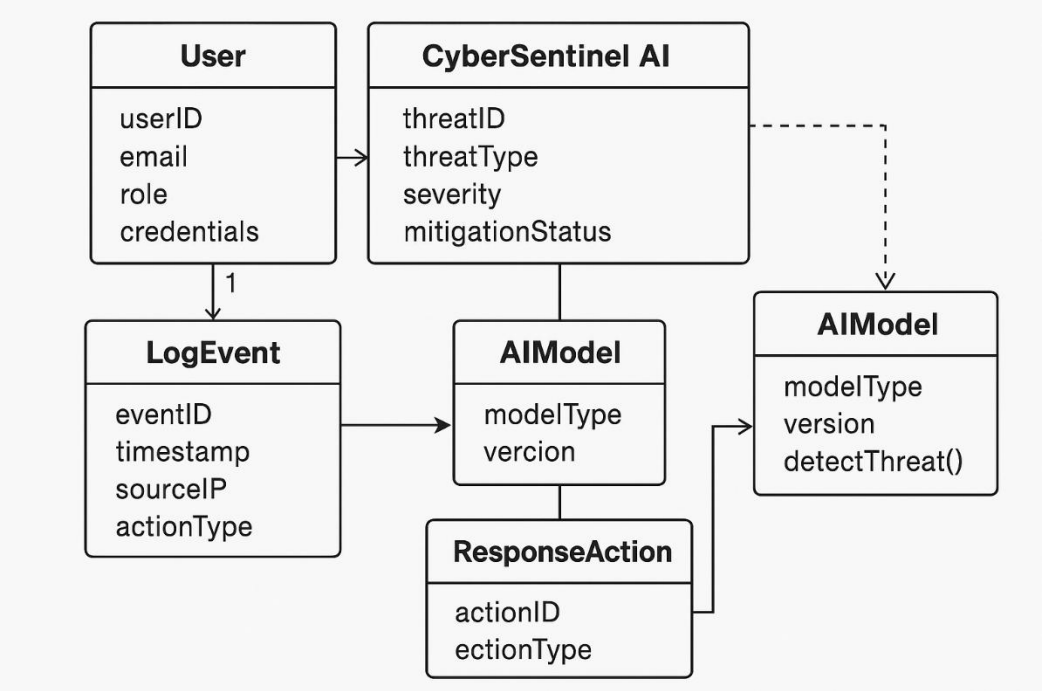


Fig 4.2: Class Diagram of CyberSentinel AI

4.2.2 Use Case Diagram :

The primary actor is the **Admin**. The system AI acts as a background process, enabling automated actions and insights.

Main Use Cases:

- **Login / Register**
  → Admin securely accesses the dashboard (via Firebase Authentication)
- **Ingest Logs**
  → Logs from systems, servers, firewalls are continuously collected.
- **Monitor Threats**
  → Admin views real-time alerts and severity levels.
- **Auto-Mitigation Response**
  → The AI system blocks malicious IPs or flags compromised sessions.
- **Feedback Loop**
  → Admin labels a threat as true/false positive for model learning.
- **Threat History Review**
  → Admin can browse historical logs, threats, and actions.

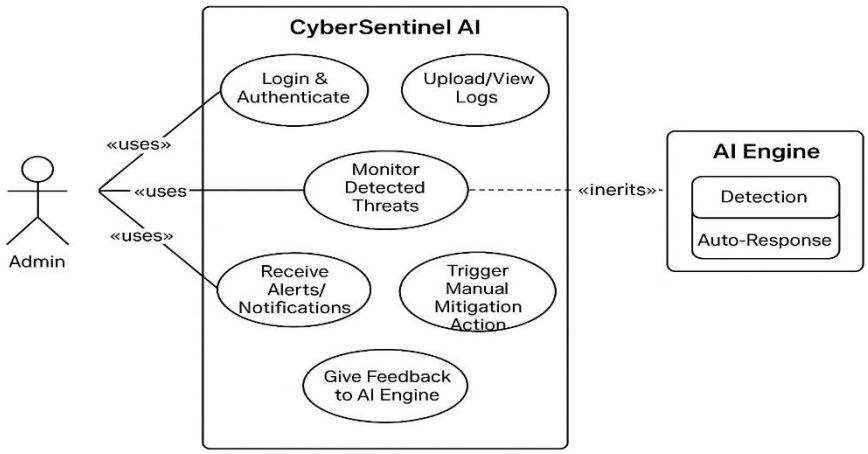


Fig 4.3: Use Case Diagram of CyberSentinel AI

4.2.3 Sequence Diagram:

Below is a typical sequence for real-time threat detection and response:

1. **Admin → System**: Opens dashboard and logs in
2. **System → Firebase Auth**: Validates credentials
3. **LogAgent → Backend API**: Sends system logs
4. **Backend API → AIModel**: Submits new log for evaluation
5. **AIModel**: Runs detection logic, scores threat
6. **AIModel → Threat DB**: Stores new threat metadata
7. **AIModel → ResponseModule**: Triggers auto-mitigation (if high severity)
8. **System → Dashboard**: Displays alerts and updates to admin

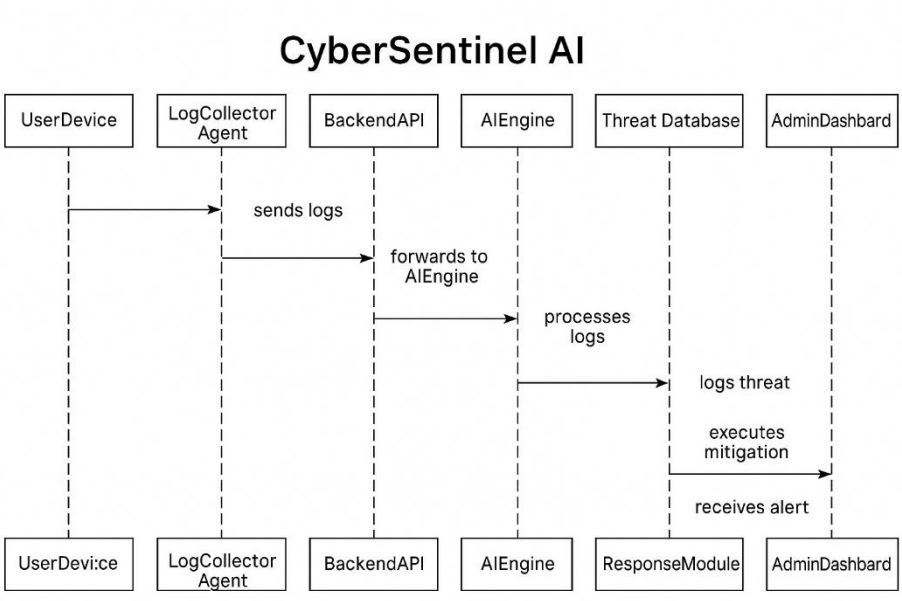


Fig 4.4: Sequence Diagram of CyberSentinel AI

4.2.4 Data Flow Diagram

- **Process 1: Log Ingestion**

  → Logs are sent by endpoints to the backend API and stored in the database.
- **Data Store: MongoDB / Firestore**

  → Stores logs, user sessions, threat metadata, and responses.
- **Process 2: Preprocessing**

  → Logs are normalized, cleaned, and structured for ML input.
- **Process 3: Threat Detection (AI Analysis)**

  → AI model classifies events as threats or benign activity.
- **Process 4: Mitigation & Alerting**

  → If needed, auto-response is triggered; dashboard and email/SMS alert is updated.
- **Output**

  → Admin dashboard shows detection logs, alerts, and historical data.

.

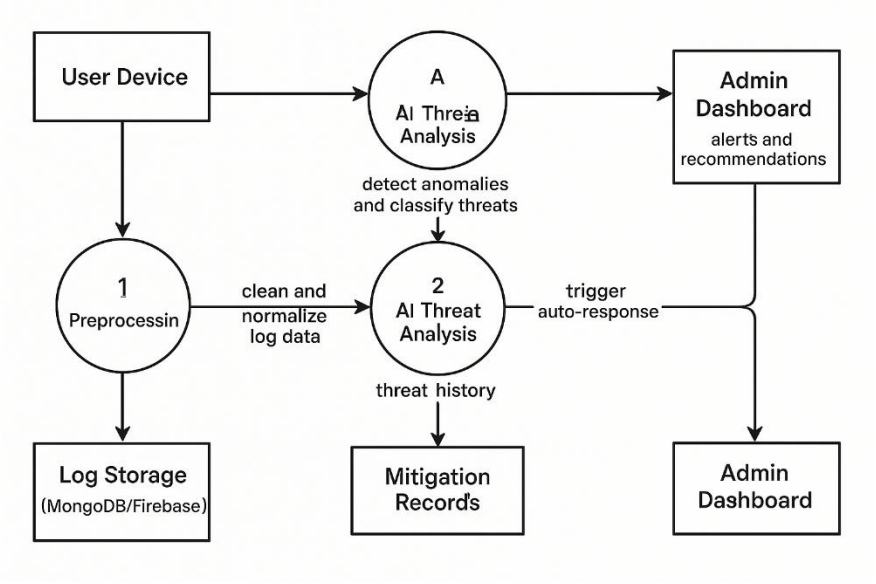


Fig 4.5: Data Flow Diagram of A-Logix

CHAPTER: 5

IMPLEMENTATION

ALGORITHMS:

The proposed **CyberSentinel AI** system integrates a combination of **machine learning**, **reinforcement learning**, and **natural language processing** to build a real-time autonomous cybersecurity solution. Each algorithm plays a key role in the system's intelligence, adaptability, and threat mitigation capabilities.Below is a detailed breakdown of the core algorithms and their roles:

1. Decision Tree / Random Forest

These supervised learning models are primarily used for **classifying cybersecurity events** such as login attempts, port scans, data transfers, and access anomalies.

- **Decision Tree:**
  - Splits event data into decision branches based on features like source IP, login method, port number, time of access, etc.
  - Easy to interpret but susceptible to overfitting.
- **Random Forest:**
  - Aggregates multiple decision trees to improve accuracy and reduce false positives.
  - More robust in noisy log environments where traditional rules fail.

Use Case in CyberSentinel AI:
Used to classify incoming log events into categories like **benign**, **suspicious**, or **malicious**—based on known behavior patterns and heuristics.

2. Natural Language Processing (NLP)

NLP is critical in interpreting unstructured log messages, system notifications, and admin commands. It converts human-readable security logs into structured data for AI analysis.

- ❖ **Preprocessing:**
    - Tokenization, stop-word removal, stemming, and lemmatization applied to log entries.
- ❖ **Modeling:**
    - **TF-IDF** and **transformer-based models** like **BERT** or **DistilBERT** extract key entities such as source IPs, attack methods, or error codes.

☑ **Use Case in CyberSentinel AI:**

Helps parse logs like:

"Multiple failed SSH login attempts from 192.168.1.45"

into:

```
{event_type: 'ssh_fail', IP: '192.168.1.45', severity: 'medium'}
```

This enables more dynamic, automated threat detection.

3. Clustering (K-Means)

An unsupervised learning technique used to discover patterns or clusters in user/system behavior. Useful when dealing with **large unlabeled datasets**.

- **Working:**
  Clusters similar log behaviors (e.g., repeated access patterns, traffic bursts, endpoint behaviors) into distinct threat groups or normal usage patterns.
- **Advantages:**
  Identifies previously unknown threats or insider attacks based on unusual clusters.

Use Case in the App:

Segments log events or users into clusters like:

- "Frequent login failures with lateral movement"
- "High-volume data transfer in off-hours"
- "Admin access anomalies"

This enables **threat prioritization** and contextual alerting.

4. Neural Networks

Artificial Neural Networks (ANNs) are used to **model complex relationships** between multi-feature security data. They excel at high-dimensional problems like **multi-feature threat classification** and **real-time alert ranking**.

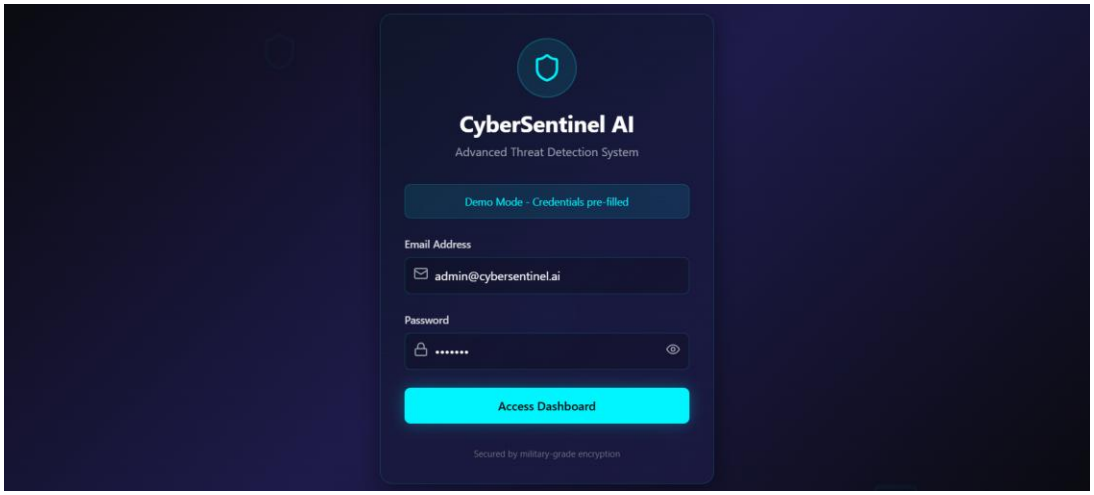
- **Architecture:**
  - Takes a vector of features (source IP, timestamp, access method, device ID, etc.)
  - Hidden layers analyze temporal + behavioral patterns
  - Outputs classification labels and confidence scores
- **Learning Process:**
  - Forward pass predicts whether an event is a threat.
  - Backpropagation adjusts weights to minimize false detection loss.

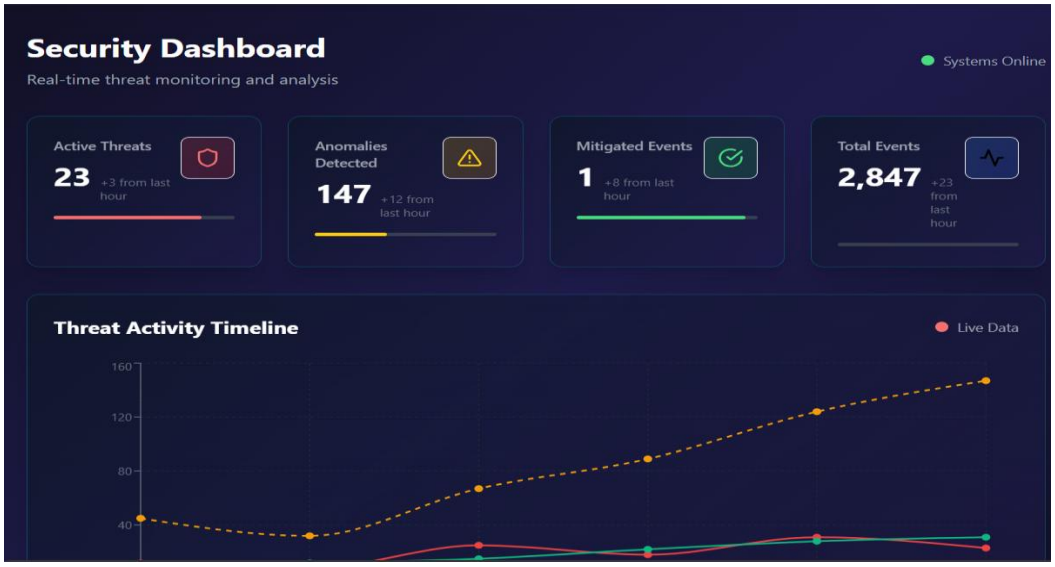
Use Case in the App:
Detects subtle anomalies like:

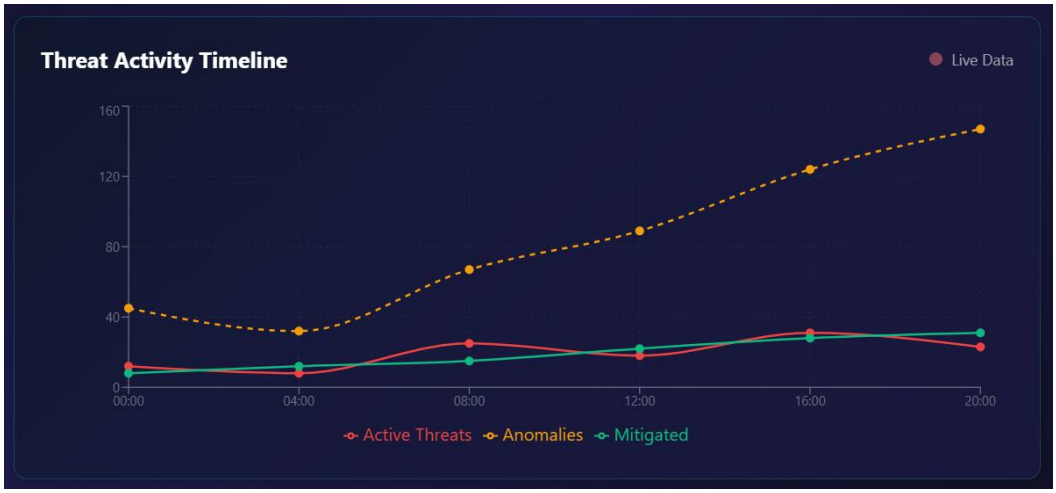
- Low-and-slow data exfiltration
- Insider reconnaissance behavior
- Privilege escalation chains

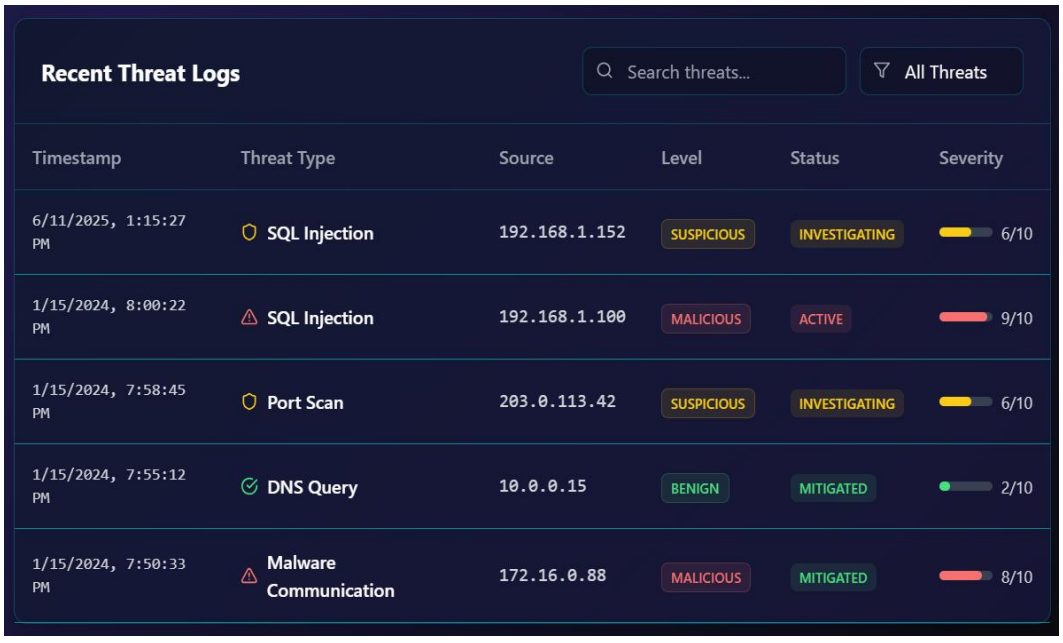
Over time, the ANN improves through **continuous learning** and **admin feedback**.

5.2 IMPLEMENTATION:




Security Dashboard
Real-time threat monitoring and analysis
Systems Online
Active Threats
23
+3 from last hour
Anomalies Detected
147
+12 from last hour
Mitigated Events
1
+8 from last hour
Total Events
2,847
+23 from last hour
Threat Activity Timeline
Live Data
160
120
80
40


Threat Activity Timeline
Live Data
160
120
80
40
0
00:00
04:00
08:00
12:00
16:00
20:00
Active Threats
Anomalies
Mitigated


Recent Threat Logs
Search threats...
All Threats
Timestamp
Threat Type
Source
Level
Status
Severity
6/11/2025, 1:15:27 PM
SQL Injection
192.168.1.152
SUSPICIOUS
INVESTIGATING
6/10
1/15/2024, 8:00:22 PM
SQL Injection
192.168.1.100
MALICIOUS
ACTIVE
9/10
1/15/2024, 7:58:45 PM
Port Scan
203.0.113.42
SUSPICIOUS
INVESTIGATING
6/10
1/15/2024, 7:55:12 PM
DNS Query
10.0.0.15
BENIGN
MITIGATED
2/10
1/15/2024, 7:50:33 PM
Malware Communication
172.16.0.88
MALICIOUS
MITIGATED
8/10

BIBLIOGRAPHY

- Patel, P. Pandey, H. Ragothaman, R. Molleti and D. R. Peddinti, "Generative AI for Automated Security Operations in Cloud Computing," 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2025, pp. 1-7, doi: 10.1109/ICAIC63015.2025.10849302.
- S. M.Nour and S. A.Said, "Harnessing the Power of AI for Effective Cybersecurity Defense," 2024 6th International Conference on Computing and Informatics (ICCI), New Cairo - Cairo, Egypt, 2024, pp. 98-102, doi: 10.1109/ICCI61671.2024.10485059.
- S. S. Gujar, "Optimizing Threat Mitigation in Critical Infrastructure through AI-Driven Cybersecurity Solutions," 2024 Global Conference on Communications and Information Technologies (GCCIT), BANGALORE, India, 2024, pp. 1-7, doi: 10.1109/GCCIT63234.2024.10862689.
- Sijjad Ali, Jia Wang, Victor Chung Ming Leung, "AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms– A comprehensive review,Information Fusion ",Volume 118,2025,102922,ISSN 1566-2535,https://doi.org/10.1016/j.inffus.2024.102922.
- Fadi Muheidat, Moayyad Abu Mallouh, Omar Al-Saleh, Omar Al-Khasawneh, Lo'ai A. Tawalbeh, "Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification, Procedia Computer Science", Volume 251,2024,Pages 287-294,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2024.11.112.
- Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions", Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535.
- F. A. Alijoyo, C. Kaur, A. Anjum, V. A. Vuyyuru and B. K. Bala, "Enhancing Cyber-Physical Systems Resilience: Adaptive Self-Healing Security Using Long Short-Term Memory Networks," 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2024, pp. 1-8, doi: 10.1109/ACCAI61061.2024.10602467.
- E. B. Blancaflor, F. G. Eleccion, F. L. Ferry, J. P. Oplado, R. E. Pajarillo and A. Villaluz, "Ethical Use of AI for Cybersecurity and Facing Digital Threats in the Philippines," 2024 IEEE 7th International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 2024, pp. 241-245, doi: 10.1109/CCET62233.2024.10837790.
- Suman Karki, A B M Mehedi Hasan, Cesar Sanin, "Use of ML and AI in Cybersecurity- A Survey", Procedia Computer Science, Volume 246, 2024, Pages 1260-1270, ISSN 1877-0509

- Mohamed Amine Ferrag, Fatima Alwahedi, Ammar Battah, Bilel Cherif, Abdechakour Mechri, Norbert Tihanyi, Tamas Bisztray, Merouane Debbah, “Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities”, Internet of Things and Cyber-Physical Systems, Volume 5, 2025, Pages 1-46, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2025.01.001.