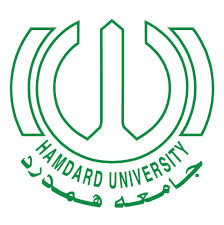
Hamdard University

Department of Computing

Final Year Project



**< INTEGRA GUARD SURVEILLANCE SYSTEM >**

**(<**FYP-022/FL24 **>)**

**Software Requirements Specifications**

Submitted by

Zainab Khalid (2326-2021)

Nida Aamir (2458-2021)

Supervisor

Mr.Afzal Hussain

Mr.Mustafa Ali

**Fall 2021**

**Document Sign off Sheet**

### **Document Information**

|  |  |
| --- | --- |
| **Project Title** | **INTEGRA GUARD SURVEILLANCE SYSTEM** |
| **Project Code** | FYP-022/FL24 |
| **Document Name** | Software Requirements Specifications |
| **Document Version** | <1.0> |
| **Document Identifier** | < FYP-022/FL24>-SRS |
| **Document Status** | Final |
| **Author(s)** | Zainab Khalid, Nida Aamir |
| **Approver(s)** | Afzal Hussain |
| **Issue Date** | <14-11-2024> |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Signature** | **Date** |
| Zainab Khalid | Team Lead |  | 24-Jan-2025 |
| Nida Aamir | Team Member 2 |  | 24-Jan-2025 |
| Mr.Afzal Hussain | Supervisor | Afzal Hussain | 24-Jan-2025 |
| Mr.Mustafa Ali | Co-Supervisor | Mustafa Ali | 24-Jan-2025 |
| Mr.Sulaiman Khan | Project Coordinator |  |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 5-11-2024 | 0.1 | First draft | Nida |
| 8-11-2024 | 0.2 | Recevised Version | Zainab |
|  |  |  |  |
|  |  |  |  |

**Definition of Terms, Acronyms, and Abbreviations**

*[This section should provide the definitions of all terms, acronyms, and abbreviations required to interpret the terms used in the document properly.]*

|  |  |
| --- | --- |
| **Term** | **Description** |
| ATM | Automated Teller Machine; enables banking transactions without human assistance. |
| AI | Artificial Intelligence; simulates human intelligence in machines. |
| CCTV | Closed-Circuit Television; used for real-time video surveillance. |
| UI | User Interface; the part of the system users interact with (e.g., dashboard) |
| Cloud Analysis | Uses cloud-based AI to analyze behavior patterns and enhance detection. |

# **Table of Contents**

[**1.** Introduction 8](#_Toc4677804)

[1.1 Purpose of Document 8](#_Toc4677805)

[1.2 Intended Audience 8](#_Toc4677806)

[1.3 Abbreviations 8](#_Toc4677807)

[**2.** Overall System Description 9](#_Toc4677808)

[2.1 Project Background 9](#_Toc4677809)

[2.2 Problem Statement 9](#_Toc4677810)

[2.3 Project Scope 9](#_Toc4677811)

[2.4 Not In Scope 9](#_Toc4677812)

[2.5 Project Objectives 9](#_Toc4677813)

[2.6 Stakeholders & Affected Groups 9](#_Toc4677814)

[2.7 Operating Environment 9](#_Toc4677815)

[2.8 System Constraints 9](#_Toc4677816)

[2.9 Assumptions & Dependencies 9](#_Toc4677817)

[**3.** External Interface Requirements 10](#_Toc4677818)

[3.1 Hardware Interfaces 10](#_Toc4677819)

[3.2 Software Interfaces 10](#_Toc4677820)

[3.3 Communications Interfaces 10](#_Toc4677821)

[**4.** System Functions / Functional Requirements 11](#_Toc4677822)

[4.1 System Functions 11](#_Toc4677823)

[4.2 Use Cases 12](#_Toc4677824)

[4.2.1 List of Actors 12](#_Toc4677825)

[4.2.2 List of Use Cases 12](#_Toc4677826)

[4.2.3 Use Case Diagram 13](#_Toc4677827)

[4.2.4 Description of Use Cases 13](#_Toc4677828)

[**5.** Non - Functional Requirements 16](#_Toc4677829)

[5.1 Performance Requirements 16](#_Toc4677830)

[5.2 Safety Requirements 16](#_Toc4677831)

[5.3 Security Requirements 16](#_Toc4677832)

[5.4 Reliability Requirements 16](#_Toc4677833)

[5.5 Usability Requirements 16](#_Toc4677834)

[5.6 Supportability Requirements 16](#_Toc4677835)

[5.7 User Documentation 16](#_Toc4677836)

[**6.** References 17](#_Toc4677837)

# **Introduction**

The Integra Guard Surveillance System is a comprehensive solution to address security challenges in ATM environments. The system focuses on identifying weapons to improve user safety and secure financial transactions by utilizing cutting-edge technologies like real-time video analysis and AI-powered detection. The system is built to proactively mitigate threats while guaranteeing regulatory compliance thanks to its intuitive interface, strong detection algorithms, and smooth integration capabilities. Rapid notification systems, encrypted data storage, and scalability to accommodate an increasing number of ATM installations are important features.

**1.1 Purpose of Document**

The Integra Guard Surveillance System was created using evolutionary prototyping, and this Software Requirements Specification (SRS) document offers comprehensive insights into its architecture, design considerations, and functionality. The technical requirements and specifications required for successful implementation are outlined in this document, which acts as a blueprint for the development team.

**1.2 Intended Audience**

• Development Team: Engineers and developers in charge of system design, implementation, and testing.

• Security analysts are experts who use the system's results to improve ATM surveillance.

• Project managers are in charge of the planning, carrying out, and completing phases of a project.

• Stakeholders: Anybody with an interest in the system's functionality and security, such as banks, law enforcement, and regulatory organizations.

# Overall System Description

**2.1 Project Background**

Important security issues in ATM environments are addressed by the Integra Guard Surveillance System. Existing security measures are insufficient in offering proactive solutions in light of the increase in occurrences involving concealed weapons and suspicious activity. This system seeks to improve response times and lessen dependency on manual surveillance by utilizing live CCTV feeds and incorporating AI-driven weapon

**2.2 Problem Statement**

Detecting concealed weapons and keeping an eye on questionable activities in real time are just two of the many difficulties ATM security faces. Current solutions mainly rely on manual monitoring and are reactive. To enable proactive reactions and guarantee client safety, a comprehensive and automated solution is required.

**2.3 Project Scope**

* + Real-time Surveillance: Use live video feeds to identify weaponry.
  + Integrated Alerts: Send out alerts using email to personnel.
  + Compliance Monitoring: Verify that privacy and financial laws are being followed.
  + Scalability: Allow for the low latency monitoring of several ATMs.

**2.4 Not in Scope**

* + Monitoring of private, non-ATM spaces.
  + Detection of fully concealed weapons.
  + Replacing manual audits or law enforcement investigations.
  + Detection of concealed or hidden weapons.
  + Facial expression or emotion recognition.Advanced AI features such as anomaly detection, audio threat detection, and crowd behavior
  + **2.5 Project Objectives**

To offer a proactive surveillance solution for ATM environments that uses automated detection and warnings to improve safety and speed up response times.

**2.6 Stakeholders & Affected Groups**

* + Bank Customers: Those who gain from increased security when using ATMs.
  + Law enforcement: Organizations that use alert data to take prompt action.
  + Bank Security Teams: End users keeping an eye on and responding to reported issues.
  + Regulators: Bodies evaluating system compliance with security standards.

**2.7 Operating Environment:**

Utilizing the dependability, scalability, and security of cloud platforms such as AWS or Azure, the Integra Guard Surveillance System will function in a cloudhosted environment. Web-based apps will be used to access the system, guaranteeing compatibility with various devices and operating systems. Linux servers will be used by the backend because of their strong security and performance, which enable scalable and effective data processing for real-time monitoring.

**2.8 System Constraints**

Limited to ATM locations; non-ATM contexts are not included.

• Budget: Some advanced features may not be able to be included due to a lack of funds.

• Technology: Relies on reliable internet access

• False Positives: The system may issue warnings for things or behaviors that are not dangerous, necessitating constant algorithmic improvement.

• Privacy Regulations: The ability to collect and retain data will be restricted in order to comply with data protection and privacy laws.

**2.9 Assumptions & Dependencies**

**Assumptions**

* + Access to CCTV footage is guaranteed for all monitored locations.
  + Stakeholders will provide necessary support for system deployment and integration.
  + The system will undergo periodic updates to enhance functionality and address emerging threats.

**Dependencies**

* Collaboration with law enforcement and banking teams to define response protocols.
* Availability of skilled AI developers and security analysts.
* Reliable infrastructure, including stable internet connections and cloud service uptime.
* Adherence to legal and regulatory frameworks for data security and surveillance.

# External Interface Requirements

**3.1 Hardware Interfaces**

The system requires standard CCTV cameras installed in ATMs for capturing video feeds. No additional hardware interfaces are needed, as the analysis is performed on the software side using these video inputs.

**3.2 Software Interfaces**

* AI Detection Framework:

**Owner:** Open-source AI framework (e.g., TensorFlow, PyTorch).

**Integration:** Integrated within the system for processing video feeds to detect weapons

**Usage:** Used for real-time object detection and behavioral analysis.

* Web-Based Dashboard:

**Owner**: Custom-built for the project.

**Integration**: Frontend and backend communication through APIs.

**Usage:** Provides monitoring personnel with real-time alerts, video clips, and live feeds for threat assessment.

* Database/Cloud Storage:

**Owner:** Cloud-based storage or on-premises database system.

**Integration**: Secure API-based interaction for storing and retrieving suspicious event data

**Usage**: Stores logs of detected anomalies, including timestamps, images, and video clips, for later review and reporting.

**3.3 Communication Interfaces**

• Alert Notifications: The system generates real-time alerts sent to the monitoring dashboard via secure web protocols (HTTPS).

• Threat Escalation: If a threat is confirmed, the system notifies security personnel through SMS, email, or push notifications using integrated communication APIs.

# System Functions / Functional Requirements

**User Functions**

**User Registration**Users (monitoring personnel or security personnel) can create an account by providing necessary credentials to access the weapon detection

**User Login**Allows users to securely log in to access their role-specific dashboard and surveillance data.

**View Real-Time Surveillance Data**Monitoring personnel can access live video feeds from ATM zones for proactive monitoring of activities.

**Monitor Suspicious Activity**Users can view alerts and flagged suspicious activities, such as the detection of visible weapons

**Log Out**Users can securely log out of the system to prevent unauthorized access.

**Operator Functions (Monitoring Personnel and Admin)**

**Manage User Accounts**

Admins can create, update, or delete user accounts to manage system access for monitoring personnel and security staff.

**Configure Surveillance Settings**Admins can adjust surveillance parameters, such as sensitivity levels for weapon detection or behavior analysis, and manage camera configurations.

**Monitor Alerts on Dashboard**Monitoring personnel can receive real-time alerts on their dashboards when weapons or suspicious behaviors are detected by the system.

**Confirm Threats and Escalate**Monitoring personnel can assess flagged events through live footage and escalate confirmed threats to security personnel if necessary.

**System Performance Monitoring**Admins can monitor the system’s health, uptime, and performance to ensure it operates optimally.

**View and Manage Security Logs**Admins can access and review alerts

**Support Functions**

**User Support**Provides assistance to users (monitoring personnel or security personnel) experiencing issues with account access or using the system features.

**System Maintenance**The system will undergo regular updates and maintenance to enhance stability, security, and detection accuracy.

**Functional Requirements**

| **Ref** | **# Functions** | **Category** | **Attribute** | **Details & Boundary Constraints** |
| --- | --- | --- | --- | --- |
| R1.1 | Detect weapons or anomalies in ATM users | Evident | System Response Time | Anomalies must be flagged within 5 seconds. |
| R1.2 | Generate and store security alerts | Evident | Notification Time | Alerts should be generated and sent to the dashboard within 2 seconds. |
| R1.3 | Monitor and log suspicious activities | Evident | Data Storage Efficiency | Logs of flagged activities should be stored in a secure database for future review. |
| R1.5 | Retrieve recorded video clips and logs | Evident | System Response Time | Logs and videos should be retrievable within 5 seconds. |

**Functional Goals Summary**

* Detection Efficiency: Real-time identification of threats like weapons or suspicious behavior, with alerts generated within seconds, enables rapid responses and escalation.
* Secure Logging: Encrypted storage of suspicious activity and logs ensures data privacy and supports detailed post-incident analysis.
* Quick Data Access: Prompt retrieval of logs ensures efficient investigation and smooth operation during critical events.

**System Attributes (Nonfunctional Requirements)**

| **Attribute** | **Details and Boundary Constraints** | **Category** |
| --- | --- | --- |
| Response Time | Critical operations (detection, logging, alerting) must respond within 5 seconds. | Mandatory |
| Concurrent User Load | The system should support monitoring by at least 10 personnel simultaneously without performance degradation. | Mandatory |
| Security | All data (alerts, logs, video clips) must be encrypted during transmission and securely stored to comply with regulations. | Mandatory |
| Availability | The system must ensure 97.9% uptime for reliable ATM security monitoring. | Mandatory |
| Usability | The dashboard interface must be user-friendly, enabling smooth operation with minimal training. | Optional |

**5.1 Use Cases**

**5.1.1 List of Actors**

1. **ATM User**
   * Interacts with the ATM. Their behavior is monitored by AI for anomalies and weapons.
2. **Monitoring Personnel**
   * Reviews flagged alerts, watches live video, and decides on escalation.
3. **Security Personnel**
   * Acts upon confirmed threats based on escalated alerts.

**5.1.2 List of Use Cases**

1. **Detect Suspicious Activity**
   * Continuously monitors ATM zones via CCTV for threats like weapons or strange behavior.
2. **Generate Alerts**
   * Triggers alerts upon detecting threats; sends alerts to monitoring dashboard.
3. **View Dashboard**
   * Monitoring personnel can view real-time alerts, live footage, and logs.
4. **Confirm Threat**
   * Determine if an alert indicates a real threat.
5. **Notify Security Personnel**
   * Sends an alert to the security team if the threat is confirmed.
6. **Log Activities**
   * Records all suspicious weapon and alerts .
7. **Access Logs**
   * Allows authorized users to retrieve stored logs and videos for investigation.

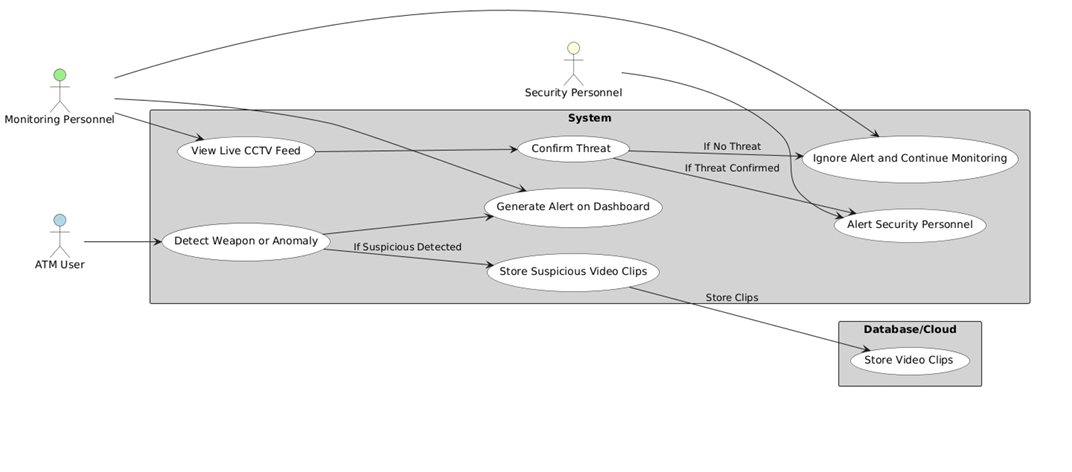
**5.1.3 Use Case Diagram**

**Actors:**

* ATM User
* Monitoring Personnel
* Security Personnel

**Use Cases:**

* Detect Suspicious Activity
* Generate Alerts
* View Dashboard
* Confirm Threat
* Notify Security Personnel
* Log Activities
* Access Logs
* Store Suspicious Video Clips



**Description of Use Case: Detect Suspicious Activity**

* **Use Case Name:** Detect Suspicious Activity
* **Actors:** ATM User, Monitoring Personnel, Security Personnel, AI-Based Detection System
* **Purpose:** Identify suspicious activities or threats (e.g., weapons, anomalous behavior) via AI-based detection through real-time CCTV monitoring.

**Preconditions:**

* AI detection system is active and integrated with ATM CCTV.

**Postconditions:**

* Monitoring personnel receive alert.
* Flagged data is saved in the database/cloud.
* Security personnel notified if necessary.

**Normal Flow:**

1. ATM user enters monitored area.
2. AI system detects threat or anomaly.
3. Alert is triggered and shown on monitoring dashboard.
4. Monitoring personnel reviews and confirms/dismisses threat.
5. If confirmed:
   * Security personnel alerted.

# Non - Functional Requirements

**6. Non-Functional Requirements**

**6.1 Performance Requirements**

* **Response Time:**All key operations, including user login, surveillance data retrieval, and suspicious activity detection, must be completed within a specified time limit (e.g., 5 seconds).
* **Data Processing Time:**Security analysis, such as suspicious activity detection, should be processed and results provided within a reasonable time frame (e.g., 10 seconds).

**6.2 Safety Requirements**

* **Data Protection:**All surveillance data and user information must be securely handled to avoid accidental loss or corruption.

**6.3 Security Requirements**

* **Authentication and Authorization:**The system must require secure login and authentication methods (e.g., two-factor authentication) to access user accounts and sensitive data.
* **Encryption:**All data, including user information and surveillance footage, must be encrypted during transmission and storage to prevent unauthorized access.
* **Compliance with Regulations:**The system must adhere to relevant security and data protection regulations, such as GDPR or other applicable regional laws.

**6.4 Reliability Requirements**

* **High Availability:**The system should ensure high availability, with a target uptime of 97.9%, ensuring minimal downtime.
* **Error Handling:**The system must be able to detect and recover from errors or failures without significant disruption to the surveillance services.
* **Data Redundancy:**Implement data redundancy mechanisms to ensure that critical system components (e.g., databases, servers) have backups and failover support.

**6.5 Usability Requirements**

* Ease of Use:  
  The system interface must be user-friendly, intuitive, and accessible to both technical and non-technical users.
* **Training Materials:**Training resources must be provided to help users and admins understand and use the system effectively.
* **Error Messaging:**Clear and concise error messages must be provided to guide users in resolving common issues.

**6.6 Supportability Requirements**

* **System Monitoring:**Admins should have the ability to monitor system performance, user activities, and security issues through built-in tools and dashboards.
* **Maintenance:**The system should allow for easy updates, maintenance, and bug fixes without requiring system downtime. Regular maintenance procedures must be in place.
* **Customer Support:**A dedicated support team must be available for resolving user or system issues, with a ticketing system for tracking and resolving support requests.

**6.7 User Documentation**

* **User Manual:**A comprehensive user manual should be provided, detailing the system features, how to register, log in, and monitor surveillance data.
* **Admin Guide:**A separate admin guide must be available to assist admins in managing user accounts, configuring system settings, and generating reports.
* **FAQ and Troubleshooting:**A section containing frequently asked questions and common troubleshooting steps should be available to help users and admins resolve common issues independently.

# References

1. [1] Ahmed, S., Bhatti, M. T., Khan, M. G., Lövström, B., & Shahid, M. (2022). Development and optimization of deep learning models for weapon detection in surveillance videos. Applied Sciences, 12(12), 5772. <https://doi.org/10.3390/app12125772>
2. [2] Abins, A. A., P, P., G C, R., & Cheran, R. (2024). Weapon Recognition in CCTV Videos: Deep Learning Solutions for Rapid Threat Identification. In 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE) (pp. 1–8). 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE). IEEE. <https://doi.org/10.1109/ic-etite58242.2024.10493569>
3. [3] Wang, G., Ding, H., Duan, M., Pu, Y., Yang, Z., & Li, H. (2023). Fighting against terrorism: A real-time CCTV autonomous weapons detection based on improved YOLO v4. Digital Signal Processing, 132, 103790. <https://doi.org/10.1016/j.dsp.2022.103790>
4. [4] Salazar González, J. L., Zaccaro, C., Álvarez-García, J. A., Soria Morillo, L. M., & Sancho Caparrini, F. (2020). Real-time gun detection in CCTV: An open problem. Neural Networks, 132, 297–308. <https://doi.org/10.1016/j.neunet.2020.09.013>
5. [5] Bamnolkar, A. K., Khakre, K. R., Gadge, A. R., Waje, M. G., Raut, V., & Khan, M. S. (2025). Cutting Edge Weapon Detection in Real-Time CCTV Videos. In 2025 10th International Conference on Signal Processing and Communication (ICSC) (pp. 345–350). 2025 10th International Conference on Signal Processing and Communication (ICSC). IEEE. <https://doi.org/10.1109/icsc64553.2025.10968883>
6. [6] Keerthana, S. M., Sujitha, R., & Yazhini, P. (2024). Weapon Detection For Security Using The Yolo Algorithm With Email Alert Notification. In 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET) (pp. 1–6). 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET). IEEE. <https://doi.org/10.1109/icicet59348.2024.10616365>