SOFTWARE REQUIREMENTS SPECIFICATION

An Ensemble-Based Machine Learning-Envisioned Intrusion Detection in Industry 5.0-Driven Healthcare Applications

Prabhu R	21BIT042
Vijesh Pethuram K	21BIT058

Table of Contents:

1.INTRODUCTION

Creating an ensemble-based machine learning intrusion detection system (EIDS-HS) for Industry 5.0-driven healthcare applications is the main goal of this research. Cybersecurity vulnerabilities pose serious dangers to patient data and system integrity as smart healthcare relies more and more on IoT and AI. To efficiently detect intrusions, the suggested system combines SVM, KNN, and Decision Tree classifiers using ensemble learning approaches. It is assessed according to accuracy, precision, recall, and F1-score after being validated using the NSL-KDD dataset. The Scyther tool's formal verification and security analysis validate its resilience to a range of cyberthreats. The findings show that in terms of accuracy and security characteristics, EIDS-HS performs better than current intrusion detection models.

1.1 PURPOSE OF THE PROJECT

The purpose of this project is to create a strong intrusion detection system that will protect medical data and infrastructure in Industry 5.0-driven healthcare settings. The system seeks to identify a range of cyberthreats, such as malware insertion, illegal access, and denial-of-service assaults, by utilizing ensemble machine learning techniques. By merging many classifiers, it improves cybersecurity in smart healthcare by increasing detection accuracy and lowering false positives. To guarantee dependability, the system is officially validated using the Scyther tool and validated using the NSL-KDD dataset. The ultimate goal of this research is to improve healthcare cybersecurity while preserving system integrity and safeguarding patient privacy.

1.2 SCOPE OF THE PRODUCT

This project's scope comprises developing, putting into practice, and assessing an ensemble-based intrusion detection system for healthcare applications driven by Industry 5.0. By identifying cyberthreats including malware injections, unauthorized access, and denial-of-service assaults, it focuses on protecting smart healthcare environments. To improve detection accuracy, the system is built utilizing machine learning techniques, particularly ensemble learning with SVM, KNN, and Decision Tree classifiers. The NSL-KDD dataset is used for testing, while the Scyther tool is used for formal security verification. The project can be modified for real-time monitoring in IoMT-based networks, expanded to different healthcare contexts, and integrated with current security frameworks.

1.3 DEFINITIONS, ACRONYMS AND ABBREVIATIONS

EIDS-HS – Ensemble-based Intrusion Detection System for Healthcare Systems
IoT – Internet of Things
VM – Support Vector Machine
KNN – K-Nearest Neighbours
DT – Decision Tree
NSL-KDD – A benchmark dataset for intrusion detection
DoS – Denial of Service
PCA – Principal Component Analysis

1.4 REFERENCES

[1] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5615–5624, Aug. 2021.

[2] L. Zou, X. Luo, Y. Zhang, X. Yang, and X. Wang, "HC-DTTSVM: A network intrusion detection method based on decision tree twin support vector machine and hierarchical clustering," IEEE Access, vol. 11, pp. 21404–21416, 2023.

[3] M. Esmaeili, S. H. Goki, B. H. K. Masjidi, M. Sameh, H. Gharagozlou, and A. S. Mohammed, "ML-DDoSnet: IoT intrusion detection based on denial-of-service attacks using machine learning methods and NSL-KDD," Wireless Communications and Mobile Computing, vol. 2022, Aug. 2022, Art. no. 8481452.

[4] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," Wireless Networks, vol. 25, no. 8, pp. 4737–4750, Nov. 2019.

[5] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 8065–8073, Nov. 2022.

2. GENERAL DESCRIPTION:

In order to improve the security of healthcare facilities driven by Industry 5.0, the project creates an ensemble-based machine learning intrusion detection system. To identify cyberthreats and guarantee the security of private medical information in IoMT-enabled systems, it makes use of several classifiers.

2.1. PRODUCT PERSPECTIVE

a. System Interfaces:

The system will integrate with external healthcare security systems, cloud-based monitoring platforms, and hospital network infrastructures to detect and prevent cyber intrusions in real-time.

b. User Interfaces:

The system will provide an intuitive interface for healthcare administrators, IT security personnel, and hospital management teams to monitor intrusion alerts, review security logs, and configure system settings. It will also offer visual dashboards for tracking detected threats and system performance.

c. Hardware Interfaces:

The system will be compatible with standard healthcare IT infrastructure, including hospital servers, cloud computing platforms, intrusion detection sensors, and network monitoring devices, to collect and process security-related data.

d. Software Interfaces:

The system should integrate with existing healthcare security frameworks, electronic health record (EHR) systems, and cloud-based security analytics tools to facilitate seamless data exchange and intrusion response automation.

e. Communication Interfaces:

The system should support secure communication protocols, such as HTTPS, TLS, and secure API integrations, to ensure encrypted and authenticated data transmission between different system components.

f. Memory Constraints:

The system will be optimized for efficient memory usage, ensuring high performance even when processing large volumes of network traffic and security event logs in real-time.

g. Operations:

The system should support key security operations, including intrusion detection, real-time threat analysis, malware identification, and security incident reporting. It should also include features such as role-based access control, encryption, and audit logging to enhance system security.

h. Site Adaptation Requirements:

The system should be adaptable to various healthcare environments, such as hospitals, telemedicine platforms, and IoMT-based healthcare systems, ensuring flexibility to accommodate different network configurations and cybersecurity policies.

2.2 PRODUCT FUNCTIONS:

The system should enable healthcare institutions to securely detect and prevent cyber intrusions, ensuring the protection of sensitive medical data and network integrity. It should provide an intuitive interface for IT security personnel and administrators to monitor security alerts, review threat logs, and configure system settings. The system should support real-time intrusion detection, leveraging an ensemble machine learning model to identify potential threats such as malware injections, unauthorized access, and DoS attacks. It should have the capability to generate detailed security reports and analytics related to network vulnerabilities, attack patterns, and system performance. The system should seamlessly integrate with existing hospital IT infrastructure, including electronic health record (EHR) systems and IoMT devices, ensuring smooth data exchange and interoperability. It should provide automated alerts and notifications for detected intrusions, suspicious activities, and potential security breaches. The system should incorporate advanced security measures, including encryption, multi-factor authentication, and audit trails, to safeguard patient data and maintain regulatory compliance.

2.3 USER CHARACTERISTICS:

The system should be designed to cater to healthcare IT security personnel, including network administrators, cybersecurity analysts, and hospital system administrators responsible for managing and monitoring security threats. Users should have a basic understanding of network security principles, intrusion detection mechanisms, and cybersecurity protocols. The system should provide different levels of access and permissions based on user roles, ensuring that only authorized personnel can configure security settings, review threat reports, and respond to detected intrusions.

2.4 GENERAL CONSTRAINTS:

The system should comply with relevant cybersecurity and healthcare regulations, such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), to ensure the privacy and security of patient data. It should be scalable to support various healthcare environments, from small clinics to large hospitals, handling increasing network traffic and security threats efficiently. The system should be compatible with standard operating systems and web-based security platforms, ensuring seamless integration with existing healthcare IT infrastructure. It should feature a responsive design, enabling access from multiple devices, including desktop computers, tablets, and mobile devices, for real-time monitoring and management of security threats.

2.5 ASSUMPTIONS AND DEPENDENCIES:

The system assumes that healthcare organizations have a stable and secure internet connection to enable real-time monitoring and communication between system components. It assumes that IT security personnel and administrators will receive proper training on using the system effectively for intrusion detection, threat analysis, and response management. The system may depend on external cybersecurity databases or APIs for threat intelligence, malware signatures, and real-time updates on emerging cyber threats to enhance detection accuracy and system performance.

3. SPECIFIC REQUIREMENTS

The system should address challenges related to cybersecurity threats in Industry 5.0-driven healthcare environments, including malware attacks, unauthorized access, and denial-of-service incidents. It should provide real-time intrusion detection, threat analysis, and automated response mechanisms to mitigate cyber risks. Compliance with regulatory frameworks, such as HIPAA, is essential to ensure the system meets industry standards for data security and privacy. The system should effectively integrate machine learning-based intrusion detection techniques, leveraging ensemble models to enhance threat detection accuracy, reduce false positives, and provide a robust security solution for healthcare networks.

3.1 EXTERNAL INTERFACE REQUIREMENTS

The system should provide a web-based dashboard for IT security personnel and administrators to monitor security threats, intrusion alerts, and system performance in real-time. It should be compatible with standard healthcare IT infrastructure, including hospital servers, cloud storage, and security hardware such as firewalls and intrusion detection sensors. The system should seamlessly integrate with electronic health record (EHR) systems, cloud-based security platforms, and external threat intelligence databases to enhance cybersecurity. Secure communication protocols such as HTTPS and TLS should be implemented to ensure encrypted data transmission and real-time alert notifications. Additionally, the system should be optimized for real-time threat detection and response, handling large volumes of network traffic efficiently while maintaining minimal latency.

3.2 FUNCTIONAL REQUIREMENTS

The system should enable real-time detection and prevention of cyber threats in Industry 5.0-driven healthcare environments, ensuring the security of medical data. It should identify and mitigate threats such as malware, unauthorized access, and denial-of-service attacks using ensemble machine learning models for improved accuracy. The system should seamlessly integrate with hospital IT infrastructure, electronic health record systems, and cloud-based security platforms. Additionally, it should support secure communication protocols, data encryption, and access controls to protect sensitive healthcare information.

3.2.1 USER CLASS 1 – IT SECURITY PERSONNEL/ADMINISTRATOR

3.2.1.1 FUNCTIONAL REQUIREMENT 1.1

ID: FR1

TITLE: User Authentication

DESC: Only authorized IT security personnel and administrators can log into the system using secure credentials and multi-factor authentication.

3.2.1.2 FUNCTIONAL REQUIREMENT 1.2

ID: FR2

TITLE: Monitor Network Traffic

DESC: The system continuously monitors network traffic in real time, capturing and analyzing data packets for potential security threats.

3.2.1.3 FUNCTIONAL REQUIREMENT 1.3

ID: FR3

TITLE: Detect Intrusions

DESC: The system identifies cyber threats, such as malware injections, unauthorized access, and denial-of-service (DoS) attacks, using an ensemble machine learning model.

3.2.1.4 FUNCTIONAL REQUIREMENT 1.4

ID: FR4

TITLE: Generate Security Alerts

DESC: When an intrusion is detected, the system generates an alert and notifies the IT security team via the dashboard, email, or SMS notifications.

3.2.1.5 FUNCTIONAL REQUIREMENT 1.5

ID: FR5

TITLE: Automated Threat Response

DESC: The system can automatically block malicious IP addresses, restrict unauthorized access, or quarantine compromised devices based on predefined security rules.

3.2.1.6 FUNCTIONAL REQUIREMENT 1.6

ID: FR6

TITLE: Review and Update Security Policies

DESC: Administrators can review security logs and update system policies, such as modifying intrusion detection thresholds or access control rules, to improve security.

3.2.2 USER CLASS 2 - ADMINISTRATOR/SECURITY ANALYST

3.2.2.1 FUNCTIONAL REQUIREMENT 2.1

ID: FR7

TITLE: View Security Logs

DESC: Administrators can access and analyse historical security logs to track past intrusions and system activity.

3.2.2.2 FUNCTIONAL REQUIREMENT 2.2

ID: FR8

TITLE: Generate Security Reports

DESC: The system provides detailed security reports on intrusion attempts, detected threats, and system performance for compliance and analysis.

3.2.2.3 FUNCTIONAL REQUIREMENT 2.3

ID: FR9

TITLE: Configure Security Policies

DESC: Administrators can define and modify security policies, such as intrusion detection thresholds and automated response settings, to improve system security.

.

3.3 PERFORMANCE REQUIREMENTS

The system should prioritize real-time processing and optimization for intrusion detection, ensuring minimal latency in threat identification and response. It should efficiently analyse large volumes of network traffic and security logs using ensemble machine learning models while maintaining high accuracy. The system should implement resource-efficient algorithms to optimize computational performance, reducing the overhead on hospital IT infrastructure. Continuous monitoring and analysis of system performance should be conducted to improve detection speed and reduce false positives. Additionally, the system should be scalable to handle increasing cybersecurity demands without compromising efficiency.

3.4 SOFTWARE SYSTEM ATTRIBUTES

a. Reliability

The system should ensure continuous and accurate detection of cyber threats in Industry 5.0-driven healthcare environments, minimizing false positives and false negatives. By leveraging ensemble machine learning models, the system should maintain high detection accuracy and resilience against evolving cyber threats. Additionally, real-time monitoring and automated threat response mechanisms should ensure the system operates without disruption, safeguarding healthcare IT infrastructure.

b. Security

The system should implement robust security measures, including encrypted communication (HTTPS, TLS), access controls, and multi-factor authentication, to protect sensitive healthcare data. It should utilize machine learning models to detect and prevent malware attacks, unauthorized access, and denial-of-service incidents. The integration of security logs and audit trails will enhance accountability and provide forensic capabilities for cybersecurity investigations.

c. Portability

The system should be designed as a web-based platform, ensuring compatibility across various devices, including desktops, tablets, and mobile devices. It should support deployment on different operating systems, such as Windows, Linux, and cloud-based environments, to provide flexibility in healthcare settings. Additionally, the system's architecture should allow integration with existing hospital networks and security frameworks, ensuring seamless interoperability.

d. Availability

The system should maintain high availability by ensuring real-time intrusion detection, automated threat response, and failover mechanisms to prevent downtime. It should provide continuous monitoring of network traffic and system logs, ensuring healthcare institutions can detect and respond to cyber threats without interruption. Cloud-based deployment options should also enhance accessibility and reliability.

e. Maintainability

The system should be designed with a modular and scalable architecture, allowing easy updates and integration of new security features. Machine learning models should be continuously trained with updated threat intelligence to adapt to emerging cybersecurity threats. The use of well-structured code and version control mechanisms should facilitate efficient software maintenance and upgrades.

f. Other Requirements

The system should integrate with external cybersecurity tools and databases to receive real-time updates on new malware signatures and intrusion patterns. It should also support automated reporting and compliance checks to ensure adherence to regulatory standards such as HIPAA and NIST. Additionally, the system should provide detailed threat analytics to assist IT security teams in optimizing cybersecurity strategies for healthcare environments.

4. APPENDICES:

4.1. USE CASE TEMPLATE

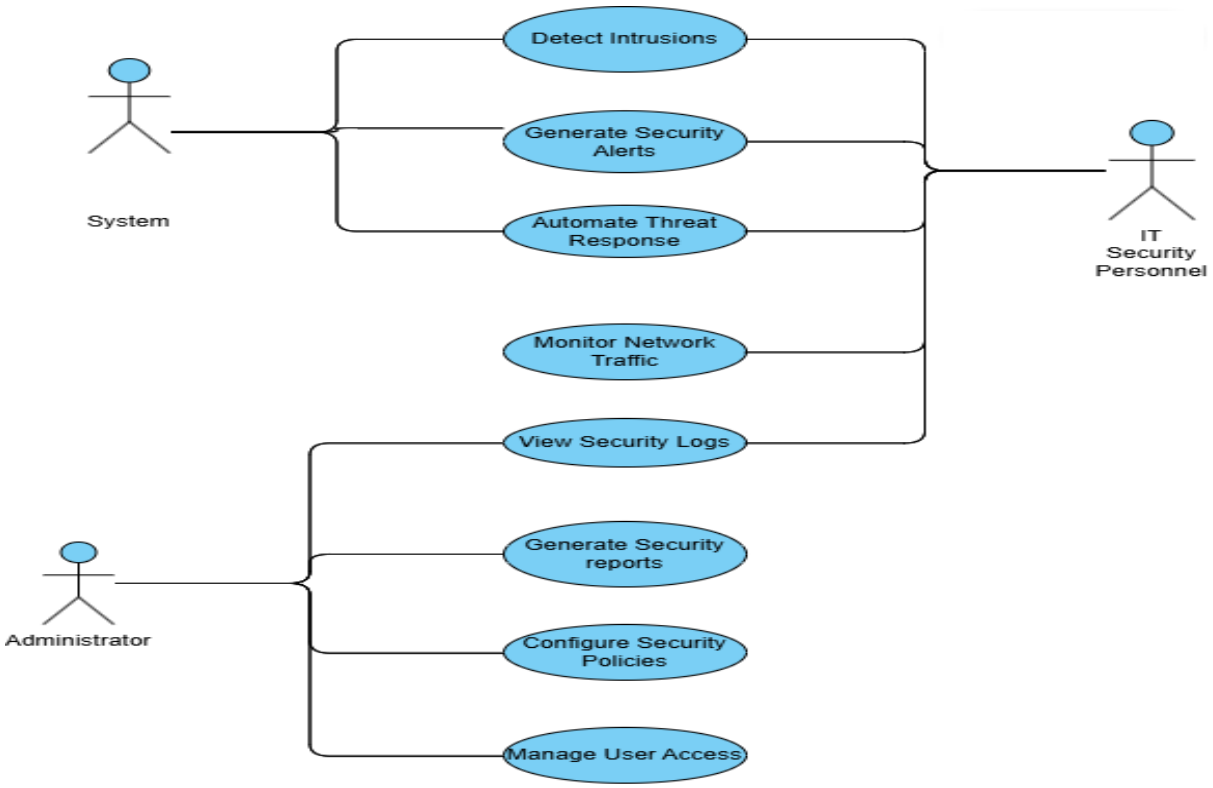

Fig 1 : Use Case Diagram

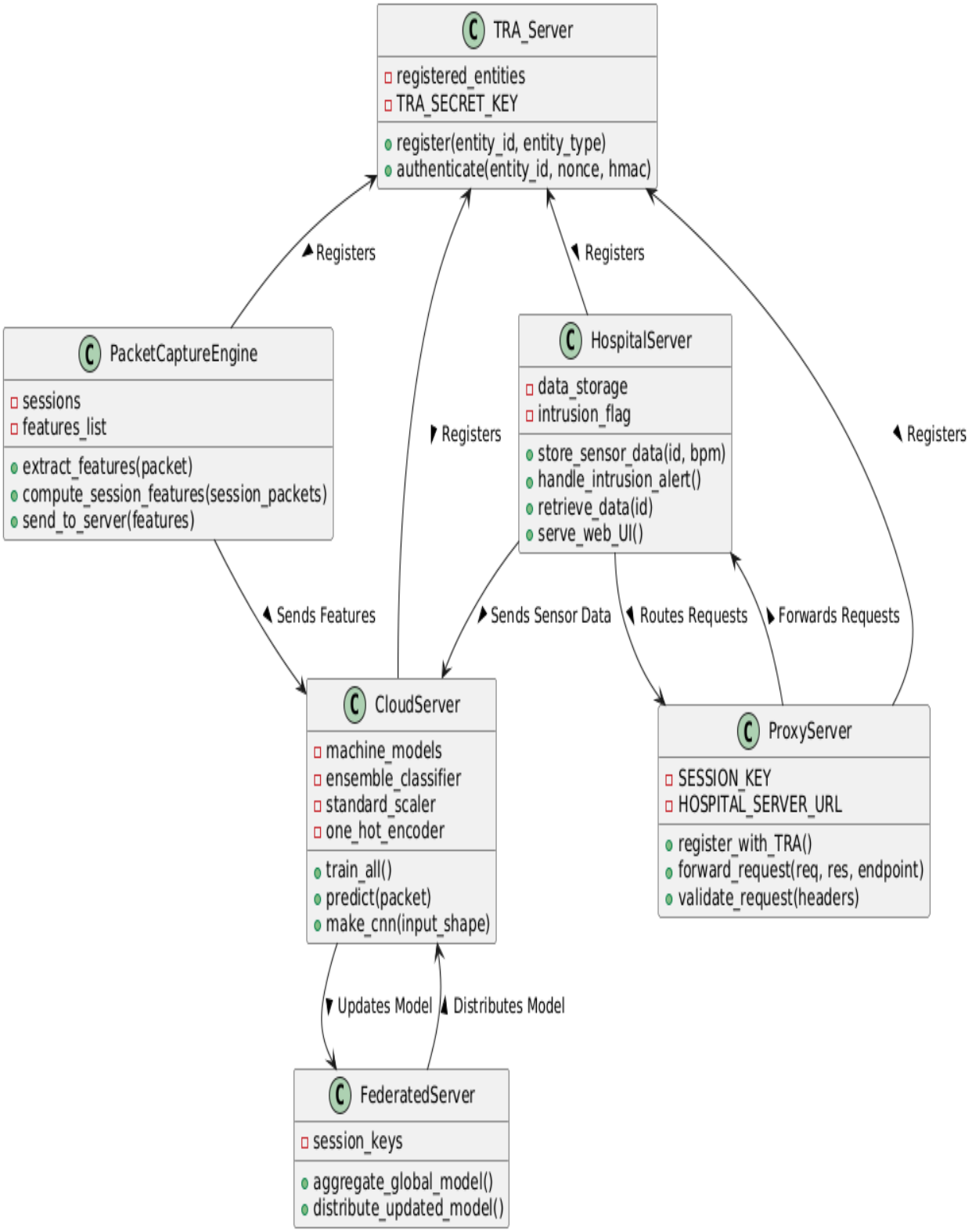

Fig 2 : Class Diagram

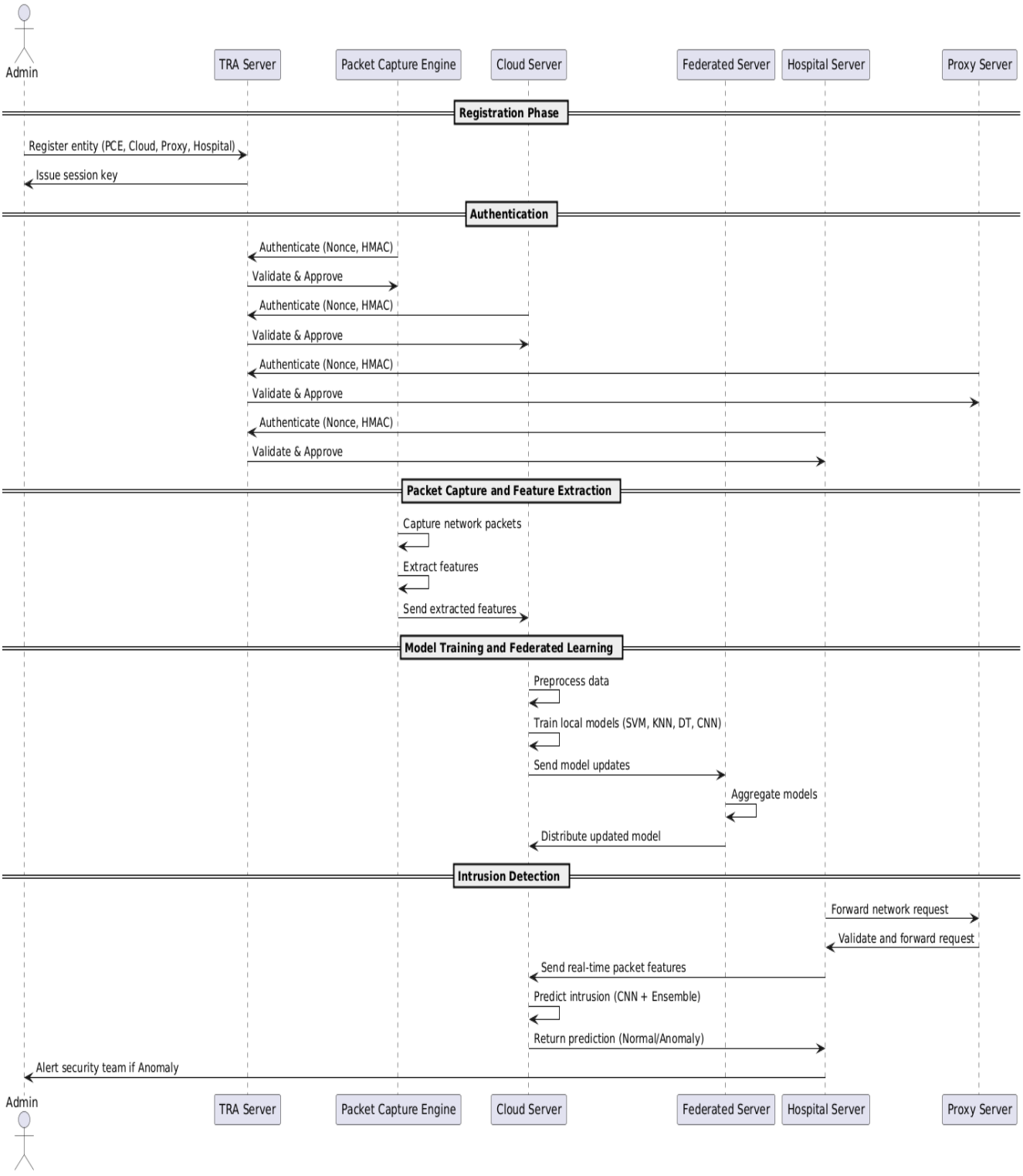

Fig 3 : Sequence Diagram

5. INDEX:

5.1. DIFFERENT NOTATIONS:

Symbol	Description
DoS	Denial of Service
HS	Hospital Server
MiTM	Man-in-the-Middle Attack
TLS	Transport Layer Security