**FYP SRS Document Template**

Final Year Project

Software Requirement Specification

For

AI Smart Behavior Analysis

BSCS

By

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S# | **Name** | **Registration #/Roll #/Section** | **Mobile #** | **E-Mail** |
| 1. | Saad Amir | Fa-21/051/B | 03285333392 | saad.amir@live.com |
| 2. | Nawab Iftikhar | Fa-21/076/B | 03331474584 | nawabpanu@gmail.com |

**Supervised by:**

Ma’am Anila Amjad **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(**Signature**)**



Department of Computer Science

Lahore Garrison University

Lahore

Table of Contents

1. Introduction...........................................................................................................

1.1 Purpose ........................................................................................................................

1.2 Document Conventions ................................................................................................

1.3 Intended Audience and Reading Suggestions ..............................................................

1.4 Product Scope ..............................................................................................................

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 ..................................................................................................

2.7 Assumptions and Dependencies ................................................................................

3. External Interface Requirements .......................................................................

3.1 User Interfaces ...........................................................................................................

3.2 Hardware Interfaces ...................................................................................................

3.3 Software Interfaces ....................................................................................................

3.4 Communications Interfaces .......................................................................................

4. System Features ..................................................................................................

4.1 System Feature 1 ........................................................................................................

4.2 System Feature 2 (and so on) .....................................................................................

5. Other Nonfunctional Requirements ...................................................................

5.1 Performance Requirements ........................................................................................

5.2 Safety Requirements ..................................................................................................

5.3 Security Requirements ...............................................................................................

5.4 Software Quality Attributes .......................................................................................

5.5 Business Rules ...........................................................................................................

References ....................................................................................................................

# **1. Introduction**

## 1.1 **Purpose**

AI Smart Behavior Analysis aids greatly in security and surveillance sector, it does this by analyzing people’s behavior, our purpose is to create a machine learning model capable of identifying and flagging unusual or potentially criminal activities in real-time. The model will analyze input data, such as surveillance footage, to detect anomalous patterns that may indicate suspicious or illegal behavior. This system is designed to assist law enforcement, security personnel, or any relevant stakeholders in monitoring and responding to potential threats in an efficient and automated manner.

## **1.2 Document Conventions**

Report traditions are basic for guaranteeing clarity, consistency, and ease of understanding in specialized and utilitarian documentation for Smart Behavior Analysis model. These traditions give a standardized way to display data, empowering clients, designers, and partners to successfully evaluate the model. Given below are the essential report traditions regularly considered:

**1. Common Organizing Traditions**

**Text style Fashion and Measure:**

Utilize a clear, proficient textual style such as Times New Roman, Arial, Calibri. Headings are regularly bigger (e.g. 14–16 pt), whereas body content is 11–12 pt.

Headings and Subheadings:

Organized employing a various leveled structure (e.g., H1, H2, H3) to recognize segments clearly.

Numbering Framework:

Utilize a coherent numbering organize (e.g., 1.1, 1.2) for segments and subsections to progress route.

**2. Phrasing and Definitions**

**Glossary:**

Incorporate a segment for key terms such as "Client," "Arrangement," "Supplier," and "Teleconsultation" to guarantee all clients have a common understanding.

Consistency:

Utilize standardized wording all through the report to maintain a strategic distance from disarray.

**6. Adaptation Control**

**Modification History:**

Keep up a table posting upgrades, counting adaptation number, changes made, date, and creator.

**Date Arrange:**

Utilize ISO standard organize (YYYY-MM-DD) for clarity and universal consistency.

## **1.3 Intended Audience and Reading Suggestions**

This Software Requirements Specification (SRS) document is intended for the following audiences:

* **Developers and Engineers**: To provide a detailed understanding of the functional and non-functional requirements, system architecture, and other technical aspects necessary for the design, development, and implementation of the machine learning model.
* **Data Scientists and Machine Learning Specialists**: To understand the specific needs and challenges of the anomaly detection model, including data inputs, feature selection, training requirements, and evaluation criteria for performance metrics.
* **Project Managers**: To gain an understanding of the project’s scope, objectives, timelines, and resource requirements for successful implementation.
* **Quality Assurance (QA) Team**: To comprehend the expected behavior of the system, including how to test the model’s effectiveness in detecting unusual or criminal activities, as well as identifying edge cases and performance requirements.
* **Stakeholders and Clients**: To understand the functional goals of the system, the outcomes expected, and how the system will impact operational security or law enforcement efforts.
* **Regulatory and Compliance Authorities**: To ensure the system complies with privacy, ethical, and legal standards related to surveillance, data collection, and the detection of criminal activity.

## **1.4 Product Scope**

The product is a machine learning-based system designed to detect unusual or potentially criminal activities, with a particular focus on identifying the presence of weapons. The system will analyze data from diverse sources such as surveillance footage (e.g., CCTV cameras), sensor data, transactional records, and other relevant information to identify abnormal behaviors or potential security threats. In particular, the model will be trained to detect the presence of weapons in images or videos, supporting law enforcement and security personnel in their efforts to prevent violent incidents and respond to potential threats effectively.

# **2. Overall Description**

## **2.1 Product Perspective**

The product is envisioned as a **standalone security tool** that complements traditional security measures such as human monitoring, surveillance cameras, and physical security. It will analyze video streams, sensor data, and other real-time inputs to detect signs of criminal activity or the presence of weapons that may pose a threat to public safety. The system will operate as an autonomous layer of detection that works alongside human oversight to provide more efficient, immediate identification of potential risks.

* Integration with Existing Systems: The model is designed to be easily integrated with various existing security infrastructures, such as CCTV camera networks, public surveillance, smart sensors, or retail security systems. It will be compatible with industry-standard video formats and sensor data inputs.
* **External Interfaces**: The system will interface with surveillance cameras and sensors to receive real-time video and data feeds. It will also be capable of sending alerts to external systems, such as law enforcement dispatch systems, security operation centers (SOCs), or other monitoring platforms.
* **User Roles and Interactions**:
  + **Security Personnel**: Users will monitor alerts generated by the system, review flagged events, and take further action when necessary. They will use the interface to interact with the model's outputs.
  + **Law Enforcement**: Law enforcement officers can use the system to review potential threats (e.g., weapons or unusual activity), prioritizing urgent cases and facilitating rapid response.
  + **Administrators**: System administrators will be responsible for maintaining and updating the model, handling system configurations, and overseeing the integration with existing infrastructure.

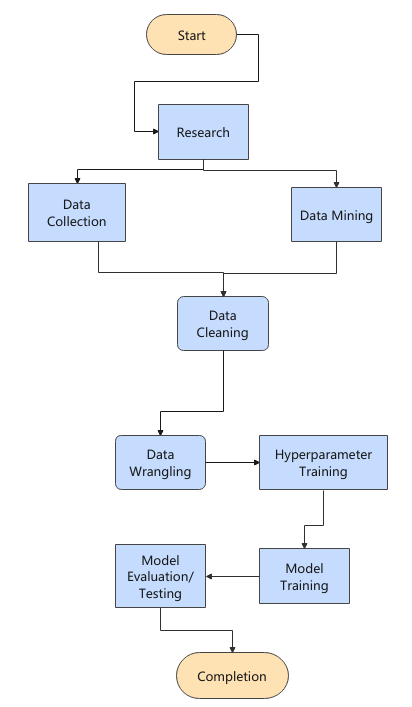
Product Position

The machine learning-based detection model will provide enhanced situational awareness by autonomously detecting unusual behaviors and the presence of weapons, thus reducing human error or mistake and improving the speed of threat identification. It will be particularly beneficial in environments where continuous monitoring and immediate response are critical, such as:

* **Public Places**: Airports, train stations, malls, or large public events, where detecting weapons and suspicious activities can help prevent violent incidents.
* **Retail Environments**: Stores and warehouses, where the system can prevent theft, violence, and detect any concealed or openly carried weapons.
* **Critical Infrastructure**: High-security areas such as government buildings, military installations, or private facilities that need to detect weapons and criminal behavior in real-time.
* **Urban Surveillance**: City-wide or community-based monitoring systems that focus on improving public safety by identifying potential threats.

****Assumptions and Dependencies****

* **Data Quality**: The effectiveness of the system will depend heavily on the quality and resolution of the input data (video, sensor feeds, etc.). High-quality cameras and sensor networks will improve the model's ability to detect weapons and anomalous activities.
* **Legal Compliance**: The system will adhere to relevant privacy and data protection regulations, especially regarding video surveillance and the handling of personal data. Compliance with local laws and ethical standards will be necessary to ensure the system can be used safely and responsibly.
* **Infrastructure Availability**: The system assumes that users have access to appropriate hardware (e.g., cameras, sensors) and software infrastructure (e.g., cloud or on-premise servers) to support the integration and operation of the model.

Flowchart:

## **2.2 Product Functions**

The AI Smart Behavior Analysis system is designed to detect unusual behavior, predict potential criminal activity, identify weapons, and recognize the occurrence of a robbery. It utilizes advanced machine learning and computer vision techniques to analyze real-time video feeds and other relevant data. The system's functions are outlined as follows:

2.2.1 Real-Time Behavior Analysis

* **Function**: The system will monitor and analyze human behavior in real-time, using input from security cameras and other data sources. It will detect abnormal or suspicious actions based on pre-defined behavioral patterns.
* **Inputs**: Real-time video feed from surveillance cameras, sensor data (if available), user-defined behavior patterns.
* **Outputs**: Behavioral status report (e.g., suspicious, normal), real-time alerts or notifications.
* **Description**: The system will continuously evaluate movement patterns, gestures, and body language, comparing them against a database of behaviors classified as normal or suspicious. It will flag any activity that deviates significantly from the norm for further investigation.

2.2.2 Predictive Crime Detection

* **Function**: The system will predict potential criminal activity by recognizing patterns of behavior that are statistically linked to criminal actions.
* **Inputs**: Real-time video data, historical crime data (if available), contextual environmental factors.
* **Outputs**: Crime prediction reports, threat assessment alerts.
* **Description**: Based on historical data and machine learning models, the system will analyze the likelihood of criminal activities such as theft, vandalism, or violent acts occurring. Alerts will be generated when the likelihood of a crime reaches a certain threshold, allowing for proactive intervention.

2.2.3 Weapon Detection

* **Function**: The system will detect and identify weapons in real-time using computer vision techniques, analyzing both objects and gestures that may indicate weapon possession.
* **Inputs**: Video feed from surveillance cameras, images from public and private spaces.
* **Outputs**: Alerts for weapon detection, weapon identification report.
* **Description**: The system will scan for visible weapons (e.g., guns, knives) in real-time. It will use machine learning models trained to recognize various weapon types in different contexts, including unusual handling or positioning of such items.

2.2.4 Robbery Detection

* **Function**: The system will detect potential robbery events based on certain behavioral and environmental factors commonly associated with robbery scenarios.
* **Inputs**: Real-time video, location data (if applicable), time of day, behavioral analysis data.
* **Outputs**: Robbery detection alerts, context-specific risk report.
* **Description**: By identifying behaviors such as forced entry, rapid movement of individuals in restricted areas, or confrontational gestures, the system will detect signs of a robbery. It will also analyze the context of the environment (e.g., nighttime, isolated areas) to increase the accuracy of detecting such events.

2.2.5 Alert System and Notifications

* **Function**: The system will trigger alerts based on detected suspicious or abnormal activity.
* **Inputs**: Suspicious behavior, predicted criminal activity, weapon detection, robbery detection.
* **Outputs**: Alerts in various formats (e.g., text, email, push notification), severity level of threat.
* **Description**: Alerts will be sent in real-time to designated personnel (e.g., security officers, law enforcement) based on the identified threat level. The system will categorize the severity of the situation (e.g., low, medium, high) and prioritize the alerts accordingly.

2.2.6 Continuous Learning and Adaptation

* **Function**: The system will continuously learn and improve its detection accuracy by incorporating new data and feedback.
* **Inputs**: New data inputs (e.g., video feeds, feedback from security personnel), performance evaluation metrics.
* **Outputs**: Improved detection models, periodic updates to the system.
* **Description**: The AI will continuously learn from its predictions and human feedback to enhance its accuracy. Over time, the system will adapt to new patterns of behavior, improving its ability to detect previously unseen anomalies and reducing false positives.

2.2.7 Integration with External Systems

* **Function**: The system will be able to integrate with external security systems, such as alarms, emergency response systems, and access control systems.
* **Inputs**: Data from external systems (e.g., alarm triggers, security database entries).
* **Outputs**: Coordinated actions with integrated systems (e.g., alarm activation, door locking).
* **Description**: In the event of a detected threat, the system will communicate with external security infrastructure to take appropriate action, such as activating alarms, locking doors, or notifying law enforcement.

## **2.3 User Classes and Characteristics**

The **AI Smart Behavior Analysis** system will serve a variety of users with distinct roles and responsibilities. Each user class will have different characteristics and levels of access to the system. Below are the defined user classes and their corresponding characteristics:

2.3.1 Security Personnel

* **Description**: Security personnel are the primary users responsible for monitoring and responding to security threats. They are typically employed by businesses, facilities, or public spaces and are tasked with ensuring the safety of the environment.
* **Characteristics**:
  + **Experience Level**: Intermediate to expert knowledge of security systems and incident response.
  + **Primary Functions**:
    - Monitor alerts generated by the system for suspicious activity.
    - Respond to detected threats (e.g., criminal behavior, weapons, or robbery).
    - View real-time video feeds and analyze detected behaviors or threats.
    - Review and analyze generated reports on security events.
    - Coordinate with law enforcement or emergency responders when necessary.
  + **Access Level**: Access to real-time alerts, video feeds, behavior analysis data, and incident reports. Permissions to interact with the system’s alerts and integrate with other security systems (e.g., alarms, locks).
  + **Device Usage**: Desktop or mobile application, typically used in monitoring stations or mobile units.

2.3.2 Law Enforcement Agencies

* **Description**: Law enforcement officers or agencies are users responsible for investigating potential criminal activities flagged by the system. They may be external or internal users who act upon more serious threats or incidents.
* **Characteristics**:
  + **Experience Level**: Expert in law enforcement procedures and criminal investigation.
  + **Primary Functions**:
    - Review detailed incident reports and alerts to determine further investigation or action.
    - Access to historical data and crime prediction analytics for ongoing investigations.
    - Collaboration with security personnel to assess crime scenarios and respond appropriately.
    - Trigger external actions, such as notifying emergency responders or investigating flagged events in-depth.
  + **Access Level**: Access to detailed incident reports, weapon detection data, predictive analytics, and historical event data. Limited control over system settings or configurations.
  + **Device Usage**: Desktop or mobile application with law enforcement-specific interfaces for deeper investigation into flagged events.

2.3.3 System Administrators

* **Description**: System administrators are responsible for maintaining and configuring the AI Smart Behavior Analysis system. They ensure the system's integrity, perform updates, and configure settings to suit the organization’s security needs.
* **Characteristics**:
  + **Experience Level**: Expert knowledge of AI systems, database management, and security software.
  + **Primary Functions**:
    - Manage user accounts and permissions for different user classes.
    - Perform system maintenance, updates, and troubleshooting.
    - Configure machine learning models for improved accuracy.
    - Monitor system performance and implement optimizations.
    - Analyze system logs for any issues and ensure data security compliance.
  + **Access Level**: Full administrative access to all system settings, logs, machine learning models, user management, and performance monitoring.
  + **Device Usage**: Desktop application, typically used in server-side environments or by IT staff.

2.3.4 Facility Managers / Supervisors

* **Description**: Facility managers or supervisors oversee the general safety and security of the facility but may not have direct responsibilities for security monitoring. They receive higher-level reports and can issue commands based on system insights.
* **Characteristics**:
  + **Experience Level**: Intermediate knowledge of facility management and security oversight.
  + **Primary Functions**:
    - Receive summarized alerts and reports on security-related incidents or trends.
    - Oversee personnel actions and coordinate responses.
    - Review system performance metrics and report effectiveness of security protocols.
  + **Access Level**: Access to high-level summary reports, alerts, and system performance dashboards. No access to real-time video feeds or granular data.
  + **Device Usage**: Desktop or mobile devices for receiving reports, notifications, and managing team coordination.

2.3.5 Data Analysts (Optional)

* **Description**: Data analysts or security researchers will work with the system to generate insights from large data sets. They will analyze the historical data generated by the system and look for patterns, trends, and opportunities to improve the model’s detection capabilities.
* **Characteristics**:
  + **Experience Level**: Expert in data analysis, machine learning, and statistical methods.
  + **Primary Functions**:
    - Analyze historical behavior patterns, crime data, and security reports.
    - Generate insights and recommendations for improving detection algorithms.
    - Develop and fine-tune predictive models to improve the system's ability to detect unusual behavior or criminal activity.
  + **Access Level**: Access to historical data, behavior analysis reports, crime prediction analytics, and system performance metrics. Limited or no access to live surveillance video feeds or real-time alerts.
  + **Device Usage**: Desktop or workstation with tools for data visualization and statistical analysis.

2.3.6 End Users / General Public (Optional)

* **Description**: In certain cases, the system may offer a public-facing interface for community safety alerts or reporting, although these users will not interact with the system in terms of monitoring or data analysis.
* **Characteristics**:
  + **Experience Level**: Basic, non-technical users.
  + **Primary Functions**:
    - Receive alerts and notifications about potential threats or suspicious activity in their area (e.g., public safety notifications).
    - Report suspicious activities via a mobile or web interface.
  + **Access Level**: Limited access to public alerts and notifications. No access to system's security data or video feeds.
  + **Device Usage**: Mobile devices or web interface for alerts and reporting purposes.

## **2.4 Operating Environment**

The **AI Smart Behavior Analysis** system is designed to operate in a range of environments, from private security installations to large-scale public safety monitoring systems. It leverages both hardware and software components to function effectively. Below are the key aspects of the operating environment in which the system will function.

2.4.1 Hardware Requirements

The system will operate on a combination of specialized hardware for video surveillance, computational power for AI processing, and standard user devices for interaction. The primary hardware components include:

* **Surveillance Cameras**: High-definition cameras with at least 1080p resolution, capable of streaming video in real-time. They may include fixed or pan-tilt-zoom (PTZ) capabilities, and should have infrared or low-light capabilities for night-time monitoring.
  + **Camera Interface**: HDMI, IP-based (e.g., ONVIF compatibility for standardization), or proprietary protocols for video feed integration.
* **Computational Servers**: Dedicated servers or cloud infrastructure with sufficient processing power to handle real-time video analytics, machine learning models, and large-scale data processing. This may include:
  + **Processor**: Multi-core CPUs (e.g., Intel Xeon or AMD EPYC) and GPUs (e.g., NVIDIA Tesla, Quadro, or equivalent) for deep learning-based image and behavior analysis.
  + **Memory**: At least 64GB of RAM (or higher depending on the system scale).
  + **Storage**: SSDs or other high-speed storage options with a minimum of 1TB for handling video and data logs, with additional backup storage for redundancy.
* **Network Infrastructure**: A reliable and secure network infrastructure to support high-bandwidth video streaming and real-time communication with client devices. This includes:
  + **Internet Connection**: Stable internet connection with a bandwidth of at least 10 Mbps for cloud-based operations or local networking if the system is hosted on-premises.
  + **Local Network**: Wired Ethernet or secure Wi-Fi network for communication between cameras, servers, and user devices.
* **User Devices**: Devices for interacting with the system, including desktops, laptops, and mobile devices. User devices should support modern operating systems and browsers to interact with the AI system's interfaces.
  + **Desktop/Laptop**: Running Windows 10 or higher, macOS, or Linux, with up-to-date web browsers (e.g., Google Chrome, Mozilla Firefox, Microsoft Edge).
  + **Mobile Devices**: Smartphones or tablets running iOS or Android with compatible apps or web browsers.

2.4.2 Software Requirements

The **AI Smart Behavior Analysis** system utilizes several software layers to operate effectively, including operating systems, databases, machine learning frameworks, and application layers.

* **Operating System**:
  + The server-side components will run on Linux-based OS (e.g., Ubuntu, CentOS) or Windows Server, depending on the deployment configuration.
  + Client-side applications may run on various platforms, including Windows, macOS, iOS, and Android.
* **Machine Learning Frameworks**:
  + TensorFlow, PyTorch, or other deep learning frameworks for behavior analysis and pattern recognition.
  + OpenCV or similar computer vision libraries for real-time image and video analysis.
  + Scikit-learn or similar libraries for data preprocessing, anomaly detection, and predictive crime models.
* **Database Systems**:
  + A relational database management system (RDBMS) such as PostgreSQL or MySQL will be used for storing structured data, such as event logs, user profiles, and system settings.
  + A NoSQL database such as MongoDB or Elasticsearch for handling unstructured data like video metadata and logs.
  + Data storage for videos and high-resolution images will likely use distributed file systems or cloud storage (e.g., Amazon S3, Azure Blob Storage).
* **Web Server & Application Framework**:
  + The web interface for monitoring and managing the system will run on a web server like Apache, Nginx, or Microsoft IIS.
  + The front-end application will be built using modern JavaScript frameworks such as React or Angular, while the back-end may be built using Python (Flask/Django), Node.js, or Java (Spring Boot).
* **Security & Encryption**:
  + TLS/SSL encryption for secure communication between all client devices, servers, and databases.
  + OAuth or JWT (JSON Web Token) for secure user authentication and authorization.
  + Regular security patches and updates to the system to prevent vulnerabilities.

2.4.3 Environmental Conditions

The system is intended to operate in a wide range of physical environments, from controlled indoor facilities to outdoor settings. Key environmental considerations include:

* **Temperature**: Hardware, especially surveillance cameras and servers, should operate within a range of 0°C to 40°C (32°F to 104°F), with the potential for higher tolerances in rugged or outdoor environments.
* **Humidity**: Systems should be designed to function in environments with humidity levels from 10% to 90% non-condensing. Cameras and hardware in outdoor environments may need additional weatherproofing.
* **Lighting**: The system is expected to work under varying lighting conditions, including low-light and nighttime scenarios. Cameras with infrared (IR) capabilities or low-light image sensors are required to ensure visibility under minimal lighting.
* **Vibration**: In outdoor or industrial settings, equipment may need to be resistant to vibrations or shock. Cameras and sensors should be housed in sturdy enclosures that meet relevant standards for physical durability (e.g., IP65 rating for dust and water resistance).
* **Power Supply**: The system requires a reliable power supply for its hardware components. Backup power solutions such as UPS (Uninterruptible Power Supply) should be considered to ensure continuous operation in case of power failure.

2.4.4 System Scalability

The **AI Smart Behavior Analysis** system is designed to scale depending on the number of cameras, sensors, and monitoring stations in place. It can be deployed across various scales, from small facilities with a few cameras to large cities with a network of hundreds or thousands of surveillance devices.

* **Small-Scale Deployment**: For small businesses or facilities, the system can be set up on a single server with limited cameras and monitoring stations.
* **Medium-Scale Deployment**: For larger facilities or multi-site installations, the system can be distributed across several servers, with centralized or cloud-based data processing and analytics.
* **Large-Scale Deployment**: For cities or public safety monitoring, the system can scale to support thousands of cameras and other devices, leveraging cloud-based infrastructures and distributed computing to handle high traffic and large datasets.

2.4.5 Network Security and Compliance

The system must ensure that all data and communications are secured to protect user privacy and meet regulatory compliance. Key network security protocols include:

* **Firewall Protection**: To secure communication between components, a firewall and intrusion detection/prevention system (IDS/IPS) should be in place.
* **Data Privacy Compliance**: The system should comply with relevant data protection regulations, including GDPR, CCPA, and other regional privacy laws. This includes securing personal data and ensuring that user data is processed only for legitimate security purposes.
* **Audit Logs**: Comprehensive logging of all user actions, system events, and data access must be enabled to maintain an audit trail for compliance and security monitoring.

## **2.5 Design and Implementation Constraints**

The **AI Smart Behavior Analysis** system is subject to several constraints that impact its design, implementation, and operation. These constraints are related to technology, regulatory requirements, hardware limitations, system performance, and user interface considerations. The following are the primary design and implementation constraints:

2.5.1 Technology Constraints

* **Machine Learning Model Limitations**:
  + The system relies heavily on machine learning algorithms for behavior analysis, weapon detection, and crime prediction. However, these models are constrained by the quality and quantity of training data available. False positives or missed detections may occur if the training data is not comprehensive enough to capture all possible behaviors and situations.
  + Continuous retraining and model updates are necessary to improve the accuracy of predictions, but these processes may be limited by available computational resources and time.
* **Video Resolution and Processing Power**:
  + The system’s ability to detect and analyze suspicious behavior is directly dependent on the resolution of the video feed. High-definition (HD) cameras are required for accurate recognition and analysis, but processing high-resolution video in real-time places significant demands on system resources, including GPU and CPU power.
  + A trade-off must be made between video quality, the number of cameras in use, and available processing power, especially in large-scale installations.
* **Real-Time Processing**:
  + The system requires real-time processing of video feeds and data to detect suspicious behavior as it occurs. This imposes limitations on the complexity of the machine learning models and the algorithms used. For real-time performance, models must be optimized for speed, which may limit their depth and predictive power.
  + The system may be constrained by network latency when processing video feeds remotely or in cloud-based infrastructures. Low-latency communication protocols are required to ensure real-time decision-making.

2.5.2 Hardware Constraints

* **Camera Compatibility**:
  + The system needs to interface with a wide range of surveillance cameras. The cameras must support industry-standard video protocols (e.g., ONVIF) for integration. However, older or non-standard cameras may not be compatible with the system, which could require the use of proprietary adapters or even limit the system’s effectiveness.
* **Server Hardware Requirements**:
  + High-performance servers with GPUs are required to handle real-time video analytics and machine learning processes. These hardware requirements may be cost-prohibitive for smaller installations, leading to scalability challenges.
  + In some environments, physical space or power limitations may prevent the installation of high-end server infrastructure. In such cases, the system may need to rely on distributed cloud-based solutions, which introduce additional concerns around latency, data security, and network reliability.
* **Battery and Power Limitations**:
  + The system’s hardware components (e.g., cameras, sensors) must operate continuously, requiring a stable power supply. In remote locations or outdoor environments, power constraints may limit system deployment. Backup power systems (e.g., UPS or solar) may be needed to ensure continuous operation, which could increase the system’s cost and complexity.

2.5.3 Security Constraints

* **Data Privacy and Compliance**:
  + The system processes sensitive video and behavioral data, which could include personally identifiable information (PII). As such, the system must comply with data privacy regulations such as GDPR, CCPA, and other applicable laws. Data encryption, anonymization, and secure access controls must be implemented to ensure compliance.
  + Video data should be retained only for as long as necessary and deleted in compliance with relevant regulations. However, storage limitations and compliance deadlines may impact how long data can be retained and how often the system can be updated or retrained.
* **Cybersecurity Risks**:
  + The system must be secured against potential cybersecurity threats, such as hacking, data breaches, or denial-of-service (DoS) attacks. Strong authentication mechanisms (e.g., multi-factor authentication) must be employed to prevent unauthorized access to the system.
  + External network communication (e.g., video streaming, data transmission) must be encrypted to prevent interception or manipulation of sensitive data.

2.5.4 User Interface and Accessibility Constraints

* **Interface Usability**:
  + The user interface (UI) must be designed to be intuitive for different user classes, from security personnel to law enforcement officers and system administrators. However, the complexity of behavior analysis and machine learning outputs may result in a steep learning curve for non-technical users.
  + Visualization of detected threats or abnormal behaviors must be clear and actionable. However, displaying real-time video alongside prediction analytics and alerts could overwhelm users, especially in high-volume environments. A balance between detail and simplicity is needed.
* **Device Compatibility**:
  + The system’s user interface must be compatible with a range of devices, including desktops, laptops, and mobile devices. However, different operating systems, screen sizes, and device capabilities (e.g., network bandwidth or processing power) may impact how the system's UI performs.
  + Mobile and remote access to the system requires careful design to optimize performance and usability. Features like video feeds and alerts must be tailored to mobile interfaces to avoid performance issues or excessive data usage.

2.5.5 Network Constraints

* **Bandwidth and Latency**:
  + The AI Smart Behavior Analysis system relies on the transfer of large amounts of video and data over networks. In environments with limited network bandwidth or high latency, video streams may be delayed or compressed, potentially affecting the quality of behavior analysis or detection accuracy.
  + In remote locations, bandwidth constraints may require the use of edge computing devices to process data locally, reducing the reliance on cloud infrastructure and minimizing latency.
* **Scalability**:
  + The system’s architecture must support scalability to accommodate different deployment sizes, from small installations to city-wide surveillance systems. However, the system’s design must consider how to balance performance and cost-efficiency as it scales.
  + For larger-scale deployments, distributed systems may be necessary to handle the computational load, introducing complexities in terms of synchronization, data consistency, and fault tolerance.

2.5.6 Legal and Ethical Constraints

* **Ethical Use of AI**:
  + The system’s AI and machine learning algorithms must be designed in a way that minimizes bias and ensures fair treatment of individuals. For example, detection algorithms should be sensitive to cultural and contextual differences to avoid false positives that could disproportionately affect specific groups.
  + Transparency in decision-making and system outputs is essential to ensure trust in the technology. Users should be able to understand why certain behavior patterns were flagged or why a particular prediction was made, especially in high-stakes environments like law enforcement.
* **Regulatory Compliance**:
  + The system must comply with local and international laws related to surveillance, data collection, and privacy. Different jurisdictions may have varying requirements for the retention of video data, notification of surveillance, and handling of personal data, which could limit how the system is deployed or operated.
  + Consent management mechanisms should be implemented to ensure that individuals being surveilled are informed of the monitoring and can exercise their rights to access, correct, or delete their data where applicable.

## **2.6 User Documentation**

The **AI Smart Behavior Analysis** system is designed to be an intuitive and powerful tool for security personnel, law enforcement, system administrators, and facility managers. This documentation provides detailed instructions on how to use the system, from basic operations to more advanced features.

2.6.1 Getting Started

2.6.2 System Requirements

Before using the **AI Smart Behavior Analysis** system, ensure that the following system requirements are met:

* **Hardware Requirements**:
  + High-definition surveillance cameras with at least 1080p resolution.
  + Computers or mobile devices with internet access for viewing live video feeds and alerts.
  + Servers with sufficient computational power (CPU, GPU) for real-time video processing.
* **Software Requirements**:
  + Windows, macOS, or Linux operating system for desktop users.
  + iOS or Android for mobile app users.
  + Web browser (e.g., Google Chrome, Mozilla Firefox, Safari) for accessing the user interface.

2.6.3 Logging In

To access the system, follow these steps:

1. **Open the Application**: Open the **AI Smart Behavior Analysis** application on your desktop or mobile device, or visit the web portal URL.
2. **Enter Credentials**: Input your username and password. If you are using multi-factor authentication, enter the additional code sent to your device.
3. **Dashboard**: After logging in, you will be redirected to the system’s main dashboard, where you can view real-time alerts, video feeds, and system status.

2.6.4 User Interface Overview

2.6.5 Dashboard

The dashboard provides an overview of the system’s current status and recent activities. Key components of the dashboard include:

* **Live Video Feed**: Displays real-time video from connected cameras.
* **Alerts Panel**: Shows any ongoing or recent alerts for suspicious behavior, crime prediction, weapon detection, or robbery events.
* **Threat Level Indicator**: A visual gauge showing the severity of current threats (e.g., low, medium, high).
* **System Health**: Displays the status of the system, including camera connectivity and data processing performance.

2.6.6 Alerts and Notifications

Alerts notify you of any detected anomalies or threats in real time. These could include suspicious behavior, weapon detection, or the occurrence of a robbery. You can take actions based on these alerts:

1. **View Alert Details**: Click on any alert to view detailed information, including a video clip of the event, the behavior detected, and any predictions made by the system.
2. **Set Alert Preferences**: Adjust the system’s alerting thresholds or specify which behaviors or threats you wish to receive notifications about. This can be configured from the “Settings” menu.
3. **Acknowledge/Resolve Alerts**: Once an alert has been reviewed, you can acknowledge it to indicate that action has been taken. Alerts may be resolved or escalated depending on the severity.

2.6.7 Behavior Analysis and Video Playback

The **AI Smart Behavior Analysis** system continuously analyzes video feeds for unusual behavior. To review detected behavior:

1. **Select Video Feed**: From the dashboard, select a camera feed to view the live stream or recorded video footage.
2. **Playback Controls**: Use the playback controls to pause, fast-forward, rewind, or step through the video in slow motion.
3. **Behavior Insights**: Click on specific segments of the video to view system annotations indicating detected behavior, such as “Suspicious movement” or “Weapon detected.”
4. **Export Video**: You can export video clips or screenshots for further investigation or evidence purposes. This can be done by clicking the "Export" button.

2.6.8 Weapon Detection

The system identifies visible weapons in real time. To review weapon detection events:

1. **Weapon Detection Alerts**: These will appear in the alerts panel with an associated visual indicator (e.g., weapon icon).
2. **Review Weapon Detection**: Click on the alert to view a detailed breakdown of the detected weapon, including the type (e.g., gun, knife) and location.
3. **Actionable Information**: The system may provide a recommendation, such as contacting law enforcement, based on the severity and nature of the weapon detected.

2.6.9 System Configuration and Settings

2.6.10 Adjusting Detection Parameters

The system’s sensitivity and detection criteria can be adjusted to better fit your environment:

1. **Navigate to Settings**: From the main menu, select “System Settings.”
2. **Adjust Sensitivity**: You can fine-tune the system’s sensitivity to different behaviors, such as lowering the threshold for suspicious activity in high-traffic areas.
3. **Configure Behavior Models**: If your system allows custom behavior models, you can update these models or upload new training data to improve accuracy.

2.6.11 Integration with External Systems

If your installation includes integration with other systems (e.g., alarms, access control), you can configure these from the **Integration Settings**:

1. **Configure Integrations**: Link the AI system with third-party security systems (e.g., automated door locks, alarm triggers).
2. **Set Response Triggers**: Define actions to be taken automatically when certain behaviors or threats are detected (e.g., trigger alarm if a weapon is detected).

2.6.12 Troubleshooting

2.6.13 Common Issues

* **Issue**: "Video feed is not displaying."
  + **Solution**: Ensure the camera is properly connected to the system and that the network connection is stable. Restart the camera or server if necessary.
* **Issue**: "Alert notifications are delayed."
  + **Solution**: Check network bandwidth and latency. Ensure that the system’s processing capabilities meet the demand for real-time analysis.

2.6.14 System Performance Issues

* If the system is lagging or not responding, check server performance and resource utilization. You may need to optimize the machine learning models or upgrade hardware for better performance.

2.6.15 Support

For further assistance, contact your system administrator or customer support. You can also refer to the **FAQ** section of the help portal for additional guidance.

2.6.16 Glossary of Terms

* **AI (Artificial Intelligence)**: The use of machine learning algorithms to identify patterns and behaviors in video feeds.
* **Behavior Analysis**: The process of analyzing human movement, gestures, and body language to detect suspicious activity.
* **Weapon Detection**: The identification of visible weapons such as guns or knives within the video feed.
* **Robbery Detection**: The identification of behaviors typically associated with a robbery, such as forced entry or rapid movement.
* **Alert Severity Levels**: The classification of alerts based on the perceived threat (e.g., Low, Medium, High).

## **2.7 Assumptions and Dependencies**

The following assumptions are made in the development, deployment, and use of the **AI Smart Behavior Analysis** system:

2.7.1 Assumptions about System Use

* **Constant Availability of Camera Feeds**: The system assumes that video feeds from surveillance cameras are consistently available for processing. If a camera is offline or experiencing connectivity issues, the system may not be able to detect or analyze behavior in that area.
* **Sufficient Data for Machine Learning**: The system assumes that there is sufficient and high-quality training data available for the machine learning models. This data should cover a wide range of behaviors, environments, and events to ensure accurate predictions and detection of anomalies.
* **User Training and Familiarity**: It is assumed that users will have basic training or familiarity with how the system works. While the interface is designed to be intuitive, users are expected to understand basic concepts of behavior analysis, alert management, and video playback.
* **Real-Time Network Connectivity**: The system assumes that a reliable and stable network connection is in place for streaming video and transmitting data. A high-bandwidth, low-latency connection is essential for real-time operation.
* **Security Clearance for Data Access**: It is assumed that only authorized personnel have access to sensitive data, including video feeds and analysis results. The system will rely on secure authentication and authorization to ensure data privacy.
* **Compliance with Local Laws**: The system assumes that the deployment complies with local and international laws related to surveillance, data privacy, and AI ethics. This includes the use of video data for security purposes, as well as compliance with regulations such as GDPR and CCPA.
* **Accuracy of Detection Models**: It is assumed that the system's machine learning models, including those for behavior analysis, weapon detection, and robbery detection, will perform accurately and consistently. While the system is designed to minimize false positives and negatives, some errors may still occur due to the complexity of human behavior.

2.7.2 Assumptions about Hardware

* **Compatibility with Common Camera Models**: The system assumes compatibility with widely available IP-based surveillance cameras. Cameras must support common protocols like ONVIF to enable seamless integration.
* **Adequate Computational Resources**: The system assumes that sufficient computational resources (e.g., high-performance servers, GPUs) will be available for real-time video analysis and machine learning model inference. For large-scale deployments, additional hardware or cloud resources may be required.

2.7.3 Assumptions about Environmental Conditions

* **Adequate Lighting for Cameras**: The system assumes that cameras are installed in areas with adequate lighting conditions, or that cameras with low-light or infrared capabilities are used to ensure visibility in dark environments.
* **Stable Power Supply**: It is assumed that a stable power supply is available for cameras, servers, and other hardware components. In cases of power failure, backup power systems (e.g., UPS or generators) may be required.

2.7.4 Dependencies

The **AI Smart Behavior Analysis** system depends on several external factors, technologies, and services to operate effectively:

2.7.5 External System Dependencies

* **Surveillance Cameras**: The system depends on external cameras to provide real-time video feeds. Cameras must be compatible with the system and support industry-standard protocols (e.g., ONVIF, RTSP). The system also depends on the cameras’ resolution, frame rate, and other specifications to ensure high-quality video for analysis.
* **Internet and Network Infrastructure**: The system requires internet or local network connectivity to transmit video feeds, access cloud-based services, and send alerts. Network infrastructure must support high-bandwidth, low-latency communication for real-time analysis. Any issues with network availability or bandwidth can impact the system’s performance.
* **Cloud Storage/Server Infrastructure**: If the system utilizes cloud services for storage or data processing, it is dependent on external cloud providers (e.g., Amazon Web Services, Microsoft Azure, Google Cloud) for infrastructure. This includes storing video data, processing machine learning models, and serving web-based applications.
* **Third-Party Security Systems**: In some installations, the system may depend on third-party security devices, such as access control systems, alarms, and locks, for triggering automated responses (e.g., locking doors, activating alarms). Integration with these systems must be seamless for the desired functionality.
* **External APIs and Integrations**: If the system integrates with external APIs (e.g., weather services, third-party analytics), the system’s functionality may depend on the availability and reliability of these services. Any changes to external APIs could impact the system's behavior.

2.7.6 Software Dependencies

* **Machine Learning Frameworks**: The system relies on external machine learning libraries and frameworks for behavior detection and analysis. These may include libraries such as TensorFlow, PyTorch, or OpenCV for image and video analysis. The correct version and compatibility of these frameworks are critical to the system’s performance.
* **Database Systems**: The system depends on relational (e.g., PostgreSQL, MySQL) and/or NoSQL (e.g., MongoDB, Elasticsearch) databases for storing structured and unstructured data, including video metadata, event logs, and user profiles. Database availability, performance, and integrity are key to the system’s functionality.
* **Web Servers and Application Servers**: The system depends on web servers (e.g., Nginx, Apache) and application servers (e.g., Flask, Node.js, Spring Boot) for hosting the user interface and providing access to the system’s features. The proper configuration and availability of these servers are critical for system uptime.

2.7.7 Legal and Regulatory Dependencies

* **Data Privacy and Security Laws**: The system must comply with data privacy laws and regulations governing the collection, storage, and processing of video data, such as GDPR, CCPA, or regional surveillance laws. The system’s design and operation may need to adapt depending on the legal requirements of the jurisdiction in which it is deployed.
* **Consent Management**: The system may depend on obtaining consent from individuals being monitored, particularly in regions with strict privacy regulations. The system should include mechanisms for obtaining, recording, and managing consent, depending on local laws.

2.7.8 Environmental Dependencies

* **Camera Installation and Placement**: The system’s ability to analyze behavior effectively depends on the proper installation and placement of cameras. The cameras must be positioned to cover key areas and avoid obstructions that could impact their field of view.
* **Lighting and Environmental Conditions**: The system depends on appropriate environmental conditions, including lighting, to perform accurate video analysis. Cameras must have the necessary features (e.g., infrared capability, low-light sensitivity) to work effectively in varying lighting conditions, especially in outdoor or poorly lit areas.

Summary of Assumptions and Dependencies:

* **Assumptions**:
  1. Reliable camera feeds are available for analysis.
  2. The system has access to sufficient data and computing power for machine learning.
  3. Users are trained and familiar with the system.
  4. Compliance with relevant security, legal, and ethical regulations.
  5. Stable power and environmental conditions for hardware operation.
* **Dependencies**:
  1. Dependent on compatible surveillance cameras, network infrastructure, and cloud storage for functionality.
  2. Relies on third-party security systems for integration.
  3. Requires external machine learning frameworks and databases.
  4. Must comply with legal and regulatory data protection requirements.
  5. Dependent on proper camera installation, environmental conditions, and lighting for accurate behavior analysis.

# **3. External Interface Requirements**

## **3.1 User Interfaces**

The **AI Smart Behavior Analysis** system provides several types of user interfaces, each catering to different roles within the system:

3.1.1 Security Personnel Interface

* **Real-Time Alerts**: A dashboard that displays incoming alerts based on behavior analysis, weapon detection, or robbery events.
* **Video Stream Access**: Security personnel can view live video feeds and navigate through historical video data.
* **Alert Management**: The interface allows security personnel to acknowledge or escalate alerts, and access relevant details on detected events.

3.1.2 System Admin Interface

* **User Management**: Admin users can manage user accounts, set permissions, and configure system settings.
* **System Health and Logs**: Admins can monitor system performance, review system logs, and perform maintenance tasks.
* **Report Generation**: The system provides tools for generating detailed reports on detected events and system performance.

3.1.3 Mobile Interface (for remote users)

* **Real-Time Push Notifications**: Alerts are pushed to mobile devices, allowing for instant notification of critical events.
* **Remote Access to Video Feeds**: Mobile users can access live video streams and playback historical data remotely.
* **Alert Response**: Users can acknowledge, resolve, or escalate alerts from their mobile device.

## **3.2 Hardware Interfaces**

The **AI Smart Behavior Analysis** system relies on several hardware components to function effectively. These components include surveillance cameras, servers, and storage devices. The system interfaces with the following hardware:

3.2.1 Surveillance Cameras

* **Camera Connectivity**: The system interfaces with IP-based surveillance cameras using industry-standard protocols, such as ONVIF, RTSP (Real-Time Streaming Protocol), or proprietary protocols depending on the camera manufacturer.
* **Resolution**: The system requires high-definition cameras capable of at least 1080p resolution to perform accurate analysis of behavior and weapon detection. In environments requiring more detail, 4K resolution cameras may be necessary.
* **Frame Rate**: Cameras should support a minimum of 30 frames per second (FPS) for smooth video streaming. Higher frame rates (e.g., 60 FPS) may be required for environments with fast-moving subjects.
* **Environmental Considerations**: Cameras should support both day and night operation, including low-light sensitivity or infrared capabilities for nighttime surveillance.

3.2.2 Server Infrastructure

* **Server Connectivity**: The system interfaces with local servers or cloud-based servers for processing and analyzing video feeds. The server infrastructure must support high-performance CPUs and GPUs for real-time video analysis and machine learning model inference.
* **Storage**: The system must interface with local or cloud storage for the retention of video data, logs, and other relevant information. The storage system must support fast read/write operations and have sufficient capacity to store high-resolution video for extended periods.
* **Backup Power**: In case of power failure, the system requires a backup power solution, such as Uninterruptible Power Supply (UPS) or battery backup for critical hardware (servers, cameras).

## **3.3 Software Interfaces**

The **AI Smart Behavior Analysis** system may interface with various software components, including machine learning frameworks, third-party applications, and database systems. Key software interfaces include:

3.3.1 Machine Learning Frameworks

* **Interface with TensorFlow, PyTorch, or other ML frameworks**: The system uses external machine learning frameworks to process and analyze video data. The interface with these frameworks includes:
  + Model Loading: The system must be able to load pre-trained models or custom models for behavior analysis and anomaly detection.
  + Inference: The system must send video frames to the ML models for inference and receive results (e.g., identified behaviors, detected weapons, robbery predictions).
  + Retraining: The system should have the ability to upload new data for retraining machine learning models.

3.3.2 Video Streaming and Processing Software

* **Video Stream Input**: The system interfaces with video streaming software that connects to surveillance cameras. The software should support video codecs like H.264 or H.265 for efficient transmission.
* **Video Processing Library**: The system integrates with video processing libraries, such as OpenCV, to process incoming video streams, extract frames, and perform initial analysis before sending the frames to the machine learning model for deeper analysis.

3.3.3 Database Management Systems

* **Database Interface**: The system interfaces with relational and/or NoSQL databases to store user information, camera metadata, event logs, alert histories, and system configurations. This may include:
  + SQL Databases: (e.g., PostgreSQL, MySQL) for structured data storage, such as user accounts, settings, and event logs.
  + NoSQL Databases: (e.g., MongoDB, Elasticsearch) for storing unstructured data, such as video metadata, alerts, and logs of detected behavior.

3.3.4 Third-Party Software Integrations

* **Security and Access Control Systems**: The system may interface with third-party security systems such as access control, alarm, and door-locking systems. This integration allows the system to trigger actions (e.g., locking doors, setting off alarms) when suspicious behavior or threats are detected.
* **Law Enforcement or Emergency Services Integration**: In case of high-severity events like a robbery or weapon detection, the system can be configured to notify or directly integrate with law enforcement agencies or emergency services, sending them alerts and real-time video feeds.

3.3.5 User Interface Software

* **Web Interface**: The system provides a web-based interface that allows users to interact with the system. The web interface should be compatible with common browsers (e.g., Chrome, Firefox, Safari) and provide real-time data on detected behaviors, alerts, and video streams.
* **Mobile Interface**: The system also provides a mobile app for iOS and Android devices. The mobile interface should allow users to view live video feeds, receive alerts, and interact with the system remotely.
* **Admin Panel**: The admin interface should provide user management features, system configuration settings, and logs, and allow for detailed analytics and reporting.

9.3 Communication Protocols

## **3.4 Communications Interfaces**

The **AI Smart Behavior Analysis** system uses various communication protocols to interface with external systems, devices, and services:

3.4.1 Video Streaming Protocols

* **RTSP (Real-Time Streaming Protocol)**: Used for streaming live video from cameras to the system for analysis. The system must support receiving video streams in this protocol for integration with IP cameras.
* **ONVIF (Open Network Video Interface Forum)**: A standard for connecting IP-based security devices, such as cameras, to the system. It ensures compatibility with a wide range of surveillance hardware.
* **H.264 or H.265**: Video codecs used for compressing video data transmitted from cameras to the system.

3.4.2 Data Transmission Protocols

* **HTTPS (Hypertext Transfer Protocol Secure)**: Used for secure web-based communication between the user interface and the backend system. Ensures encrypted transmission of sensitive data, including video streams, alerts, and user credentials.
* **MQTT or WebSockets**: Protocols used for real-time messaging and alerts. The system may use MQTT or WebSockets to push alerts and notifications to users in real time.
* **RESTful API**: The system exposes RESTful APIs for integration with other third-party systems or applications. These APIs may be used for pulling event data, video analysis results, and system statuses.

3.4.3 Database Communication

* **SQL (Structured Query Language)**: The system interfaces with relational databases (e.g., PostgreSQL, MySQL) using SQL to perform CRUD operations (Create, Read, Update, Delete) on structured data, including user information and event logs.
* **NoSQL**: If using NoSQL databases (e.g., MongoDB, Elasticsearch), the system interfaces with the database using specific query languages (e.g., MongoDB Query Language) to retrieve and store unstructured data like video metadata and alerts.

# **4. System Features**

The **AI Smart Behavior Analysis** system is designed to provide real-time surveillance, behavior analysis, and threat detection through advanced AI algorithms. The following system features describe the core functionalities available to users, including security personnel, system administrators, and law enforcement agencies.

4.1 Real-Time Behavior Analysis

**Description**:  
The **AI Smart Behavior Analysis** system continuously analyzes video feeds in real-time to identify and classify human behaviors. This feature uses machine learning models trained to detect various types of suspicious or abnormal behavior.

**Key Functions**:

* **Suspicious Movement Detection**: Identifies and flags unusual movement patterns, such as people loitering in a restricted area or walking in unusual directions.
* **Crowd Behavior Monitoring**: Detects potential crowd-related incidents, such as overcrowding or dangerous group movements, which may indicate a riot or escalation of conflict.
* **Abnormal Behavior Alerts**: Sends alerts when the system detects abnormal behaviors that deviate from normal patterns, such as running, sudden jerky movements, or aggressive gestures.

**User Actions**:

* View video feed with behavior annotations in real-time.
* Receive notifications of detected suspicious behaviors.
* Review historical data for flagged behavior patterns.

4.2 Weapon Detection

**Description**:  
The system uses advanced object detection algorithms to identify weapons (such as firearms, knives, or blunt objects) within the video feed, providing a real-time alert if a weapon is detected.

**Key Functions**:

* **Weapon Recognition**: Detects visible weapons in real-time based on shape, size, and motion, including guns, knives, and other dangerous objects.
* **Weapon Location Detection**: Provides location-based information on where the weapon is being carried or brandished, helping security teams respond more efficiently.
* **Automatic Alerting**: Sends immediate alerts to security personnel and law enforcement if a weapon is detected, with visual evidence attached.

**User Actions**:

* View a live alert with a snapshot of the detected weapon.
* Access historical footage to review the context in which a weapon was detected.
* Respond to alerts by escalating the event to law enforcement or activating safety protocols.

4.3 Robbery Detection

**Description**:  
The system is capable of identifying behaviors commonly associated with robberies, such as forced entry, rapid movement, or confrontational gestures. It can predict the likelihood of a robbery based on real-time behavioral analysis.

**Key Functions**:

* **Forced Entry Detection**: Detects when an individual attempts to break into a building or area by force, including actions such as smashing windows, breaking locks, or unauthorized entry.
* **Aggressive or Confrontational Behavior**: Identifies behaviors that typically accompany robberies, such as people threatening or physically confronting others.
* **Robbery Prediction**: Using historical data and real-time analysis, the system predicts possible robbery events based on suspicious behavior patterns, such as people congregating in an unusual manner or carrying large bags.
* **Alert and Video Evidence**: Sends an alert with visual evidence of the robbery attempt or ongoing robbery, allowing security personnel to respond immediately.

**User Actions**:

* Review historical data and analyze flagged behaviors.
* Access real-time alerts with video evidence when a robbery is detected or predicted.
* Escalate the alert to law enforcement or trigger facility-wide security measures (e.g., alarm, lock doors).

4.4 Incident Alerting and Notification

**Description**:  
The system includes an advanced alerting and notification mechanism to immediately notify users of detected unusual behavior, weapons, or robbery events. Alerts can be sent via the system dashboard, email, SMS, or mobile push notifications.

**Key Functions**:

* **Real-Time Notifications**: Security personnel, administrators, and law enforcement can receive real-time alerts via the system interface, email, SMS, or mobile app.
* **Alert Categories**: Alerts are categorized based on severity (e.g., low, medium, high) and type (e.g., suspicious activity, weapon detection, robbery).
* **Multilingual Support**: Alerts can be configured to display in multiple languages to support a diverse user base.
* **Location-Based Alerts**: Alerts can be tied to specific camera locations, helping users quickly pinpoint areas of concern.

**User Actions**:

* Acknowledge or escalate alerts based on severity and type.
* Review detailed alert information, including a timestamp, video evidence, and analysis data.
* Customize alert thresholds and notification preferences from the system settings.

4.5 Video Feed Monitoring and Playback

**Description**:  
The system provides a live video feed and playback feature, allowing users to monitor real-time surveillance and review recorded footage for behavior analysis or event investigation.

**Key Functions**:

* **Live Video Stream**: View live video feeds from connected cameras in real-time, with the option to zoom in and out or adjust the view for detailed monitoring.
* **Incident Review**: Search historical video footage based on time, date, and event type to review incidents flagged by the system.
* **Video Analytics**: Overlays on video footage show detected behaviors, such as “Suspicious movement” or “Weapon detected,” providing real-time context.
* **Export Video Clips**: Users can export specific video clips or screenshots for further analysis or reporting.

**User Actions**:

* Monitor live video feeds and watch for alerts or suspicious behaviors.
* Navigate through archived footage to investigate past events.
* Export clips for reporting or legal evidence.

4.6 User Management and Role-Based Access Control

**Description**:  
The system includes role-based access control (RBAC) to ensure that only authorized users have access to certain features and data. Administrators can manage user roles and permissions to tailor access to system resources based on user needs.

**Key Functions**:

* **Role Definition**: Define roles such as "Security Personnel," "System Administrator," "Law Enforcement," and "Guest," each with specific access levels to system functionality.
* **User Permissions**: Set permissions for each role to control access to video feeds, alerts, system settings, and reporting tools.
* **Audit Logs**: Track user actions and system changes to ensure accountability and detect potential security breaches.

**User Actions**:

* Administrators can create, edit, or delete user accounts.
* Assign users to specific roles with appropriate permissions for accessing data or taking actions.
* Monitor audit logs to review user activities and ensure compliance.

4.7 Reporting and Analytics

**Description**:  
The system offers comprehensive reporting and analytics capabilities, allowing users to generate detailed reports based on detected events, system activity, or performance metrics.

**Key Functions**:

* **Event Reports**: Generate reports detailing detected behaviors, weapons, or robberies within a selected time period.
* **System Performance Metrics**: Track system performance, such as video processing speed, alert accuracy, and system uptime.
* **Trend Analysis**: Perform trend analysis on behavior patterns, crime prediction, or weapon detection to identify recurring issues or potential areas of concern.
* **Customizable Reports**: Users can customize reports to include specific data points, date ranges, and system configurations.

**User Actions**:

* Generate and export event, performance, and trend analysis reports.
* Filter reports based on time, event type, camera location, or severity.
* Share reports with stakeholders or law enforcement for further investigation.

4.8 System Configuration and Settings

**Description**:  
The system includes configuration settings to customize its behavior and adapt to specific security environments. Users can modify settings related to detection parameters, alert preferences, video feed options, and system integrations.

**Key Functions**:

* **Detection Sensitivity**: Adjust the sensitivity of the system’s behavior analysis and weapon detection models to reduce false positives or increase detection accuracy in specific environments.
* **Alert Settings**: Configure alert thresholds, notification channels (email, SMS, mobile app), and escalation procedures for critical events.
* **Camera Integration**: Add or remove cameras from the system, configure camera parameters (e.g., frame rate, resolution), and assign cameras to specific areas or zones.
* **Data Retention Policy**: Set policies for how long video data and alert logs should be retained, ensuring compliance with data privacy regulations.

**User Actions**:

* Modify detection and alert settings based on the operational environment or specific security needs.
* Add new cameras or adjust settings for existing ones.
* Set data retention policies and configure storage options.

## **4.1.1 Description and Priority**

Each feature of the **AI Smart Behavior Analysis** system is critical to its overall functionality, but certain features may be more essential to core system operations than others. Below is a description and priority assignment for each feature of the system.

4.1.1.1 Real-Time Behavior Analysis

**Description**:  
The **Real-Time Behavior Analysis** feature continuously analyzes video feeds from surveillance cameras to detect suspicious or abnormal behavior in real-time. It helps to identify potential threats and reduce security risks by flagging unusual patterns, such as loitering, aggressive movements, or crowd-related incidents.

**Priority**:  
**High**  
This is a core feature of the system and is crucial for maintaining proactive surveillance. Real-time detection and alerting of abnormal behaviors are essential for the system’s functionality, ensuring that security personnel can respond quickly to potential threats.

4.1.1..2 Weapon Detection

**Description**:  
The **Weapon Detection** feature uses machine learning algorithms to identify visible weapons (guns, knives, etc.) in video streams. When a weapon is detected, the system generates immediate alerts, enabling a rapid security response to prevent violence or other harmful actions.

**Priority**:  
**High**  
Weapon detection is critical for public safety, making it a high-priority feature. It directly contributes to preventing violent incidents and helps ensure security in sensitive areas, such as airports, schools, and malls. Fast detection and alerting are essential for timely intervention.

4.1.1.3 Robbery Detection

**Description**:  
The **Robbery Detection** feature is designed to identify behaviors associated with robbery attempts, such as forced entry or confrontational actions. It also predicts potential robbery events by analyzing suspicious group movements or patterns. When a robbery is detected or predicted, the system alerts security personnel.

**Priority**:  
**Medium**  
While essential, robbery detection is a lower priority compared to real-time behavior and weapon detection. However, it is still highly important for preventing criminal activity in commercial or high-risk locations. Predictive capabilities and accurate identification of robbery behaviors improve overall security.

4.1.1.4 Incident Alerting and Notification

**Description**:  
The **Incident Alerting and Notification** feature sends real-time alerts to security personnel and relevant stakeholders when suspicious behavior, weapon presence, or robbery events are detected. Alerts are communicated through various channels, including push notifications, email, SMS, or direct system alerts.

**Priority**:  
**High**  
Incident alerting is a fundamental component of the system, as it ensures security teams can respond to detected threats without delay. Real-time notifications allow for immediate action to be taken, whether to escalate an incident or review surveillance footage.

4.1.1.5 Video Feed Monitoring and Playback

**Description**:  
This feature provides users with live video streams and access to recorded footage, allowing for both proactive monitoring and post-event review. It helps security personnel to observe real-time activities and investigate incidents that occurred in the past by reviewing historical video data.

**Priority**:  
**Medium**  
While essential for investigation and monitoring, video feed monitoring and playback are secondary to real-time detection and alerting. However, this feature is important for post-event analysis and providing evidence during investigations.

4.1.1.6 User Management and Role-Based Access Control

**Description**:  
The **User Management and Role-Based Access Control** feature enables administrators to define and manage user roles and permissions, ensuring that sensitive data and functionalities are only accessible to authorized personnel. This includes assigning roles, controlling access to video feeds, alert management, and system settings.

**Priority**:  
**High**  
User management and role-based access control are crucial for maintaining the security and integrity of the system. This feature ensures that only authorized users can access sensitive data and perform critical actions, preventing misuse and unauthorized access.

4.1.1.7 Reporting and Analytics

**Description**:  
The **Reporting and Analytics** feature allows users to generate detailed reports on detected events, system performance, and behavior analysis trends. It supports system audits, event investigations, and operational optimization by providing actionable insights into system operations and incidents.

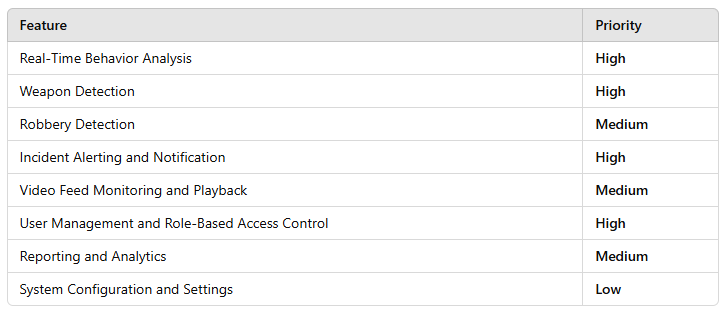
**Priority**:  
**Medium**  
Reporting and analytics are important for ongoing system optimization and compliance with security policies. However, this feature is secondary to real-time detection and alerting, as it primarily supports investigative tasks and system monitoring after the fact.

4.1.1.8 System Configuration and Settings

**Description**:  
The **System Configuration and Settings** feature provides administrators with the ability to configure system parameters, such as alert thresholds, video feed settings, detection sensitivities, and data retention policies. This ensures that the system is customized to meet the specific needs of each environment and that it complies with applicable regulations.

**Priority**:  
**Low**  
System configuration is important for tailoring the system to the specific operational environment, but it is not as time-sensitive as features like behavior analysis, weapon detection, and alerting. It is a secondary feature that can be adjusted during setup or maintenance rather than requiring constant attention.

Graphical Representation:



## **4.1.2 Stimulus/Response Sequences**

4.1.2.1 Stimulus: Detection of Suspicious Behavior

**Stimulus**:  
The system detects suspicious behavior, such as an individual loitering in a restricted area or exhibiting erratic movement (e.g., running, sudden stops).

**Response**:

1. The system analyzes the video feed using machine learning algorithms to classify the behavior as suspicious.
2. The system triggers a **real-time alert** to the **Security Personnel** interface, including a snapshot or video frame of the suspicious behavior.
3. The **alert** is categorized as “Suspicious Behavior” and includes details such as the location, time, and a confidence score of the detection.
4. The system logs the event in the database for future reference and potential follow-up analysis.
5. The **Security Personnel** receive a push notification on their mobile device, if configured.
6. The **Security Personnel** can choose to acknowledge, dismiss, or escalate the alert.

4.1.2.2 Stimulus: Detection of Weapon

**Stimulus**:  
The system detects the presence of a weapon (e.g., firearm, knife, blunt object) in the video feed using object detection algorithms.

**Response**:

1. The system analyzes the video feed and confirms the presence of a weapon based on visual cues such as shape, size, and motion.
2. The system triggers a **high-severity alert** to **Security Personnel**, with a detailed notification indicating the weapon type (e.g., "Firearm detected").
3. The **alert** includes a snapshot or video frame highlighting the weapon’s location.
4. The system logs the detection event in the database, noting the exact time and location.
5. A **real-time push notification** is sent to **Security Personnel**’s mobile app, or an SMS is sent to designated security staff.
6. If the system is integrated with law enforcement or emergency services, the system sends an automated notification with relevant data (video feed, weapon location, etc.).
7. The **Security Personnel** review the alert and video feed, choosing to either acknowledge the situation, trigger an emergency protocol, or escalate to law enforcement.

4.1.2.3 Stimulus: Detection of Robbery (Forced Entry or Aggressive Behavior)

**Stimulus**:  
The system detects behaviors typically associated with a robbery, such as forced entry into a building, aggressive physical confrontations, or individuals displaying robbery-related actions (e.g., masked individuals).

**Response**:

1. The system analyzes the video feed and classifies the detected behavior as "potential robbery," based on predefined patterns for forced entry or aggressive behavior.
2. A **robbery-related alert** is triggered, categorized as a “High-Severity Event.”
3. The **alert** includes video footage or an image of the event, timestamp, and location details.
4. The system sends an alert to the **Security Personnel** dashboard, along with a **push notification** to their mobile devices.
5. The system logs the event with detailed metadata in the database for further investigation.
6. The system may initiate automatic safety protocols, such as locking doors or triggering alarms, if integrated with local security systems.
7. **Security Personnel** can acknowledge, dismiss, or escalate the alert. If escalation is chosen, the system forwards the event to law enforcement or emergency services.
8. In case of a severe event (e.g., active robbery), the system may initiate a direct communication line with local law enforcement or call emergency services.

## **4.1.3 Functional Requirements**

The **AI Smart Behavior Analysis** system is designed to detect abnormal or suspicious behavior, predict criminal activities such as robberies, detect weapons, and send appropriate alerts to security personnel. The following functional requirements describe the essential features and behavior of the system.

4.1.3.1 Behavior Detection

4.1.3.2 Suspicious Behavior Detection

* **Description**: The system must be capable of detecting abnormal human behaviors, such as loitering, running, erratic movement, and other actions that may indicate suspicious activity.
* **Functional Requirement**:
  + The system shall continuously monitor live video feeds for behavior patterns.
  + The system shall analyze detected behaviors and flag abnormal actions based on predefined thresholds for suspicious behavior.
  + The system shall send real-time alerts to security personnel when suspicious behavior is detected.
  + The system shall categorize suspicious behavior and assign a severity level (low, medium, high).
  + The system shall record suspicious behavior events with timestamp and location.

4.1.4 Weapon Detection

4.1.3.1 Detection of Visible Weapons

* **Description**: The system must be able to detect the presence of weapons such as firearms, knives, or blunt objects in real-time.
* **Functional Requirement**:
  + The system shall use machine learning and computer vision algorithms to detect weapons in the video feed.
  + The system shall classify the type of weapon detected (e.g., firearm, knife) and highlight it on the video feed.
  + The system shall trigger an alert if a weapon is detected, including the time, location, and type of weapon.
  + The system shall generate an immediate notification to security personnel (through the dashboard, mobile app, or SMS).
  + The system shall record the weapon detection event with timestamp, location, and associated video footage.

4.1.5 Robbery Detection

4.1.5.1 Detection of Forced Entry

* **Description**: The system must be able to detect forced entry into a building or restricted area, such as when doors or windows are smashed.
* **Functional Requirement**:
  + The system shall identify actions indicative of forced entry, including breaking windows, tampering with locks, or removing barriers.
  + The system shall flag forced entry events as high-severity alerts and notify security personnel.
  + The system shall display relevant video footage and timestamp of the forced entry event.
  + The system shall allow security personnel to review past forced entry events and related video footage.

4.1.5.2 Detection of Robbery-Related Behavior

* **Description**: The system must be able to identify behavior patterns typically associated with a robbery, such as aggressive confrontations or the presence of individuals with covered faces or unusual actions.
* **Functional Requirement**:
  + The system shall analyze behavior patterns to detect potential robbery activities based on predefined algorithms and machine learning models.
  + The system shall send real-time alerts to security personnel when robbery-related behavior is detected.
  + The system shall classify the severity of the robbery threat and provide a confidence score of detection.
  + The system shall store robbery-related events with relevant metadata (e.g., video footage, timestamp, location).

4.1.6 Incident Alerting and Notification

4.1.6.1 Real-Time Alert Generation

* **Description**: The system must generate real-time alerts for detected suspicious activities, weapon detections, or robbery-related events.
* **Functional Requirement**:
  + The system shall automatically trigger an alert when suspicious or abnormal behavior is detected, including weapon sightings or robbery attempts.
  + Alerts must include a description of the detected event (e.g., weapon detected, suspicious behavior), location, timestamp, and a video snapshot.
  + Alerts shall be sent via multiple communication channels, including the security dashboard, email, SMS, and mobile notifications.
  + The system shall categorize alerts by severity (e.g., low, medium, high) to help prioritize response actions.

4.1.7 Video Feed Monitoring and Playback

4.1.7.1 Live Video Feed Monitoring

* **Description**: The system must provide real-time live video feeds from connected surveillance cameras.
* **Functional Requirement**:
  + The system shall display video feeds from connected cameras in real-time.
  + The system shall allow users to zoom in and adjust the view to focus on specific areas of interest.
  + The system shall overlay behavior or event tags (e.g., “Suspicious behavior detected”) on the live video stream.
  + The system shall support multi-camera viewing, allowing users to monitor several locations simultaneously.

4.1.7.2 Video Playback and Search

* **Description**: The system must provide the ability to replay recorded video footage for analysis or investigation.
* **Functional Requirement**:
  + The system shall allow users to search video footage by date, time, event type, or camera location.
  + The system shall display video footage and relevant metadata for reviewed events.
  + The system shall allow users to export specific clips or images from the recorded video for reporting purposes.
  + The system shall allow users to tag events within the video footage for further analysis or follow-up.

# **5. Other Nonfunctional Requirements**

## **5.1 Performance Requirements**

5.1.1 Latency for Behavior Detection

* **Requirement**:  
  The system must process video feeds and detect suspicious behavior (e.g., loitering, running, aggressive movements) in **real-time** with a latency of **less than 2 seconds** from the moment the event is captured in the video feed.

5.1.2 Latency for Weapon Detection

* **Requirement**:  
  The system must detect the presence of a weapon in the video feed and trigger an alert within **1-3 seconds** of the weapon appearing in the frame.

5.1.3 Latency for Robbery Detection

* **Requirement**:  
  The system must identify robbery-related behavior (e.g., forced entry or aggressive confrontations) and generate a real-time alert with a latency of **no more than 5 seconds** from the moment the event is detected.

5.2.1 Accuracy and Detection Reliability

5.2.2 Detection Accuracy for Behavior Analysis

* **Requirement**:  
  The system must maintain a **minimum accuracy rate of 95%** for detecting suspicious behaviors such as loitering, running, or sudden stops, measured over a period of continuous operation.

5.2.3 Detection Accuracy for Weapon Detection

* **Requirement**:  
  The system must achieve an accuracy rate of **no less than 98%** for weapon detection, including firearms, knives, and blunt objects, across various environmental conditions and camera angles.

5.2.4 Detection Accuracy for Robbery Events

* **Requirement**:  
  The system must maintain a **minimum accuracy rate of 90%** for detecting robbery-related behaviors (e.g., forced entry, masked individuals), measured across a variety of incident types and scenarios.

5.3 Scalability

5.3.1 Number of Cameras Supported

* **Requirement**:  
  The system must be able to process video feeds from **up to 100 cameras simultaneously** without degradation in performance, provided sufficient network bandwidth is available.

5.3.2 System Load Handling

* **Requirement**:  
  The system should be capable of handling **up to 100 simultaneous user logins** without any significant delays in system response times or functionality. This includes users viewing video feeds, generating reports, or receiving alerts.

5.3.3 Distributed Processing

* **Requirement**:  
  The system must support **distributed processing** for video analysis, enabling horizontal scaling as the number of cameras or users increases. The system should be able to scale to accommodate **up to 1,000 cameras** without sacrificing analysis performance.

5.3.4 Availability and Reliability

5.3.4.1 System Uptime

* **Requirement**:  
  The system must provide a **99.9% uptime**, ensuring that the system is operational and available for use at all times, excluding scheduled maintenance periods.

5.3.4.2 Backup and Redundancy

* **Requirement**:  
  The system must have automatic **data backup mechanisms** in place to ensure that video footage and event logs are preserved in the event of a failure. Backup systems should ensure that no data is lost during unexpected outages or failures.

5.3.4.3 Recovery Time Objective (RTO)

* **Requirement**:  
  In the event of a system failure, the system must recover and return to full functionality within **15 minutes**, ensuring minimal disruption to security operations.

5.3.4.4 Recovery Point Objective (RPO)

* **Requirement**:  
  The system should ensure that data loss due to failure is limited to **no more than 15 minutes** of video footage or event logs.

## **5.2 Safety Requirements**

5.1.2 Operational Safety

5.1.2.1 System Failure Mechanisms

* **Requirement**:  
  In the event of a system failure (e.g., hardware or software malfunction), the system must automatically switch to a backup mode, maintaining minimal operational functionality. Critical functions, such as alerting security personnel about suspicious activities or weapons, must remain operational even in backup mode.
* **Safety Impact**:Ensures that security monitoring continues even during system downtime, preventing a gap in coverage that could result in unsafe situations.

15.1.2.2 Emergency Shutdown Procedure

* **Requirement**:  
  The system must include an emergency shutdown option that allows administrators or operators to quickly and safely disable certain functionalities, including video feeds or alerting systems, in the event of a security breach, data breach, or emergency.
* **Safety Impact**:This ensures that in emergency situations, security personnel can take manual control of the system and prevent false alerts or malicious interference.

5.1.3 Overheating and Hardware Safety

* **Requirement**:  
  The system must include overheating protection for hardware components (e.g., servers, cameras, or sensors). If any hardware component exceeds the safe operating temperature, the system must initiate automatic shutdown or throttle operations to prevent overheating damage.
* **Safety Impact**:Prevents damage to critical hardware components, ensuring the system remains operational and safe in various environmental conditions.

5.1.3.1 Cybersecurity and Data Protection

5.3.1.2 Secure Communication and Data Storage

* **Requirement**:  
  The system must use **end-to-end encryption (AES-256)** for all data in transit (e.g., video feeds, alerts) and at rest (e.g., event logs, stored video). Data must be stored in secure servers with restricted access to prevent unauthorized tampering or breach.
* **Safety Impact**:Protects the system from cybersecurity threats, ensuring that malicious actors cannot intercept or tamper with critical surveillance data.

## **5.3 Security Requirements**

The **AI Smart Behavior Analysis** system must ensure the highest level of security to protect sensitive data, maintain system integrity, and prevent unauthorized access or misuse. The following security requirements outline the key measures the system must adopt to safeguard its components, users, and data.

5.3.1 Authentication and Access Control

5.3.1.2 User Authentication

* **Requirement**:  
  The system must implement **strong authentication mechanisms** to ensure that only authorized users can access the system. This should include the following:
  + Use of **multi-factor authentication (MFA)** for all user logins, requiring at least two of the following: a password, a one-time PIN (sent via SMS or email), or a biometric factor (e.g., fingerprint or face recognition).
  + Support for **role-based access control (RBAC)**, ensuring that users only have access to features and data relevant to their role.
* **Security Impact**:Prevents unauthorized access by ensuring that only authenticated users with appropriate permissions can interact with the system.

5.3.1.3 Session Management

* **Requirement**:  
  The system must enforce **secure session management**, including:
  + Automatic session timeout after **15 minutes** of inactivity, requiring users to re-authenticate.
  + Secure session cookies with **HTTPOnly** and **Secure** flags to prevent session hijacking.
  + Preventing session fixation attacks by issuing a new session ID after login.
* **Security Impact**:Reduces the risk of unauthorized access through stolen or abandoned sessions.

5.3.1.4 Data Protection and Privacy

5.3.1.5 Data Encryption

* **Requirement**:  
  All sensitive data, including video feeds, event logs, and user information, must be **encrypted** using **AES-256 encryption** both during transmission (in transit) and when stored (at rest).
  + Video footage must be encrypted to prevent unauthorized viewing or tampering.
  + Event logs, including alerts, user actions, and system status, must also be encrypted.
* **Security Impact**: Ensures data confidentiality and integrity, preventing unauthorized access to sensitive information.

5.3.1.6 Data Minimization

* **Requirement**:  
  The system must adhere to **data minimization principles**, ensuring that only necessary data is collected, stored, and processed. For example:
  + Video footage should be stored only as long as necessary for security or regulatory purposes (e.g., 30 days), after which it must be securely deleted or archived.
  + Personal data (e.g., facial recognition data, user login data) must be anonymized or pseudonymized whenever possible.
* **Security Impact**: Limits the exposure of sensitive data to unauthorized access and reduces the risk of data breaches.

## **5.4 Software Quality Attributes**

<Specify any additional quality characteristics for the product that will be important to either the customers or the developers. Some to consider are adaptability, availability, correctness, flexibility, interoperability, maintainability, portability, reliability, reusability, robustness, testability, and usability. Write these to be specific, quantitative, and verifiable when possible. At the least, clarify the relative preferences for various attributes, such as ease of use over ease of learning.>

## **5.5 Business Rules**

<List any operating principles about the product, such as which individuals or roles can perform which functions under specific circumstances. These are not functional requirements in themselves, but they may imply certain functional requirements to enforce the rules.>

# **References**

<List any other documents or Web addresses to which this SRS refers. These may include user interface style guides, contracts, standards, system requirements specifications, use case documents, or a vision and scope document. Provide enough information so that the reader could access a copy of each reference, including title, author, version number, date, and source or location.>