IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

OPEN DESK: Intelligent Cyber-Physical Security System

[1]Om Amonkar, [2]Samruddh Jadkar, [3]Rushiraj Chaudhari, [4]Jigisha Ghanekar, [5]Mahendra Patil
[1]Student, [2] Student, [3]Student, [4]Student, [5]Senior Professor
[1]Department Of Computer Engg.,
[1]Atharva College Of Engineering, Mumbai, India

Abstract: This project focuses on creating a robust corporate security framework to protect sensitive data and intellectual property. Using a multilayered approach, it integrates advanced cybersecurity technologies, stringent access controls, and continuous monitoring to defend against internal and external threats [10]. A key component is a risk management strategy to identify and address vulnerabilities in corporate networks, cloud systems, and endpoint devices. [9] Employee training and awareness are also emphasized, acknowledging the importance of human factors in maintaining security. [15] The project delivers a resilient and adaptive security posture, ensuring long-term protection of corporate assets and data integrity against evolving cybersecurity threats.[9]

INTRODUCTION

In today's interconnected business landscape, corporate security is a top priority across industries. The rise in cyber threats, coupled with reliance on digital assets, amplifies the risks of data breaches and intellectual property theft. This project aims to tackle these challenges by creating a robust security framework that protects against current and future threats.[8] By integrating advanced cybersecurity technologies, implementing strict access controls, and promoting a culture of security awareness, the project aims to build a resilient defense mechanism. This mechanism will ensure long-term protection of sensitive data and compliance with regulatory standards. The focus will be on both technical and human factors that contribute to a secure corporate environment. [10]

Keywords - Corporate Security, Cyber Threats, Digital Assets, Data Breaches, Intellectual Property Theft, Cybersecurity Technologies, Access Controls, Security Awareness, Regulatory Compliance, Resilient Defense

RELATED WORKS

The integration of system-level monitoring and biometric surveillance for enterprise security has gained significant attention in recent years. Various commercial solutions and academic studies have explored individual components of what OpenDesk aims to unify into a single intelligent platform.

1. *System Monitoring and Employee Productivity Tools:*

Tools like **ActivTrak**, **Teramind**, and **Hubstaff** provide real-time monitoring of employee desktop activity, application usage, and productivity metrics. These systems emphasize behavioral analytics and user-based access control but typically lack integration with physical tracking or real-time threat detection at the service/process level. Research by [P. D. Turnbull et al. (2020)] highlights the effectiveness of system-level behavioral analytics in detecting insider threats through anomalous system usage.

2. *Biometric Surveillance and Access Control*

Biometric access systems such as those described in [Kumar et al., 2019] use facial recognition to grant or deny access to secure zones. Smart surveillance systems powered by deep convolutional networks (CNNs) have demonstrated significant success in real-time facial identification and crowd analysis. However, these systems often operate in isolation and are limited to access control rather than continuous presence validation across the premises. *Integrated Physical and Digital Security Models*

Recent literature suggests a move toward **converged security systems** that merge IT and physical security infrastructures. For example, [Ahmed et al., 2021] proposed a hybrid architecture that combines biometric data with RFID-based zone access and computer logon activity to improve contextual decision-making. While promising, such models have yet to be adopted at scale due to integration complexity and lack of modularity.

3. *Path Tracking and Movement Analysis*

Studies in smart surveillance, such as [Zhang & Luo, 2022], propose spatio-temporal tracking frameworks to trace individual movements through camera networks in indoor environments. These frameworks typically focus on public safety or retail analytics, and lack extensions into enterprise productivity, compliance auditing, or real-time alerting.

METHOD

The proposed solution, **OpenDesk**, integrates system-level monitoring and physical surveillance into a unified corporate security framework. The methodology adopted for the design and implementation of OpenDesk is modular and scalable, ensuring real-time performance, threat detection, and secure data handling. The approach consists of four primary components working in a synchronized pipeline, as described below:

1. *System Monitoring Agent (SMA)*

This desktop-based agent operates continuously on employee machines and performs the following tasks:

a. **Performance Metrics Collection:** Resource utilization statistics (CPU, memory, disk I/O, and network usage) are captured at regular intervals to assess system health and employee activity levels.

b. **Threat Detection & Classification:** System processes, services, and background tasks are analysed using rule-based and heuristic algorithms to identify anomalous behaviours indicative of malware, unauthorized software, or misuse.

c. **Event Logging & Transmission:** Monitored data is logged locally and transmitted periodically to the central backend using secure, encrypted channels.[9][10]

2. *Biometric Surveillance Engine*

A network of surveillance cameras integrated with a facial recognition system handles the physical tracking of individuals within the workplace:

a. **Face Detection and Recognition:** Video streams from CCTV/IoT cameras are processed in real-time. Faces are detected and matched against a pre- registered employee database using deep learning models.[1][2][4]

b. **Access Validation:** Each camera is mapped to a predefined physical zone. Detected faces are cross-verified against zone permissions to detect unauthorized presence.

c. **Unknown Face Logging:** Faces that do not match any registered profiles are logged, and snapshots are forwarded to the central system for manual review. [3][5][6]

3. *Central Backend Server*

The central server acts as the aggregation and processing hub for all incoming data streams:

a. **Data Fusion:** Inputs from the SMA and Biometric Surveillance Engine are merged and organized into structured records linked by employee identifiers and timestamps.

b. **Anomaly Detection Engine:** Correlation-based checks are performed to identify behavioural anomalies, such as discrepancies between system usage and physical presence, or access violations.

c. **Storage & Indexing:** All data is securely stored using an encrypted database, with optimized indexing for fast retrieval and *report generation [13][14]*

4. *Report Generation and Movement Analysis*

Based on collected data, OpenDesk supports both descriptive and predictive analytics for organizational insight:

a. **Daily & Monthly Reports:** Aggregated summaries of productivity, resource usage, zone access, and threat detection incidents are auto-generated. These reports are exportable in various formats (PDF, CSV) and can be scheduled for delivery.

b. **Path Reconstruction & Visualization:** The system reconstructs individual movement paths by chaining camera detections throughout the day. Time- stamped trajectories are visualized on office floorplans, enabling retrospective analysis and incident tracking.

c. **Alert Mechanism**: Configurable thresholds allow automated alert generation for suspicious activity, such as high-risk application usage or entry into restricted areas.[9][7]

Keywords - System Monitoring, Threat Detection, Facial Recognition, Biometric Surveillance, Access Control, Anomaly Detection, Data Fusion, Encrypted Storage, Movement Analysis, Productivity Reporting, Real-Time Monitoring, Secure Communication, Corporate Security, CCTV Integration, Behavior Analytics.

Use Case Diagram

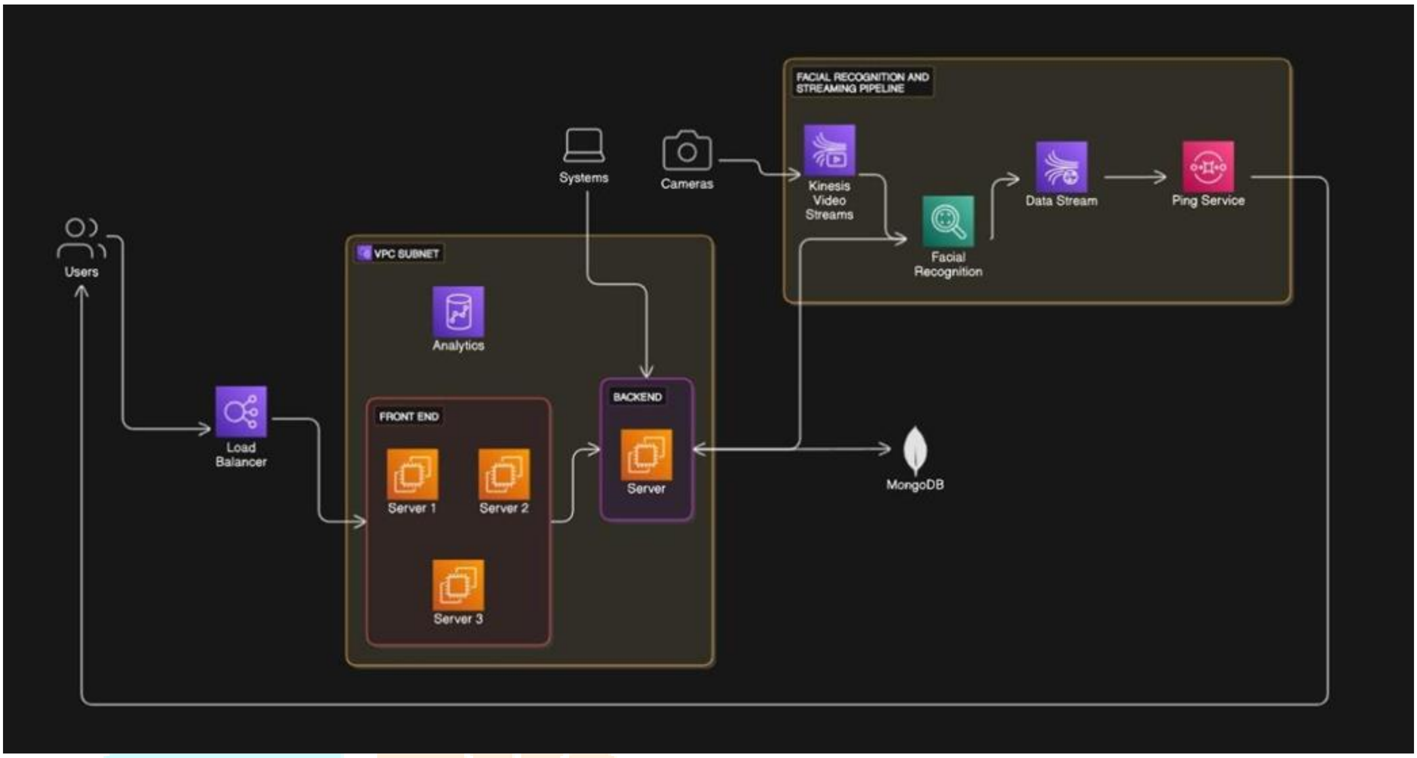
The use case diagram visually represents the system's functional requirements by outlining the different actors (users or external systems) and their interactions with the system's functionalities. It helps in understanding the system's scope and the various actions that users can perform within the system, ensuring that all necessary operations are captured.

System Architecture

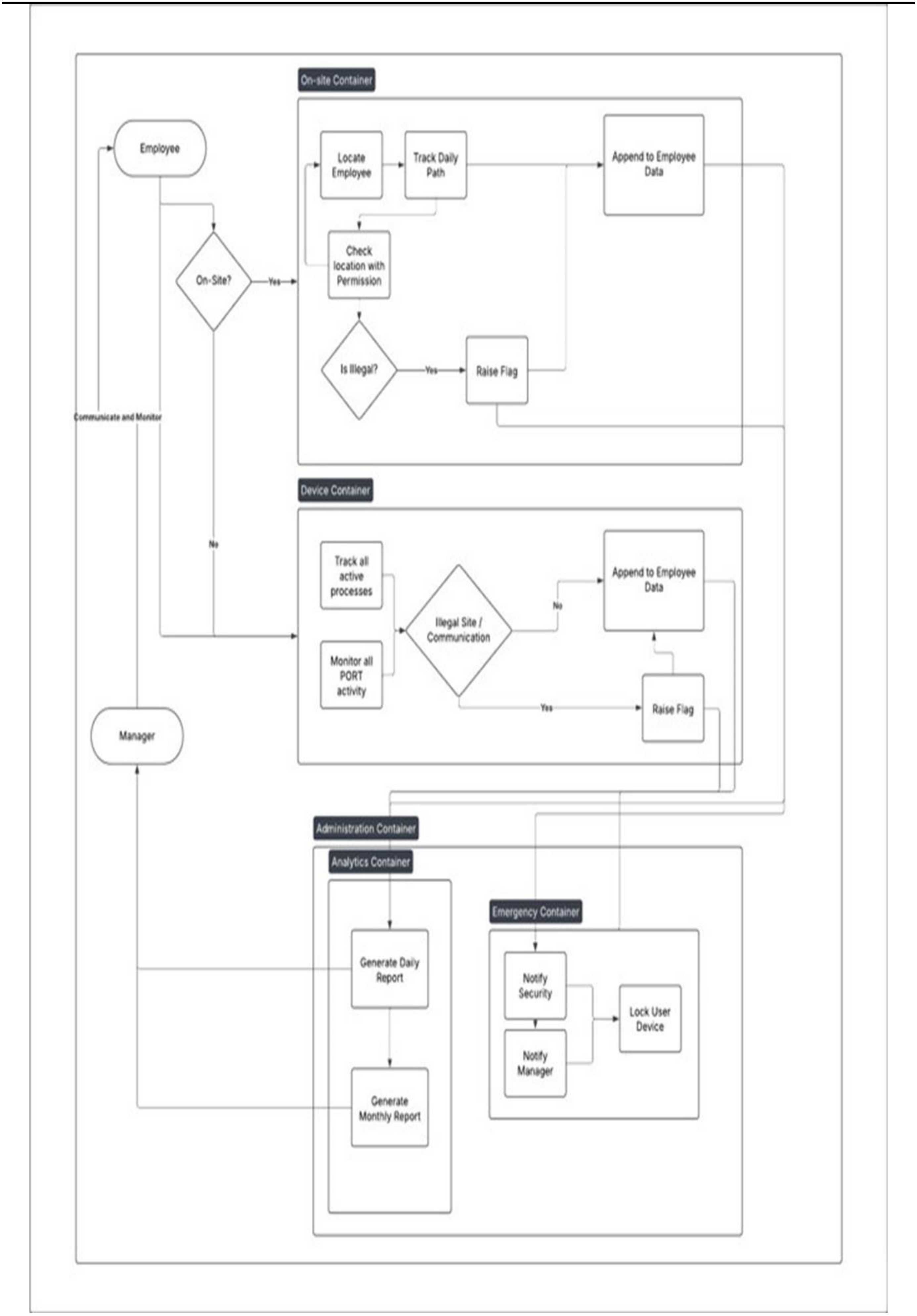
The system architecture defines the structure of the entire system, including its components, modules, and the interactions between them. It outlines how different parts of the system communicate, ensuring that data flows efficiently and processes are handled correctly. This high-level overview helps in understanding the technical infrastructure and integration of system components.

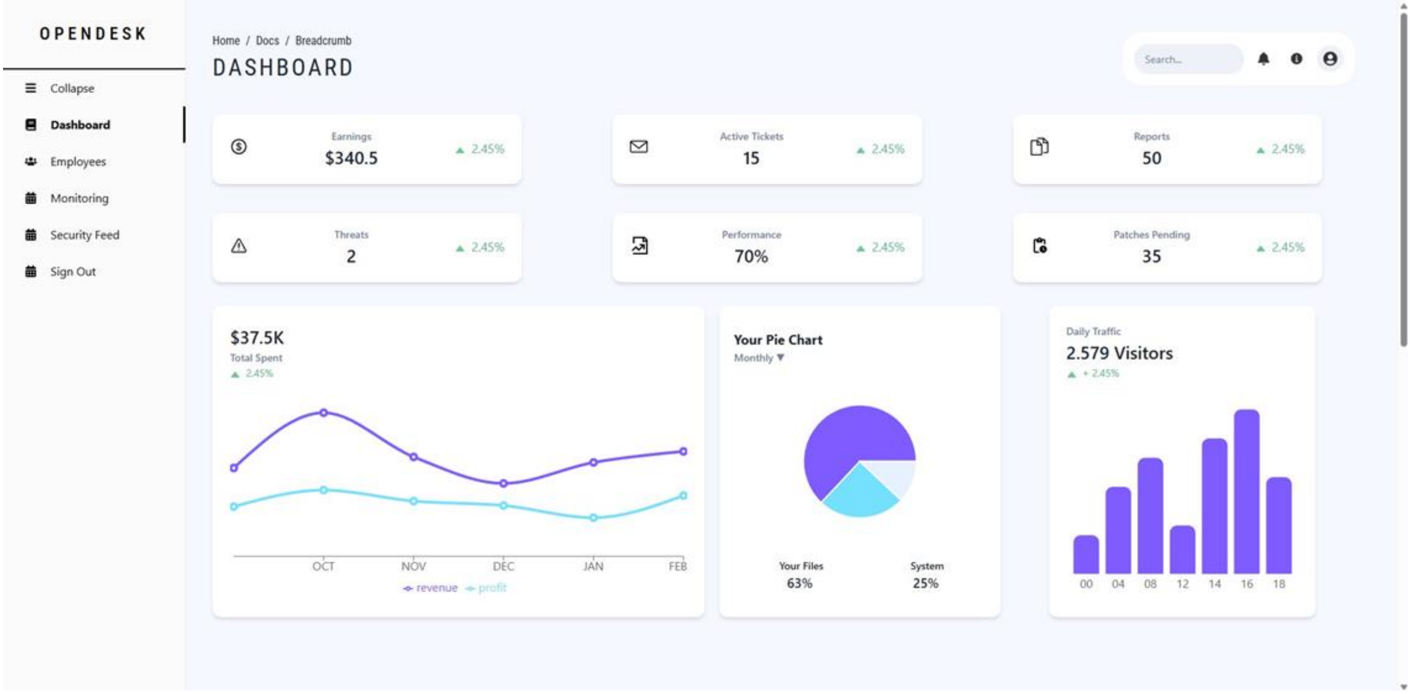
Implemented Dashboard

The implemented dashboard is a user-friendly interface that presents key performance indicators and relevant data in an organized and visually appealing manner. It allows users to monitor real-time data, analyze trends, and interact with the system seamlessly. The dashboard is designed to provide actionable insights and improve decision-making processes, making it a crucial part of the overall user experience.



SYSTEM ARCHITECTURE


On-site Container
Employee
Locate Employee
Track Daily Path
Append to Employee Data
Check location with Permission
On-Site?
Yes
Is Illegal?
Yes
Raise Flag
Communicate and Monitor
Device Container
No
Track all active processes
Illegal Site / Communication
No
Append to Employee Data
Monitor all PORT activity
Yes
Raise Flag
Manager
Administration Container
Analytics Container
Emergency Container
Generate Daily Report
Notify Security
Lock User Device
Notify Manager
Generate Monthly Report



USE CASE DIAGRAM DESKTOP VIEW OF DASHBOARD

Result

The integration of system-level monitoring with biometric surveillance in OpenDesk is theoretically expected to result in a more comprehensive and context-aware corporate security system. By continuously analysing system resource usage and user activity, the platform can detect subtle deviations from normal behaviour that may indicate insider threats, malware, or policy violations. The use of behavioural heuristics and service-level inspection offers the potential for identifying threats that signature-based systems often miss.[9] [10]

In parallel, the facial recognition module enhances physical security by validating presence in restricted zones and identifying unknown individuals in real time. The synchronization of digital and physical activity—such as verifying that a user logged into a workstation is physically present in the expected area—adds a new dimension to threat detection, reducing false positives and improving accountability.[11]

Furthermore, the automated reporting and data aggregation mechanisms theoretically improve decision-making by providing structured insights without manual effort. Daily and monthly reports compiled from multiple data streams offer visibility into both security incidents and organizational patterns such as employee productivity, zone utilization, and access anomalies.[7]

Lastly, the path tracking system based on sequential camera detections provides a timeline of movement across the office space. This contributes to post-incident investigations, compliance auditing, and safety management. Overall, the unified architecture of OpenDesk is expected to deliver proactive threat detection, reduce security blind spots, and foster a culture of transparency and safety in the corporate environment.[13][14]

Keywords - Governance, Organizational Security Policy, Compliance, Risk Management, Regulatory Requirements, Procurement, Technical Controls, Incident Response, Cybersecurity Awareness Training, Corporate Security

Review of Literature

1. C.-S. Chang and others

   Development of an ARM-based human face recognition system using a modified PCA algorithm, emphasizing efficient on-device authentication through biometric analysis.

2. L. Khurana and others

   Comparative evaluation of OpenCV face recognition algorithms, analyzing the effectiveness of different recognizers and highlighting advancements in user-friendly, non- intrusive biometric authentication

3. K. S. Rao and others

   Survey of state-of-the-art techniques for recognizing occluded face images, categorizing methods from PCA-based to neural networks, and analysing their effectiveness across standard facial recognition datasets.

4. K. Qiu and others

   Introduces a post-processing model based on Hidden Markov Models (HMM) to enhance face recognition in videos, addressing challenges posed by pose and illumination variations— termed the "curse of data source."

5. S. Wattamwar and others

   Proposes an optimal face recognition system combining Haar cascades and LBPH algorithms, focusing on improving accuracy under challenging conditions for applications like smart voting authentication.

6. J. Howse

   Tutorial on training object detectors and recognizers using Python and OpenCV, focusing on Haar cascades and LBPH/Fisherface/Eigenface methods, with real-time GUI-based learning and cross-platform deployment potential.

7. A. Rahmati and others

   Introduces a hybrid employee performance evaluation model combining Fuzzy AHP and Fuzzy TOPSIS to minimize bias from subjective judgments and enhance decision-making accuracy in organizational assessments.

8. H. Dong and others

   Presents an optimized performance evaluation indicator system for Xuzhou Coal Mining Group, addressing gaps in coverage, clarity, and quantification to enhance assessment accuracy and organizational effectiveness.

9. S. Safrizal and others

   Proposes an employee performance evaluation system using the profile matching method to objectively rank employees based on key criteria, achieving 93% accuracy in identifying top performers for awards.

10. A. I. Belaya and others

    Analyzes various classes of corporate information systems and their functionalities in innovative project management, using comparative analysis to guide selection for optimal project outcomes.

11. H. Mliki and others

    Presents an automatic facial expression recognition system that overcomes variations in expression intensity, with automatic detection and segmentation of facial features for accurate emotion identification.

12. S. Manzoor and others

    Analyzes object tracking models, with SiamMask excelling in single-object tracking and YOLOv4+DeepSort in multi-object tracking, both struggling with full occlusion.

13. R. Raj Bharath and G. Dhivya

    Proposes a method for moving object detection and classification in video surveillance, including speed calculation and parameter evaluation for dynamic scenes.

14. A. P. Jana and others

Utilizes YOLOv2 for real-time object detection and classification in video records, offering a faster alternative to traditional machine learning methods using GPU acceleration.

15. R. Saáry

Defines corporate security responsibility (CSecR) through expert interviews, identifying three key dimensions for further industry-specific research.