ALIRO: Secured system design for tracking of visitor access in Tech Parks

Himanshi Agarwal,
Department of Computer Science,
CHRIST (Deemed to be University),
Bengaluru, Karnataka 560029
himanshi.agarwal@bca.christuniversity.in

Gaurav Jain,
Department of Computer Science,
CHRIST (Deemed to be University),
Bengaluru, Karnataka 560029
gaurav.jain@bca.christuniversity.in

Sumit Roberts Emmanuel,
Department of Computer Science,
CHRIST (Deemed to be University),
Bengaluru, Karnataka 560029
sumit.emmanuel@bca.christuniversity.in

Dr. Logeshwaran J,
Department of Computer Science,
CHRIST (Deemed to be University),
Bengaluru, Karnataka 560029
logeshwaran.j@christuniversity.in

***Abstract*— The Access Control App for Tech Parks is an innovative mobile application designed to enhance security and streamline access management within tech park environments. Utilizing Kotlin and machine learning (ML) focusing on facial recognition technology, the app provides a robust employee and visitor access control solution. Employees are granted access through facial recognition matching with an existing database, ensuring secure and efficient entry. Visitors must register via the app, specifying their purpose and the employee they intend to visit. Upon arrival, the visitor's face is scanned, and the associated employee is notified to approve or disapprove the visit. The employees can pre-register visitors for direct access on specified dates, with notifications sent upon entry. This system also includes two-step verification of the visitors with time-sensitive entry codes to enhance security. The app features movement history tracking for employees and visitors, offering a comprehensive overview of access activities within the tech park. In addition to managing personal access, the app also handles vehicle entry. It includes a feature for scanning visitors' vehicle number plates and allocating parking spaces in their parking lot. This information is communicated to the visitor via the app, guiding them to their designated parking spot and reducing congestion and confusion in the parking area. Moreover, the app includes a Visitor Diary module where visitors can see feedback from other visitors and upload their own, fostering a community-driven environment and continuous improvement based on visitor experiences. Enhancing security and improving the overall user experience, the app makes tech parks safer and more manageable environments.**

Keywords*— *Security, Access Control, Scan, Tracking, Face Recognition, Tech Parks

I. INTRODUCTION

In today's technology-focused world, the need for good security and quality management in technology schools has never been greater. These areas have become innovation and production centers, hosting many technology companies and sensitive projects, and ensuring people's and equipment's safety is essential [1]. Traditional access control systems such as physical ID cards and visitor records need to be improved to meet the security needs of schools today. Although old systems were once effective, they no longer meet the needs of today's dynamic and evolving technology environment. On the other hand, manual visitor entry is more than just time-consuming and prone to human error. It must immediately provide the information and insights for reasonable management security [2]. The administrative burden of managing and analyzing this information can be inefficient and slow, ultimately disrupting business processes in technology-enabled offices. Mobile technology has become ubiquitous, and smartphones and mobile apps are changing every aspect of our daily lives [3]. Machine learning, especially in artificial intelligence, has shown its potential to improve security through its ability to analyze and process large amounts of data accurately and efficiently. The program aims to solve these problems by integrating facial recognition technology and vehicle control into the control system [4]. Aliro is not a further development of traditional methods but a complete rethinking of access management in school technology [5]. Aliro uses state-of-the-art machine learning algorithms to accurately and instantly identify individuals, ensuring that only authorized personnel can enter the site. This device overcomes the limitations of physical ID cards and provides a secure and reliable way [6]. The facial recognition system used in Aliro is designed to continuously learn and adapt, improving accuracy over time and reducing issues caused by changes in environment and appearance [7]. The vehicle access control system feature simplifies the process of vehicle access and station allocation by using high-resolution cameras and optical character recognition (OCR) to identify and verify vehicle licenses. Aliro reduces parking congestion and confusion by automating access control, improving overall efficiency and user experience [8]. Users can register, receive notifications, and manage access rights directly from their smartphones. This order-driven approach streamlines the user experience and allows employees to securely monitor and control access to remote work, providing greater convenience and work that can manage the entire visitor lifecycle from registration to payment. Visitors can pre-register for the app to receive real-time notifications about their entry status and view their play history using the park's technology. This change ensures guests a friendly and efficient experience while maintaining strict security. These features create a collaborative environment that encourages continuous improvement based on user experience, understanding, and strength. By combining facial recognition and automated vehicle control, Aliro offers a robust, efficient, and effective solution for modern park technology. This article looks closer at Aliro's design and implementation, highlighting its potential to revolutionize environmental technology management.

II. Related Works

Access control systems have undergone a remarkable metamorphosis over recent decades, shifting from rudimentary manual procedures to sophisticated digital innovations [9]. Though functional, antiquated methods such as physical identification cards and paper logs were plagued by human error and inefficiency [10]. The emergence of electronic systems heralded the introduction of key cards and PIN codes, bolstering security and refining access management. However, a genuine paradigm shift emerged with the advent of biometric systems, which leverage unique physiological attributes for authentication. Facial recognition, in particular, has surged in prominence owing to its unobtrusive nature and significant accuracy enhancements propelled by machine learning advancements [11]. Initial facial recognition systems grappled with precision and environmental inconsistencies. However, contemporary methodologies utilizing deep learning algorithms, such as convolutional neural networks (CNNs), have achieved extraordinary performance. The proliferation of mobile technology has further revolutionized access management by enabling real-time updates and remote oversight via mobile applications. Studies suggest mobile solutions augment user convenience and operational efficiency by integrating security features such as notifications and movement tracking. Machine learning is pivotal in modern access control systems, with algorithms continually evolving and adapting to enhance precision and alleviate administrative burdens [12]. Case studies, exemplified by those conducted at Stanford University, underscore the efficacy of facial recognition systems in enterprise settings, achieving high accuracy and markedly curtailing unauthorized access. Implementations in technology parks and analogous facilities have demonstrated that incorporating facial recognition into mobile applications can adeptly manage visitor access and streamline operations. Despite these advancements, challenges persist, particularly regarding privacy and ethical concerns. Collecting and storing biometric data raise apprehensions about misuse and unauthorized access, necessitating stringent data security measures and adherence to regulations such as GDPR [13]. Additionally, addressing algorithmic bias and ensuring fairness in access control systems are imperative to prevent discrimination.

III. Proposed Model

Secured system design for tracking visitor access in tech parks refers to implementing various physical and digital security measures to monitor and control the entry and movement of visitors within a technology park. This includes using access control systems, such as biometric or RFID-based identification, to ensure that only authorized individuals are granted entry. It also involves using CCTV cameras to monitor visitor activity and track their movements within the park. Moreover, visitor data is securely stored and managed through encrypted databases to ensure the privacy and confidentiality of personal information. This system design not only helps prevent unauthorized access and potential security breaches but also allows for efficient tracking and record-keeping of visitor activity. With the increasing threat of data theft and physical security risks, a well-designed secure system is vital for maintaining a safe and secure environment within tech parks..

A. User Registration and Authentication

The cornerstone of access is the user registration and authentication system, which ensures that only authorized individuals can enter the technology park. Employees undergo a unique registration process during which their personal and facial data is collected and securely stored in a central database. This involves capturing top-quality images from different angles to create a comprehensive facial profile. The data is encoded and protected to prevent unauthorized access and maintain confidentiality. Before visiting, guests must register, provide personal details, specify the purpose of their visit, and confirm that they are meeting with an employee. With this information, the system can grant or deny access based on the employee's approval. Advanced facial recognition technology is used in the authentication process to verify identity. It compares real-time facial data with the stored profiles, ensuring secure and smooth access for staff and authorized visitors. The fig.1 (a) and 1 (b) shows the respective DFD level 0 and level 1 in the following,

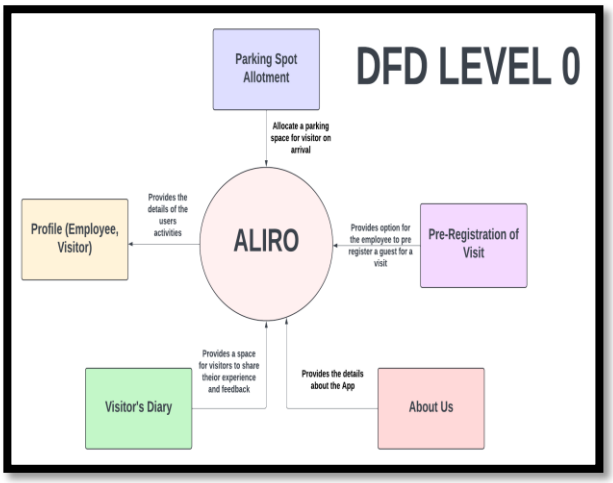

Fig.1 (a): DFD Level 0

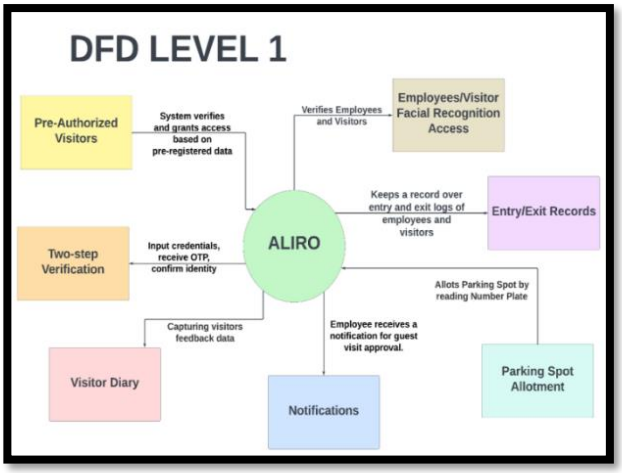

Fig.1 (b): DFD Level 1

B. Facial Recognition

Aliro's security infrastructure heavily relies on the Facial Recognition module, which utilizes cutting-edge machine learning algorithms to ensure that only authorized individuals

are granted access. This module uses CNN to analyze and process facial features, generating unique biometric signatures for each person. The system operates in real-time, enabling instant access decisions by comparing live facial images with data stored in the system. As the system is exposed to more data and feedback, the algorithms are continuously enhanced, improving their accuracy and reducing false positives and negatives. This adaptive learning feature ensures that the facial recognition technology remains reliable and effective under various conditions, including changes in appearance or environmental factors

C. Visitor Management

The Visitor Management module is designed to facilitate a smooth and efficient process for managing visitors from registration to departure. Upon arrival, visitors undergo a registration process that captures their personal information, visit purpose, and the employees they meet. The module tracks the visitor's movements within the tech park, managing permissions and updating their status in real time. Visitors receive notifications regarding their visit status, including approval or denial of access and any pertinent updates. Employees are also informed of their guest's arrival, enabling timely preparation. The system maintains a comprehensive log of visitor movements within the tech park, ensuring enhanced security and facilitating auditing processes. This streamlined system assures that visitors are well taken care of.

D. Vehicle Entry Management

The Vehicle Entry Management module optimizes vehicle access and parking within the technology park. When visitors arrive, the system uses high-resolution cameras to scan their license plate, utilizing optical character recognition (OCR) to process and identify the vehicle. Based on this identification, the system assigns a parking space in the visitor parking area. Visitors receive real-time information about their assigned parking spot via the app, guiding them to the designated area. This automated process reduces parking congestion and confusion, contributing to overall efficiency. By effectively managing parking resources, the system ensures visitors have a smooth and organized parking experience.

E. Visitor Diary

The Visitor Diary module enhances the visitor experience by providing a platform for feedback and community interaction. Visitors can submit reviews and comments about their experience, providing valuable insights into their visit. This feedback mechanism helps identify areas for improvement and promptly address any issues. Additionally, the module allows visitors to view feedback from others, fostering a transparent and collaborative environment. The Visitor Diary encourages open communication and engagement, creating a community-driven atmosphere. The insights gathered from visitor feedback are heard and actively utilized to continuously improve the app and enhance the overall visitor experience. This ensures that the system evolves to meet user needs and expectations.

IV. Results and Discussion

The process of detecting faces using the BlazeFace classifier in a mobile application, a versatile and adaptable tool, is outlined in this flowchart. It begins with accessing the camera and continuously verifying its availability. After successfully accessing the camera, a frame is captured, and the image is converted to grayscale. The BlazeFace classifier is then loaded to scan the grayscale image for facial features. If a face is detected, a rectangle is drawn around it, and the identified face is returned for further processing. The process loops back to capture a new frame if no face is detected. This cycle continues until the process is manually stopped or the camera is closed. Fig.2 shows the different flow of the current access detection process.

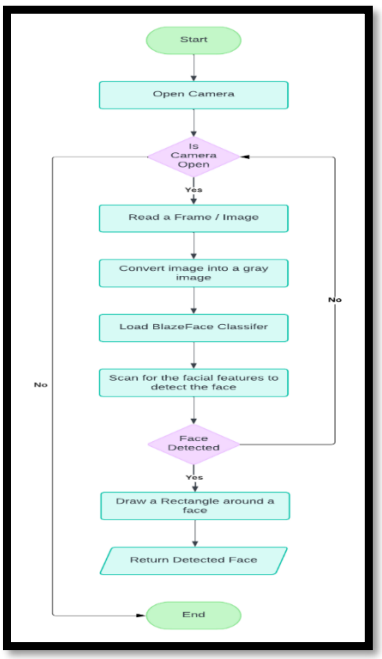

Fig.2(a): Face Detection Flow

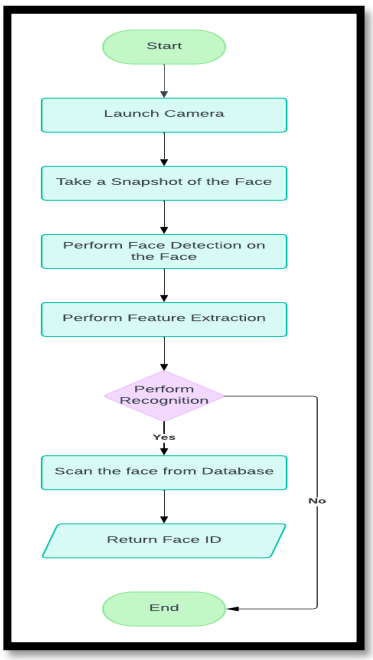

Fig.2(b): Face Recognition Flow

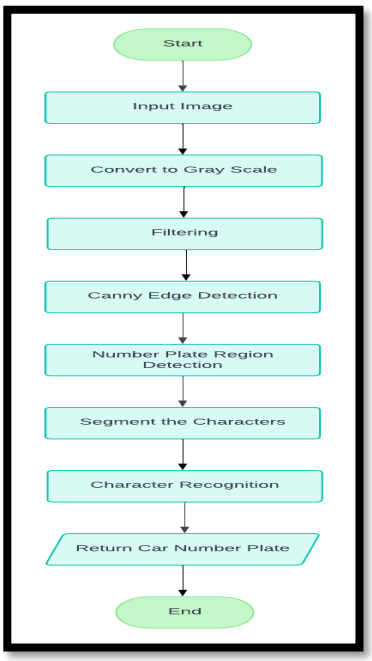

Fig.2(c): Number plate Recognition Flow

The face recognition algorithm starts by activating the camera to take a face snapshot. Once the snapshot is taken, the system performs face detection to locate the face within the image. Following this, feature extraction is carried out, which involves identifying and extracting key facial features such as the eyes, nose, and mouth. The algorithm then moves to the recognition step, where the extracted features are compared against a database of known faces. If a match is found, the system searches the database to identify the face and returns the corresponding face ID. If no match is found, the process does not return an ID. Finally, the process ends. The algorithm for recognizing a car number plate, an efficient and effective tool, begins with submitting an image, which is then converted to grayscale to simplify processing. Filtering is then used to eliminate noise and improve image quality, followed by Canny edge detection to identify the edges. The algorithm then identifies the number plate region using the highlighted edges, segments the individual characters within this region, and carries out character recognition using optical character recognition (OCR) techniques. Lastly, the recognized characters are combined to return the complete car number plate, concluding the process.

A. Functional Working

The functional working of Aliro, the advanced access control app for tech parks, is a seamless integration of multiple sophisticated technologies designed to enhance security and streamline access management. The system begins with a robust User Registration and Authentication module where employees undergo a one-time registration process, capturing and securely storing their facial data in a database. Visitors register each time they intend to visit, providing necessary details, which allows for pre-approval based on the employee's authorization. Upon arrival, the Facial Recognition module utilizes cutting-edge machine learning algorithms to verify identities in real time, ensuring only authorized individuals gain access. This module continuously learns and improves accuracy, adapting to changes in appearance and environmental conditions. The Visitor Management module efficiently handles the entire visitor lifecycle, from registration to exit. Visitors receive instant notifications about their visit status, including approvals and updates, and employees are notified when their guests arrive. This module maintains a comprehensive log of visitor movements within the tech park, enhancing security and providing valuable data for audits. Simultaneously, the Vehicle Entry Management module optimizes vehicle access by scanning number plates. The system automatically allocates parking spaces, guiding visitors to their designated spots and reducing congestion. Adding to the user experience, the Visitor Diary offers a platform for feedback and community interaction. Visitors can submit reviews and view comments from others, fostering a collaborative environment and encouraging continuous improvement based on real user experiences. The mobile-centric approach of Aliro ensures convenience and real-time communication, with users managing their access permissions directly through their smartphones. This integration of facial recognition, automated vehicle management, and mobile technology provides a comprehensive, secure, and efficient solution for modern tech parks, revolutionizing traditional access control systems.

V. CONCLUSION

Aliro revolutionizes access control for tech parks with advanced facial recognition, automated vehicle entry management, and mobile application capabilities. It replaces traditional methods with a secure, efficient alternative, integrating smoothly with existing systems. The system features robust user registration and authentication, visitor management, and vehicle entry management. It also includes a visitor diary module for feedback and operates on a mobile-centric approach, allowing users to manage access permissions and receive smartphone notifications. Aliro sets a new standard for access management in tech parks, ensuring security, organization, and productivity, and is scalable to adapt to changing needs.

REFERENCES

[1] Zhao, Z., Lin, P., Shen, L., Zhang, M., & Huang, G. Q. (2020). IoT edge computing-enabled collaborative tracking system for manufacturing resources in industrial park. Advanced Engineering Informatics, 43, 101044.

[2] Tan, L., Shi, N., Yu, K., Aloqaily, M., & Jararweh, Y. (2021). A blockchain-empowered access control framework for smart devices in green internet of things. ACM Transactions on Internet Technology (TOIT), 21(3), 1-20.

[3] Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), 4682-4696.

[4] Gupta, M., & Kumar, B. S. (2023). Lightweight secure session key protection, mutual authentication, and access control (LSSMAC) for WBAN-assisted IoT network. IEEE Sensors Journal, 23(17), 20283-20293.

[5] Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal, 8(14), 11717-11731.

[6] Bera, B., Saha, S., Das, A. K., & Vasilakos, A. V. (2020). Designing blockchain-based access control protocol in IoT-enabled smart-grid system. IEEE Internet of Things Journal, 8(7), 5744-5761.

[7] Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J., & Park, Y. (2020). BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE access, 8, 95956-95977.

[8] Xie, X., Zheng, L., Wang, R., & Gou, Z. (2024). Visitors' experience of using smart facilities in urban parks: A study in Shenzhen. Journal of Outdoor Recreation and Tourism, 46, 100759.

[9] Hanna, B., Vasyl, B., Mariia, B., Liudmyla, D., Tatiana, T., & Vitalii, P. (2024). Capacity for Innovation Frugal: The Look from Companies Incubated in Park Technology and Inco-Working Spaces. In Technology-Driven Business Innovation: Unleashing the Digital Advantage, Volume 1 (pp. 567-580). Cham: Springer Nature Switzerland.

[10] Qin, H., David, A., Harun, A., Mamun, M. R. A., Peak, D., & Prybutok, V. (2024). Assessing user benefits and privacy concerns in utilitarian and hedonic mobile augmented reality apps. Industrial Management & Data Systems, 124(1), 442-482.

[11] Zhang, Z., Mao, X., Zhou, K., & Yuan, H. (2020). Collaborative sensing-based parking tracking system with wireless magnetic sensor network. IEEE Sensors Journal, 20(9), 4859-4867.

[12] Yang, L., & Song, M. (2009). Formation Mechanism of Green Strategic Alliances and Its Cooperative System for Coal-Mining Eco-Industrial Parks Based on Synthetic Decision Support System. J. Comput., 4(11), 1109-1116.

[13] Tseng, M. L., Negash, Y. T., Nagypál, N. C., Iranmanesh, M., & Tan, R. R. (2021). A causal eco-industrial park hierarchical transition model with qualitative information: Policy and regulatory framework leads to collaboration among firms. Journal of environmental management, 292, 112735.