**Weapon Detection**

**ABSTRACT**

The proposed system introduces a comprehensive and modular application that seeks to optimize the operational dynamics and communication channels within a banking organization. The system is structured around a series of interconnected modules, each serving a specific purpose and catering to the needs of distinct user roles, encompassing administrators, branch managers, staff members, and an innovative camera-based detection module. The primary functions of each module are as follows:

Admin Module:

At the core of the system, the Admin module empowers administrative users with authority over crucial aspects such as designations, branches, staff management, attendance tracking, detection incidents, customer complaints, responses, and notifications. Serving as the control hub, this module facilitates seamless coordination.

Login Module:

Ensuring stringent security measures, the Login module grants authorized access to users across all other modules, guaranteeing the integrity of data and validating user identities.

Manage Designation Module:

For administrators, the Manage Designation module facilitates the creation and oversight of various staff designations, optimizing human resource allocation and management.

Manage Branch Module:

The Manage Branch module equips administrators to efficiently handle diverse branches of the bank, fostering streamlined branch operations and effective communication.

View Staff Module:

Administrators benefit from the View Staff module, which offers a comprehensive overview of staff members' information, supporting efficient human resource management.

View Detection Module:

By collating detection incident data from the Camera Module, the View Detection module enables administrators to assess and respond to potential security threats effectively.

View Complaints Module:

Addressing customer feedback becomes more efficient with the View Complaints module, allowing administrators to gain insights into customer concerns and tailor responses accordingly.

Send Reply Module:

To enhance customer satisfaction and communication, administrators utilize the Send Reply module to compose and send well-crafted responses to customer complaints.

Send Notification Module

Critical announcements and updates are disseminated through the Send Notification module, ensuring timely and effective communication with both staff members and customers.

Branch Module:

Branch-specific operations are managed through the Branch module, which encompasses branch manager login, staff management, attendance tracking, detection incident reporting, complaint submission, reply viewing, and notification reception.

Staff Module:

Catering to individual staff members, the Staff module encompasses features such as attendance logging, profile viewing, profile editing, complaint submission, response viewing, and notification reception.

Camera Module:

The innovative Camera Module integrates seamlessly, leveraging advanced image processing techniques to detect weapons and bolstering security measures within the bank.

Detect Weapon Module:

A vital component of the Camera Module, the Detect Weapon module employs image analysis to identify potential weapons, triggering swift and appropriate responses to enhance security protocols.

Send Alert Module:

Upon weapon detection, the Send Alert module instantly notifies relevant personnel, ensuring immediate responses to security incidents.

In summary, the proposed modular system aims to establish a structured and efficient framework for managing various facets of a banking organization. By catering to diverse user roles, the system enhances communication, security, and customer service. The integration of specialized modules creates a harmonious and secure operational environment, enhancing the overall effectiveness of the banking institution.

Modules

* **Admin (bank)**
  + Login
  + Manage designation
  + Manage branch
    - View staff
  + View detection
  + View complaints
    - Send reply
  + Send notification
* Branch
  + Login
  + Manage staff
  + View attendance
  + View detection
  + Send complaints
    - View reply
  + View notification
* **staff**
  + Login
    - Mark attendance
  + View profile
    - Edit profile
  + Send complaints
    - View reply
  + View notification
* Camera Module
  + Detect Weapon
  + Send Alert

**Existing System**

While banks have implemented various security measures to protect their premises and assets, there are several drawbacks associated with the current systems. Traditional security measures, such as security guards, surveillance cameras, and alarm systems, may have limitations in effectively preventing and responding to modern security threats. Security personnel might not always be able to respond rapidly to emergencies, and relying solely on human monitoring can result in blind spots and human errors. Surveillance cameras, while valuable for recording incidents, might not be able to proactively identify suspicious behavior in real-time. Additionally, false alarms from alarm systems can lead to desensitization among staff and authorities, potentially delaying responses to genuine threats. Access control mechanisms like PIN codes and access cards can be vulnerable to theft or duplication, undermining their effectiveness. Furthermore, the costs associated with installing, maintaining, and upgrading these systems can be substantial, particularly for smaller banks. The evolving landscape of security risks, including technological advancements made by criminals, underscores the need for more advanced and adaptable security solutions to overcome these limitations

**Proposed System**

The proposed system introduces a comprehensive and technologically advanced approach to enhancing security within banks. Centered around YOLO-based weapon detection, this system aims to overcome the limitations of the current security measures. By leveraging the capabilities of YOLO (You Only Look Once) object detection, the system can automatically identify and alert security personnel to the presence of weapons in real-time. This offers a proactive means of threat detection that complements existing security measures. YOLO's rapid processing and accurate identification can significantly reduce response times during potential security incidents. However, it's important to note that the proposed system's effectiveness is contingent upon the accuracy of the YOLO model, and false positives or negatives could potentially occur. Additionally, successful implementation requires integrating the YOLO-based detection module seamlessly into the bank's existing security infrastructure, along with appropriate training for security personnel. While this proposed system represents a significant step forward in bolstering security, it's essential to consider potential challenges, such as system maintenance, model updates, and costs associated with technology adoption.

**SOFTWARE REQUIREMENTS**

A software requirement specification (SRS), a requirements specification for a software system, is a complete description of the behavior of a system to be developed and may include a set of use cases that describe interactions the users will have with the software. In addition it also contains non-functional requirements. Non-functional requirements impose constraints on the design or implementation (such as performance engineering requirements, quality standards, or design constraints) the software requirements specification document enlists all necessary requirements that are required for the project development. To derive the requirements we need to have clear and thorough understanding of the products to be developed. This is prepared after detailed communications with the project team and customer.

Operating System: WINDOWS 8 or above for better performance

Front end: Python (For web application), Android (Mobile Application)

Back end: MYSQL

Software: SubLime Text, WAMP, Android Studio

Web Browser: Internet Explorer/Google Chrome/Firefox

Web Server: Apache

**HARDWARE REQUIREMENTS**

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware. A hardware requirements list is often accompanied by a hardware compatibility list (HCL), especially in case of operating systems. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular operating system or application.

Processor: Intel Pentium or above.

Hard Disc: 320GB.

Display Type: PC Display.

Keyboard: PC/AT Enhanced PS/2Keyboard (110/10Key).

Mouse: First/Pilot Mouse Serial (c48).

Input Device: Mouse, keyboard

Output Device: Monitor, Mobile Display