Application analysis report of big data in campus security system

I. Introduction

This report focuses on the application of big data in the campus security system, discusses its middleware functions, data requirements and database selection in different security scenarios, as well as related communication and artificial intelligence technology applications, aiming to provide a comprehensive technical reference for building an efficient campus security system.

Second, the middleware function analysis of the campus security system

(1) Data integration and transformation

Middleware collects data from different sensors (e.g., cameras, infrared detectors, access control systems, etc.) and devices (e.g., security robots) and converts it into a uniform format for subsequent processing and analysis. For example, the video stream data of the camera can be parsed into structured data containing key information such as time, place, and character characteristics, so that data from different sources can be compatible and correlated with each other.

(2) Real-time communication and coordination

Ensure real-time communication between various components of the security system, and ensure the smooth transmission of information between security robots and between robots and monitoring centers. When an abnormal situation is found, the middleware can quickly coordinate the robot to respond, such as sending nearby robots to the incident site and timely feedback the on-site situation to the monitoring center.

(3) Intelligent decision support

Based on the data collected and processed, pre-set algorithms and rules are used to support security decisions. For example, by analyzing the flow data and historical event patterns, the current security risk level in the campus can be judged, which provides a basis for security personnel to formulate patrol routes and resource allocation, and improves the pertinence and efficiency of security work.

3. Data requirements and database selection in security scenarios

(1) Scenario 1: Personnel intrusion detection

1. **Data Requirements**

- Video surveillance data: Record real-time footage of various areas of the campus to identify the appearance and behavioral characteristics of intruders.

- Access control record data: record the time, place, and identity information of personnel entering and leaving the campus, and assist in judging the entry path of intruders.

- Geographic data: Campus map information to clarify the specific location of the break-in incident, so that security personnel can respond quickly.

2. **Database Selection and Reasons**

- For video surveillance data (semi-structured data), a document-based database (such as MongoDB) is appropriate. It can efficiently store and query large-scale video-related metadata, facilitate the rapid retrieval of video clips in specific time periods and regions, and flexibly adapt to changes in video data formats and content.

- Access log data and geospatial data (structured data), choose a relational database (e.g., MySQL). This is because relational databases are good at processing data with complex relationships, and can realize multi-table association queries through a powerful query language, such as associating access control records, personnel information tables, and geographic information tables, to quickly and

accurately obtain relevant information, ensure the consistency and integrity of data, and meet the needs of accurate analysis of personnel intrusion events.

(2) Scenario 2: Fire alarm

1. **Data Requirements**

- Smoke sensor data: Monitor smoke concentration changes in real-time to determine the likelihood and location of a fire.

- Fire equipment status data: including information such as the location, availability, and last maintenance time of fire extinguishers, hydrants, etc., so that they can be quickly deployed in the event of a fire.

- Building structure data: Floor plans, floor plans, evacuation routes, and other information of campus buildings to plan the best evacuation routes.

2. **Database Selection and Reasons**

- Smoke sensor data (real-time data streams, semi-structured data) with the option of a time-series database such as InfluxDB. It is optimized for time series data, which can efficiently handle massive sensor data writing and querying, quickly analyze the trend of smoke concentration, and issue fire warnings in time.

- Fire equipment status data and building structure data (structured data) suitable for relational databases such as PostgreSQL. The relational database can ensure the accuracy and completeness of fire-fighting equipment information and building structure information, and support complex query operations through strict schema definition and transaction processing, such as querying the available fire-fighting equipment closest to the fire occurrence point, and planning a safe evacuation path according to the building structure, so as to ensure the reliability and efficient use of data in the event of a fire emergency.

(3) Scenario 3: Early warning of campus violence

1. **Data Requirements**

- Social Media Monitoring Data: Collect information on students' speech and emotional tendencies on social media platforms on campus to detect potential signs of violent conflict in advance.

- Personnel behavior data: Through the surveillance cameras and sensors on campus, analyze the daily behavior patterns of students, such as abnormal gatherings, violent quarrels, and other behavioral characteristics.

- Student profile data: including the student's basic information, past disciplinary records, mental health assessment, etc., to

comprehensively assess the risk factors of the student's participation in violent incidents.

2. **Database Selection and Reasons**

- Social media monitoring data (unstructured data) with a text-based database (e.g., Elasticsearch) is appropriate. It has powerful full-text search and data analysis capabilities, and can quickly index, query and analyze a large amount of text data, dig out the key information and emotional tendencies in it, and discover the potential risks related to school violence in a timely manner.

- Human behavior data (semi-structured data), consider using a graph database such as Neo4j. The graph database is good at processing complex relational network data, and can visualize the behavioral interaction between students in a graphical way, which is convenient for analyzing the abnormal associations in human behavior patterns, and quickly identifying potential violent incident transmission paths and key people.

- Student profile data (structured data), choose a relational database (e.g., Oracle). The relational database can strictly ensure the accuracy and completeness of student file data, and realize multi-dimensional student information association analysis through a perfect transaction processing mechanism and powerful query function, such as combining students' basic information, disciplinary

records and mental health status, accurately assessing the risk of students participating in school violence incidents, and providing reliable data support for preventing and intervening in school violence incidents.

Fourth, the application of communication and artificial intelligence technology in the campus security system

(1) Communication technology

1. **Starlink 卫星通信（https://www.starlink.com/）**

- Benefits: High-speed Internet access with global coverage ensures stable communication of campus security systems in remote areas or areas with weak network infrastructure. In the case of a large campus area or network blind spots, satellite communication can ensure real-time data transmission between the security robot and the monitoring center, avoiding potential security risks caused by network interruption.

- Application: The security robot can upload monitoring video, sensor data and other information to the monitoring center in real time through Starlink satellite communication, and receive instructions from the monitoring center at the same time to achieve remote control and real-time scheduling. For example, in remote

corners around the campus or areas with unstable network signals on campus, security robots can still maintain close contact with the monitoring center to ensure the seamless operation of the entire campus security system.

(2) Artificial intelligence technology

1. **Microsoft Azure Machine Learning as a Service （https://azure.microsoft.com/en-us/products/machinelearning/?msockid=1a36027e6e10605d085e16946f5a6192）**

- Applied to anomalous behavior recognition: Uses machine learning algorithms to analyze the behavior of people and vehicles on campus in real time. Through the learning and training of a large number of normal behavior data, a behavior pattern model is established, and when a large difference from the normal mode is detected, such as personnel entering a restricted area during non-opening hours, speeding or abnormal wandering, etc., the system will automatically send out an alarm to remind security personnel to pay attention to and deal with it.

- Fire risk prediction: Machine learning models are used to predict fire risk based on historical fire data, environmental data (such as temperature, humidity, smoke concentration, etc.) and building

facility information on campus. Identify potential fire risk factors in advance and provide decision-making support for campus fire management, such as arranging fire equipment inspections in advance and optimizing the allocation of fire resources, so as to reduce the possibility of fire occurrence and the degree of loss.