Software Requirement Specification

for

**Human Intrusion Detection System for defense Assistance**

Submitted as a part of course curriculum for

**Bachelor of Technology**

in

**Computer Science**



**Submitted by**

Asmit Tyagi {2100290120058}

Ashish Sikarwar {2100290120053}

Archit Kaushik {2100290120046}

Arun Kumar {2000290120042}

**Under the Supervision of**

Mr. Sreesh Gaur

Assistant Professor

**KIET Group of Institutions, Ghaziabad**

**Department of Computer Science**

**Dr. A.P.J. Abdul Kalam Technical University**

**2022-2023**

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
|  | Page No. |
| TITLE PAGE ....................................................................................................................   1. INTRODUCTION …………………………………………………………………..    1. Introduction …………………………………………………………………….    2. Purpose ………………………………………………………………………….    3. Scope ……………………………………………………………………………    4. Document Conventions …………………………………………………………    5. Intended Audience ……………………………………………………………… 2. OVERALL DESCRIPTION ………………………………………………………….   2.1 Product Perspective ……………………………………………………………….  2.2 Product Functions …………………………………………………………………  2.3 User Classes and Characteristics ………………………………………………….  2.4 Operating Environment ……………………………………………………………  2.5 Design and Implementation Constraints ………………………………………….  2.6 User Documentation ………………………………………………………………   * 1. Assumptions and Dependencies ………………………………………………….   3. SPECIFIC REQUIREMENTS ……………………………………………………….  3.1 External Interface Requirements ………………………………………………….  3.1.1 User Interfaces ……………………………………………………………..  3.1.2 Hardware Interfaces ………………………………………………………..  3.1.3 Software Interfaces …………………………………………………………  3.1.4 Communication Interfaces …………………………………………………  3.2 Functional Requirements …………………………………………………………  3.2.1 Surveillance Camera Integration …………………………………………..  3.2.2 Deep Learning Model ……………………………………………………..  3.2.3 Alerting Mechanism ……………………………………………………….  3.2.4 User Interface ………………………………………………………………  3.3 Performance Requirements ……………………………………………………….  3.4 Security Requirements ……………………………………………………………  3.5 Software Quality Attributes ………………………………………………………  3.5.1 Reliability ………………………………………………………………….  3.5.2 Availability …………………………………………………………………  3.5.3 Maintainability ……………………………………………………………..  3.5.4 Portability ………………………………………………………………….  3.6 Other Requirements …………………………………………………………  4. SYSTEM MODELS …………………………………………………………………..  4.1 ER Diagram ………………………………………………………………………  4.2 Activity Diagram …………………………………………………………………  5. REFERENCES ………………………………………………………………………… | I  3-4  3  3  3  4  4  5-7  5  5  5  6  6  6  7  8-12  8  8  8  8  9  9  9  9  10  10  10  10  11 11  11  11  12  12  13-16  13-14  15-16  17 |

**CHAPTER-1**

**INTRODUCTION**

**1.1 Introduction**

The Human Infiltration Detection System (HIDS) represents a critical endeavor in the realm of security technology, aimed at addressing the persistent challenge of unauthorized human infiltrations in defense and sensitive areas. In today's dynamic security landscape, traditional surveillance methods often fall short in providing real-time detection and prevention capabilities necessary to thwart sophisticated infiltration attempts. As a response to this pressing need, the HIDS project endeavors to harness the power of advanced artificial intelligence (AI) and deep learning techniques to develop a robust and proactive security solution.

**1.2 Purpose**

The purpose of this Software Requirements Specification (SRS) document is to provide a comprehensive understanding of the requirements and specifications for the development of the Human Infiltration Detection System (HIDS). The HIDS is envisioned as a cutting-edge security solution designed to mitigate the risk of unauthorized human infiltrations in defense and sensitive areas. This document serves as a foundation for system design, development, testing, and deployment phases of the project.

**1.3 Scope**

The scope of this document encompasses both functional and non-functional requirements of the HIDS, covering its features, interfaces, performance criteria, security measures, and other relevant system attributes. It delineates the system's boundaries and provides a roadmap for system developers, stakeholders, and other project participants. The scope also includes any assumptions and constraints that may impact the development and implementation of the HIDS.

**1.4 Document Conventions**

This document adheres to established conventions for documenting software requirements. It utilizes a standardized format for presenting requirements, including unique identifiers, detailed descriptions, acceptance criteria, and traceability matrices. The terminology used in the document follows industry standards and conventions to ensure clarity and consistency across all sections. Additionally, references to external sources, standards, and documents are provided to support the understanding and implementation of the requirements outlined herein.

**1.5 Intended Audience**

The intended audience for this SRS document includes:

System developers and engineers responsible for designing, implementing, and testing the HIDS.

Project managers and stakeholders overseeing the development and deployment of the system.

Security experts and personnel involved in the operation, maintenance, and monitoring of the HIDS.

Regulatory authorities, auditors, and compliance officers responsible for assessing the system's adherence to security standards and regulations.

**CHAPTER-2**

**OVERALL DESCRIPTION**

**2.1 Product Perspective:**

The Human Infiltration Detection System (HIDS) operates as an independent security solution designed to complement existing surveillance and security infrastructure in defense and sensitive areas. While the HIDS interfaces with surveillance cameras and other security systems, it functions autonomously to detect and prevent unauthorized human infiltrations in real-time. The system provides a proactive approach to security by leveraging advanced artificial intelligence (AI) and deep learning algorithms to analyze surveillance footage and identify suspicious activities.

**2..2 Product Functions:**

The primary function of the HIDS is to detect and prevent unauthorized human infiltrations in defense and sensitive areas. Key functionalities include:

Real-time surveillance: The system continuously monitors video feeds from surveillance cameras to identify potential security threats.

Anomaly detection: Advanced deep learning algorithms analyze surveillance footage to detect suspicious activities and anomalies indicative of unauthorized infiltrations.

Alerting mechanism: Upon detection of a security threat, the HIDS generates real-time alerts to notify security personnel, enabling prompt response and intervention.

User interface: The system provides a user-friendly interface for security personnel to monitor infiltration detection activities, view live video feeds, and manage alert notifications.

**2.3 User Classes and Characteristics:**

The HIDS is designed to serve security personnel and stakeholders involved in the monitoring and management of security operations in defense and sensitive areas. User classes and their characteristics include:

Security personnel: Users responsible for monitoring infiltration detection activities, responding to security alerts, and managing system settings.

System administrators: Users tasked with configuring and maintaining the HIDS, including software updates, user management, and system configuration.

Stakeholders: Individuals or entities with a vested interest in the security of the protected area, such as government agencies, military personnel, or private security organizations.

**2.4 Operating Environment:**

The HIDS operates in diverse environmental conditions commonly found in defense and sensitive areas, including indoor and outdoor environments, varying lighting conditions, and adverse weather conditions. The system is designed to withstand environmental factors such as temperature fluctuations, humidity, and dust, ensuring reliable performance in challenging environments.

**2.5 Design and Implementation Constraints:**

The design and implementation of the HIDS are subject to certain constraints and considerations, including:

Hardware compatibility: The system must be compatible with a wide range of surveillance cameras and hardware components commonly used in security applications.

Data privacy and security: The HIDS must adhere to strict data privacy and security regulations to protect sensitive information captured by surveillance cameras and ensure compliance with legal requirements.

Scalability: The system should be scalable to accommodate the needs of varying deployment scenarios, from small-scale installations to large-scale deployments covering extensive areas.

**2.6 User Documentation:**

Comprehensive user documentation will be provided to support system installation, configuration, and operation. Documentation will include user manuals, installation guides, troubleshooting procedures, and system specifications to facilitate user understanding and ensure efficient use of the HIDS.

**2.7 Assumptions and Dependencies:**

The successful development and deployment of the HIDS are contingent upon certain assumptions and dependencies, including:

Availability of surveillance footage: The system relies on continuous access to surveillance footage from integrated cameras to detect and prevent unauthorized infiltrations.

Adequate network connectivity: The HIDS requires stable network connectivity to transmit surveillance data, generate alerts, and facilitate communication between system components.

Compliance with regulations: The system assumes compliance with relevant regulations and standards governing security operations, data privacy, and surveillance technology.

**CHAPTER-3**

**SPECIFIC REQUIREMENTS**

**3.1 External Interface Requirements**

**3.1.1 User Interfaces**

The user interface of the HIDS shall be intuitive and user-friendly, providing security personnel with access to critical system functionalities. Key requirements include:

Graphical User Interface (GUI): The GUI shall feature interactive controls for monitoring surveillance footage, viewing alerts, and managing system settings.

Real-time Updates: The GUI shall display live video feeds from surveillance cameras, with real-time updates to ensure timely detection of security threats.

Alert Notifications: The GUI shall provide visual and auditory alerts upon detection of unauthorized infiltrations, allowing security personnel to respond promptly.

**3.1.2 Hardware Interfaces**

The HIDS shall interface with a variety of hardware components commonly used in security applications, including surveillance cameras and network infrastructure. Requirements include:

Compatibility: The system shall support integration with a wide range of surveillance cameras, including IP cameras, analog cameras, and thermal imaging cameras.

Network Connectivity: The system shall interface with Ethernet networks for data transmission and communication with surveillance cameras and other system components.

**3.1.3 Software Interfaces**

The HIDS shall interface with software components for data processing, analysis, and management. Requirements include:

Compatibility: The system shall be compatible with operating systems commonly used in security applications, including Windows and Linux.

Integration with Deep Learning Frameworks: The system shall interface with deep learning frameworks, such as TensorFlow or PyTorch, for implementing advanced AI algorithms for infiltration detection.

**3.1.4 Communication Interfaces**

The HIDS shall support communication between system components for seamless operation. Requirements include:

Network Protocols: The system shall use standard network protocols, such as TCP/IP, for communication between surveillance cameras, alerting mechanisms, and user interfaces.

Encryption: Communication between system components shall be encrypted to ensure data security and prevent unauthorized access.

**3.2 Functional Requirements**

**3.2.1 Surveillance Camera Integration**

The HIDS shall integrate with surveillance cameras to capture video footage for infiltration detection. Requirements include:

Video Capture: The system shall capture video feeds from surveillance cameras installed in the secured area.

Multiple Camera Support: The system shall support integration with multiple surveillance cameras to provide comprehensive coverage of the monitored area.

**3.2.2 Deep Learning Model**

The HIDS shall utilize deep learning algorithms for analyzing surveillance footage and detecting unauthorized infiltrations. Requirements include:

Anomaly Detection: The system shall employ advanced deep learning techniques to identify anomalies indicative of unauthorized human presence or suspicious activities.

Real-time Processing: The system shall perform real-time processing of surveillance footage to enable timely detection of security threats.

**3.2.3 Alerting Mechanism**

The HIDS shall generate real-time alerts upon detection of unauthorized infiltrations. Requirements include:

Alert Generation: The system shall generate alerts with details such as location, time, and nature of the infiltration attempt.

Customizable Alerts: Security personnel shall be able to customize alert settings, including threshold levels for triggering alerts.

**3.2.4 User Interface**

The HIDS shall provide a user-friendly interface for monitoring infiltration detection activities and managing system settings. Requirements include:

Graphical User Interface: The system shall feature a graphical user interface with interactive controls for viewing live video feeds, managing alerts, and adjusting system settings.

Mobile Compatibility: The user interface shall be compatible with mobile devices, allowing security personnel to monitor system activities remotely.

**3.3 Performance Requirements**

The HIDS shall meet performance criteria to ensure efficient operation and timely detection of security threats. Requirements include:

Real-time Detection: The system shall detect unauthorized infiltrations within milliseconds of occurrence to minimize response times.

Scalability: The system shall be scalable to accommodate varying deployment scenarios, from small-scale installations to large-scale deployments covering extensive areas.

**3.4 Security Requirements**

The HIDS shall adhere to strict security measures to protect sensitive information and prevent unauthorized access. Requirements include:

Data Encryption: Communication between system components shall be encrypted to prevent eavesdropping and data tampering.

Access Control: The system shall implement access control mechanisms to restrict access to sensitive functionalities and data.

**3.5 Software Quality Attributes**

**3.5.1 Reliability**

The HIDS shall operate reliably under varying environmental conditions and system loads. Requirements include:

Fault Tolerance: The system shall continue to operate in the event of hardware or software failures, ensuring uninterrupted surveillance and infiltration detection.

Error Handling: The system shall handle errors gracefully, providing informative error messages and recovering from errors whenever possible.

**3.5.2 Availability**

The HIDS shall maintain high availability to ensure continuous surveillance and infiltration detection capabilities. Requirements include:

Redundancy: The system shall incorporate redundant components to mitigate the risk of single points of failure and ensure uninterrupted operation.

Failover Mechanisms: The system shall implement failover mechanisms to switch to backup components in the event of failure, minimizing downtime.

**3.5.3 Maintainability**

The HIDS shall be easy to maintain and update to address evolving security threats and system requirements. Requirements include:

Modularity: The system shall be modular, allowing individual components to be updated or replaced without impacting the overall system.

Documentation: Comprehensive documentation shall be provided to support system maintenance tasks, including installation, configuration, and troubleshooting procedures.

**3.5.4 Portability**

The HIDS shall be portable across different hardware and software environments to accommodate varying deployment scenarios. Requirements include:

Platform Independence: The system shall be platform-independent, allowing it to run on different operating systems and hardware architectures.

Compatibility: The system shall be compatible with a wide range of surveillance cameras and network infrastructure components commonly used in security applications.

**3.6 Other Requirements**

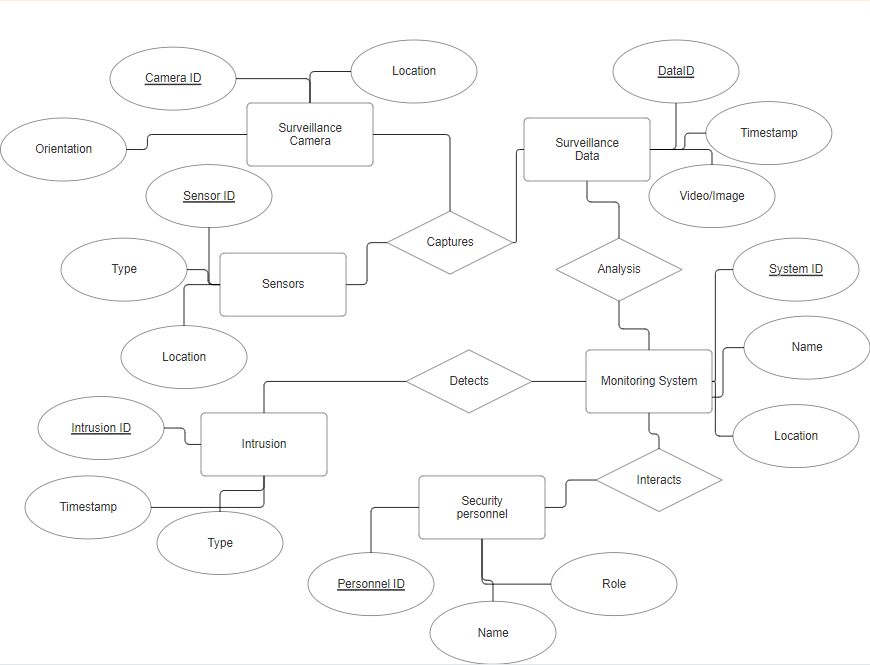
Compliance: The HIDS shall comply with relevant regulations and standards governing security operations, data privacy, and surveillance technology.

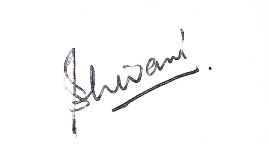
Performance Testing: The system shall undergo rigorous performance testing to validate its capabilities and ensure compliance with specified performance criteria.

**CHAPTER-4**

**SYSTEM MODELS**

**4.1 ER Diagram-**

****



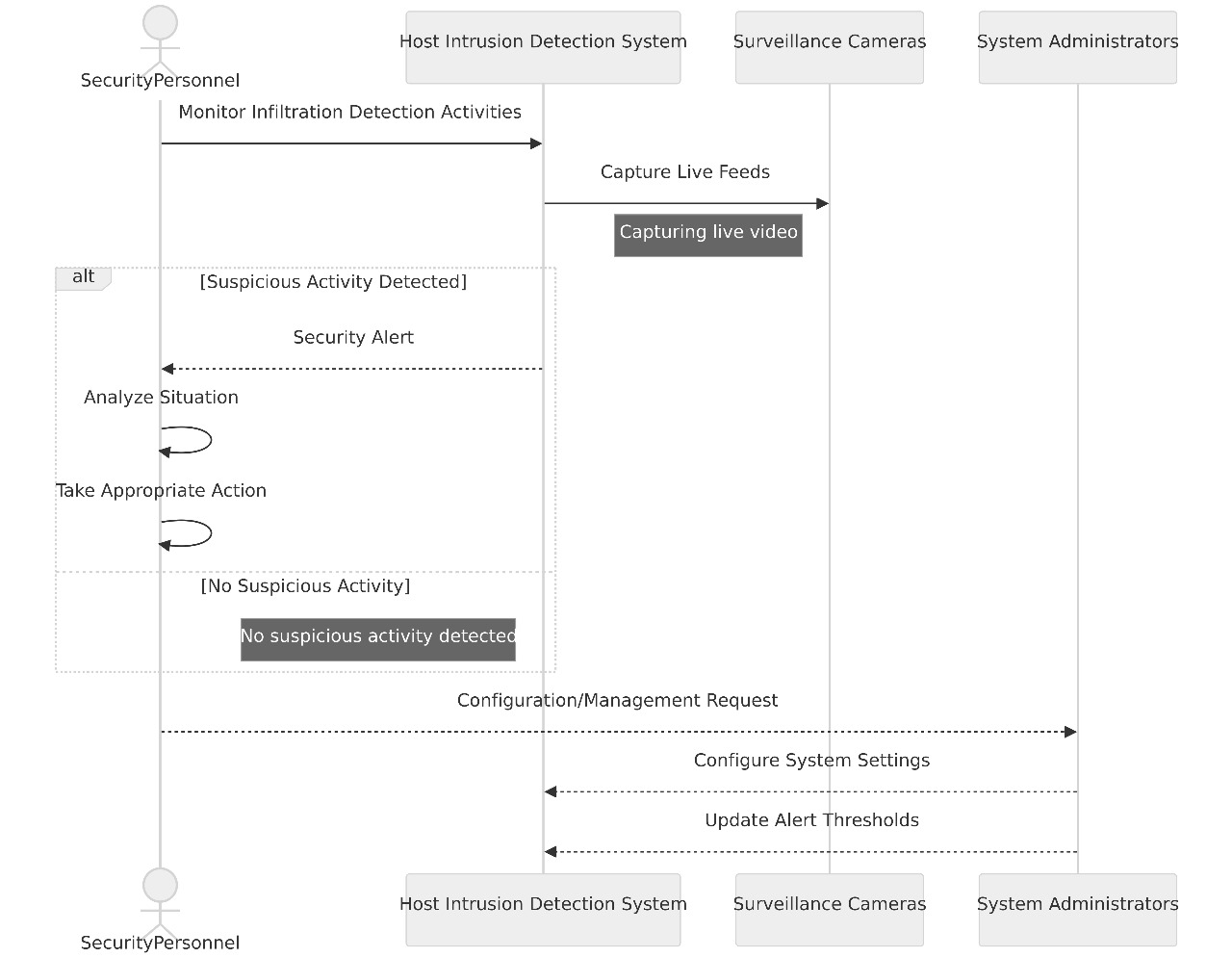
Entities:

1. **Surveillance Camera**:
   * Attributes: Camera ID, Location, Orientation
   * Description: Represents cameras deployed within the defense installation to capture surveillance data.
2. **Sensor**:
   * Attributes: Sensor ID, Type, Location
   * Description: Represents sensors deployed within the defense installation to detect environmental conditions such as motion, temperature, or sound.
3. **Surveillance Data**:
   * Attributes: Data ID, Timestamp, Video/Image
   * Description: Represents the raw data captured by surveillance cameras, including video footage or images.
4. **Monitoring System**:
   * Attributes: System ID, Name, Location
   * Description: Represents the central monitoring system responsible for analysing surveillance data and detecting intrusions.
5. **Intrusion**:
   * Attributes: Intrusion ID, Timestamp, Type
   * Description: Represents detected intrusions within the defence installation, categorized by type (e.g., unauthorized entry, suspicious behaviour).
6. **Security Personnel**:
   * Attributes: Personnel ID, Name, Role
   * Description: Represents security personnel responsible for monitoring the system and responding to detected intrusions.
7. **Alert**:
   * Attributes: Alert ID, Timestamp, Description
   * Description: Represents alerts generated by the system to notify security personnel of detected intrusions or abnormal events.

Relationships:

* Surveillance Camera captures Surveillance Data.
* Sensor detects Environmental Conditions.
* Surveillance Data is analysed by the Monitoring System.
* Intrusion is detected by the Monitoring System.
* Security Personnel receive Alerts.
* Security Personnel interact with the Monitoring System.

**4.2 Sequence Diagram:**

****

**Description :**

**Actor Lifelines:**

Security Personnel

System Administrators

Surveillance Cameras

Sequence of Actions:

Security Personnel initiates the sequence by requesting to monitor infiltration detection activities.

HIDS receives the request and begins monitoring the live feeds from Surveillance Cameras.

If suspicious activity is detected, HIDS generates a security alert.

Security Personnel, upon receiving the alert, responds by analyzing the situation and taking appropriate action.

System Administrators may also intervene by configuring or managing system settings, which could affect the monitoring and alerting processes.

**Message Exchanges:**

Security Personnel sends a "Monitor Infiltration Detection Activities" request to HIDS.

HIDS communicates with Surveillance Cameras to capture live video feeds.

If suspicious activity is detected, HIDS sends a "Security Alert" message to Security Personnel.

Security Personnel responds with a "Take Action" message, indicating their response to the security alert.

System Administrators may send messages related to managing system settings, such as "Configure System Settings" or "Update Alert Thresholds".

**Order of Events:**

The sequence begins with Security Personnel initiating the monitoring process.

Surveillance Cameras capture video feeds, which are monitored by HIDS in real-time.

If an intrusion is detected, HIDS generates a security alert and notifies Security Personnel.

Security Personnel then analyze the situation and respond accordingly, possibly with further actions or interventions.

**REFERENCES**

1. Li, S., Zhu, Y., Tian, Z., & Fang, B. (2018). Deep learning-based human intrusion detection system for surveillance video. IEEE Access, 6, 33321-33331. doi:10.1109/ACCESS.2018.2834545
2. Zhang, H., Yang, Y., Wang, X., & Li, C. (2020). Hybrid CNN-RNN architecture for real-time human intrusion detection in surveillance videos. Sensors, 20(15), 4198. doi:10.3390/s20154198
3. Sharma, A., & Jain, A. (2019). Human Intrusion Detection System using Convolutional Neural Networks. In 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 75-79). doi:10.1109/SPIN.2019.8711786
4. Alzubi, J. A., Alsmadi, M. K., Al-Ayyoub, M., & Jararweh, Y. (2019). Deep learning-based intrusion detection system for industrial internet of things. Computers & Electrical Engineering, 75, 309-318. doi:10.1016/j.compeleceng.2019.01.031
5. Khani, M., & Kazemi, S. (2020). Human intrusion detection using deep learning techniques. Journal of Ambient Intelligence and Humanized Computing, 11, 1667–1676. doi:10.1007/s12652-019-01389-4
6. Arivazhagan, S., Jayapriya, A., & Gokulnath, C. (2021). A review on human intrusion detection system using deep learning algorithms. Journal of Ambient Intelligence and Humanized Computing, 12, 891–899. doi:10.1007/s12652-020-02852-8