Use of Computer Vision for Access Control and Security at Accenture

Tanvee Proag, 2422814
under the supervision of Dr (Mrs) Maleika Heenaye-Mamode Khan
Faculty of Information Communication and Digital Technologies, University of Mauritius

Abstract

Computer vision proves helpful when it comes to creating unique features tailored to an organization's needs. This paper outlines a project that aims to help *Accenture Services Ltd.* improve the existing system by facilitating access control in the office and strengthening data security. A series of technologies and techniques are observed to conceptualize a system that enhances the existing one by relying on artificial intelligence applications. The aim is to decrease the dependence of physical badges that allow employees to unlock doors since they are not ideal, with the possibility of being lost or being shared, thus posing security risks. Computer vision, in comparison, provides the ability to allow access through facial recognition, enabling secure, badge-free access for employees.

Keywords: Facial Recognition, Access Control, Security, Camera System, Employee Verification, Computer Vision, Artificial Intelligence Applications

1 Introduction

1.1 Background Study

Accenture Services Ltd. is a consultancy firm in which the technology division is dedicated to address clients' software needs and deliver insights and solutions - that is, it involves helping organizations meet their current software requirements as well as set them up for future requirements. Accenture has always focused on how important it is to innovate and to be able to adapt in today's rapidly evolving business landscape, by having *Change* as its emblem. The solutions that Accenture offers to help businesses in their digital tasks are suited to their specific problems. Accenture approaches each challenge like so- it tries to have a comprehensive understanding of the latest technological advancements and then provides strategic guidance that aligns with the clients' goals. Basically, Accenture succeeds in staying competitive in this business environment by encouraging businesses to embrace new technologies. Therefore, it is perfectly aligned for Accenture to implement Computer Vision techniques which represent some of the most common and advanced artificial intelligence technologies available in the present day.

1.2 Problem Statement

The technology division of Accenture (*Software Development* and *IT Consulting*) can be considered as substantial because it has over hundreds of employees working a regular 9-to-5 seven days a week at the office located in Ébène, Mauritius. This means that Accenture has to span its office space over multiple floors - with each floor of the building only accommodating people from specific fields. For example, the common ground of floors *1*, *2* and *9* accommodate software developers of all ranks, that is, junior levels to senior levels. However, there are subsections of these floors (known as *Secure Bay*) that only a few select ranks can have access to. For now, these doors are controlled by a special badge access control system that uses a radio frequency identification technology. The proximity card reader is a touchless device that reads the credentials of a previously registered card when it is within the detection radius. This way, when an employee donning a badge gets close to the reader, it is scanned and the encoded information is read. Depending on whether that employee should or should not have access to that section of the facility, the magnetic door locks are activated or deactivated by the badge reader to grant or deny access.

Despite being modern and efficient, this technique of allocating a badge to each employee and expecting them to wear it on the neck at all times is not exactly ideal, instead it presents possible cases of misuse, intentionally or unintentionally. Firstly, an employee may misplace or lose their badge, leading to the security item potentially getting in the wrong hands. Secondly, am employee may abuse this system by unlocking the door and enter the room, followed by someone else who might not necessarily be allowed in. Accenture considers tailgating as a serious security offense. Additionally, if ever the situation arises that an employee needs temporary access to an area, the latter might need to physically call to Floor *6* to seek the security personnel of the organization for help. Floor *6* of the building includes a Help Desk for all employees as well as several server rooms that are highly confidential to the organization - An outsider getting access to one of these rooms would corrupt what Accenture stands for - the promise of safety and reliability of the handling of sensitive client information.

1.3 Literature Review

Computer Vision Based Employee Activities Analysis [Alom et al., 2014] presents a real-time face recognition system designed to automate employee attendance and monitor work hours in an office setting. The proposed system addresses problems caused by traditional methods by using a Haar cascade classifier for face detection and Principal Component Analysis (PCA) for face recognition, assessing the time employees spend at their workstations. Three components - a local server application, a web application and a mobile app - allow administrators to view attendance and work hour reports remotely thus improving management transparency. At the Sevastopol State University of Russia [Zhilenkhov, 2021], an analysis of computer vision technologies in the field of face recognition in a digital video signal is observed and analyzed. In *Facial Recognition Attendance Scheme on CCTV cameras using open computer vision and deep learning* [Kagona, 2022] a facial recognition-based attendance system using CCTV cameras, OpenCV and deep learning is explored. Face recognition through face embeddings and deep metric learning involves face detection, feature extraction and face comparison steps. The legacy system was analyzed to gather requirements for the new system which was developed using HTML, Bootstrap and the Django framework. Finally, the system was tested, validated and deployed in an attempt to improve attendance tracking accuracy with live monitoring capabilities. *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face* [Metz, 2019] uses a technology learns how to identify people by analyzing as many digital pictures as possible using "neural networks," which are complex mathematical systems that require vast amounts of data to build pattern recognition.

1.4 Proposed Solution

In an attempt to improve on this existing system, a new approach using computer vision to detect the presence of an employee might be more efficient. A camera installed at each entrance could use facial recognition to scan an employee's face in real time, check it against stored data and then take the decision of unlocking the door or not depending on whether the identity is verified.

2 Data Requirements

For the implementation of the computer vision techniques, a variety of data is needed to ensure the face recognition and real-time detection are reliable.

Employee data needed are high-resolution and front-facing image to train the facial recognition model. It would be ideal to collect multiple images per employee, each under different lighting conditions and angles. Accenture already has a unique identifier for each employee and this shall be used to associate each face with an employee found in the database. Each ID is linked to the employee's other details, such as name, department and role. This facilitates generating reports and access logs. For role-based restrictions, access permissions are to be defined, that is, which employee gets to have access to which areas.

To train the model, a large training dataset of labeled images is required. There are LFW (Labeled Faces in the Wild) and MS-Celeb-1M publicly available that can be used as base model. Then, FaceNet or DeepFace deep learning models could create facial embeddings, that is, numerical vector representations of each face.

To better detect anomalies, some behavioral data might be required. Time-stamped data of entries and exits for each employee (Entry-Exit Logs) would help in tracking patterns and unusual activities. Video footage from restricted areas would help for training and testing the system's real-time behavior and movement detection. Labeled examples of abnormal behavior, such as loitering, tailgating or unauthorized access attempts, to train anomaly detection models. These could be manually labeled or collected over time. To demonstrate these abnormal behavior for testing, labeled examples of these need to be provided.

To test and fine-tune the model for different environments, images and video samples taken under different lighting conditions - day, night, indoor tube lights - can be collected. The model can be trained to accurately detect the presence of employees and identify them in varying scenarios by having footage showing different crowd levels.

Data about access control, that is rules and permissions that define who can enter specific areas at what times, is required to give or deny access to every individual to each room. Some employees might have access only during work hours which would make data about time-based access permissions a requirement.

To identify issues and improve accuracy, logs of unsuccessful recognition attempts, access denials and data on system usage patterns can be collected.

3 Methodology

Firstly, for the hardware components, high-resolution cameras with Infrared capabilities that work well in low-light conditions are needed to capture clear images of the face. Small but powerful edge devices like NVIDIA Jetson Nano and Google Coral can be used to process data locally. This improves privacy and reduces latency. As for servers, the *Accenture Cloud First* and *Momentum Digital Transformation Platform* cloud-based platforms that serve as centralized repositories to store and manage a wide array of data including operational reports, client information and analytics can be used.

Secondly, for the software components, facial recognition libraries are to be used. OpenCV provides basic facial detection which can be combined with deep learning models for facial recognition. Dlib's `get_frontal_face_detector` is good for the detection and matching of faces. FaceNet and DeepFace map faces to embeddings (128-dimensional vectors) which makes it easier to compare faces by calculating Euclidean distances. Accenture collaborates with Microsoft Azure, Amazon Web Services and Google Cloud for data storage solutions that can be used as datasets for analytics and machine learning. For cloud-based facial recognition, Microsoft Face API and AWS Rekognition can recognize faces, detect emotions and identify individuals with high accuracy. For real-time detection, YOLO (You Only Look Once) is an object detection algorithm that is fast and hence suitable for real-time applications. It can be trained to detect individuals in restricted areas and recognize specific behaviors like tailgating. An alternative would be SSD (Single Shot MultiBox Detector) real-time object detection model as it is faster than YOLO but it is less accurate so it would perform better in detecting and counting people in crowded areas. The OpenPose activity and behavior recognition identifies human posture and can detect specific actions like loitering or unauthorized movements which might indicate suspicious behavior detected. Optical Flow Analysis tracks the movement of individuals over time which is useful because continuous tracking is required to detect suspicious activity and monitor entry-exit patterns. Algorithms like PointNet can verify if the face detected is three-dimensional to know if it is a real person or a two-dimensional picture thus helping prevent spoofing. Additionally, Dlib and OpenCV can be used to detect blinks and slight head movements to ensure that the face detected belongs to a live person.

Next, for the frameworks and machine learning, TensorFlow deep learning framework can be used for training custom models for facial recognition and anomaly detection. Integrating the Keras API with TensorFlow facilitates building and training models quickly. Scikit-learn offers clustering or classification algorithms that can be implemented for anomaly detection or behavior analysis. For edge computing with low-latency requirements, MxNet can be used.

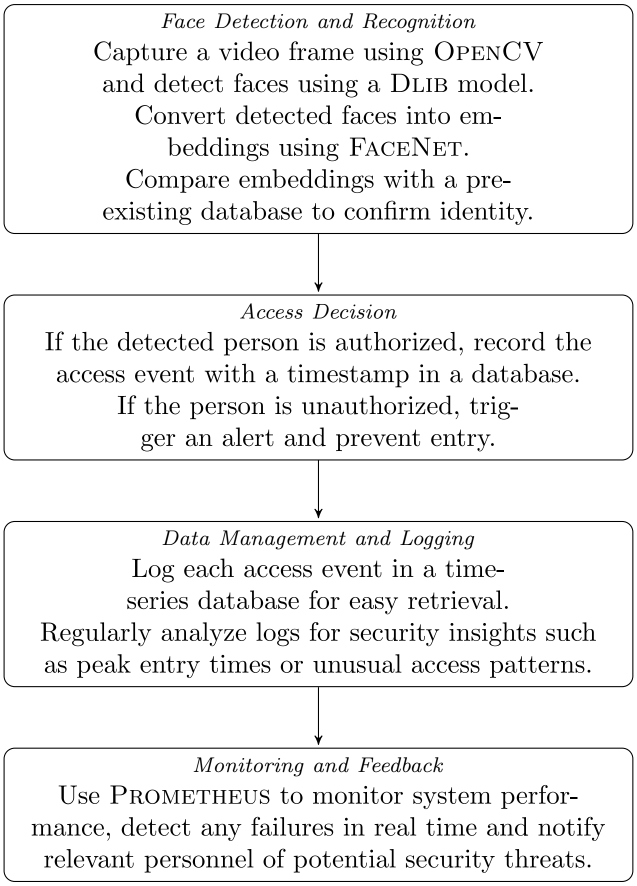
The databases to be used are an important consideration for the data management. SQL Databases like MySQL, PostgreSQL and SQL Server can store structured access logs, timestamps and employee data. NoSQL Databases like MongoDB and DynamoDB can store unstructured data such as images or JSON-like data of facial embeddings. Time-Series Databases like InfluxDB and TimescaleDB can track real-time access patterns and monitor entry-exit data. This is useful for generating security reports and auditing purposes.

To integrate the access control systems, REST APIs can be used to communicate between the facial recognition software, access control systems, cloud storage and local databases. However, queries like fetching historical access logs or querying specific timestamps can be more complex. For these, GraphQL can be used to facilitate data retrieval.

Additionally, privacy is crucial to Accenture which claims to attach great importance to people's right to privacy and the protection of their personal data. Sensitive data such as facial embeddings and personal information must be encrypted at all times. Libraries like OpenSSL and built-in encryption in cloud providers (AWS KMS and Azure Key Vault since Accenture collaborates with Amazon and Microsoft) can be used. Implementing Role-Based Access Control (RBAC) within the database and application to control access to sensitive data strengthens the security aspect as it allows only authorized personnel to have access.

Finally, to track the system health, detect failures and ensure that the system is running as expected, logging frameworks like ELK Stack (Elasticsearch, Logstash, Kibana) or Prometheus/Grafana can help. Regular compliance checks can be done to ensure automated data retention policies, consent tracking and audit logs are monitored.

The workflow is illustrated below.



Face Detection and Recognition

Capture a video frame using OpenCV and detect faces using a Dlib model. Convert detected faces into embeddings using FaceNet. Compare embeddings with a pre-existing database to confirm identity.

Access Decision

If the detected person is authorized, record the access event with a timestamp in a database. If the person is unauthorized, trigger an alert and prevent entry.

Data Management and Logging

Log each access event in a time-series database for easy retrieval. Regularly analyze logs for security insights such as peak entry times or unusual access patterns.

Monitoring and Feedback

Use Prometheus to monitor system performance, detect any failures in real time and notify relevant personnel of potential security threats.

4 Expected Results

The results to be expected after the successful implementation of this computer vision-based access control and security system in the workplace include better security and more efficient monitoring of employees. Authorized employees can unlock doors and have access to secure rooms without physical access cards, using face recognition. This reduces heavy reliance on key cards and prevents issues from lost card or card sharing. To achieve high accuracy in identifying employees and matching them with stored profiles, a low false acceptance rate (FAR) and false rejection rate (FRR) would be ideal. The system is expected to do quick and efficient processing, that is, it should recognize and grant access within a second or two for smooth workflow, avoiding delays at doorsteps. After accurately identifying unauthorized attempts (e.g., visitors, former employees), the system should prevent access and trigger alerts to the security personnel on Floor 6. The alerts should also indicate if the system has identified security risks like tailgating (following an authorized person through a door) or loitering around. The security personnel can respond quickly as the system provides real-time notifications and alerts for any unauthorized access attempts, unusual movements and unexpected behavior. Over time, the system can identify patterns like frequent access to sensitive areas or high entry times and it can provide insights into building usage and employee routines. The system is anti-spoofing as it can differentiate between live images and photographs. Automated logging of each access attempt - including timestamp and entry location - facilitates tracking and auditing of access history. This can help with investigating security incidents and auditing workplace policies. The system being automated helps minimize human error and bias and since the organization no longer heavily relies on security personnel, operational costs will go down. The data collected on traffic patterns can help with space planning, facility management and adjusting staffing or resource allocations during peak hours. The evaluation of the performance of the system can be done through some key metrics. They include high accuracy rates in correctly identifying authorized personnel and denying access to unauthorized ones. The speed of recognition is important as the system should process each access attempt in under two seconds to not cause delays especially during peak times. The system should be convenient and reliable to ensure employee satisfaction. Additionally, regulatory compliance is essential to ensure that the system respects the data privacy laws of Accenture.

5 Discussion

Overall, the proposed computer vision-based access control and security system presents a modern and efficient solution to improve workplace security by automating access and improving monitoring capabilities. As for the feasibility of this system, it shows strong potential to manage access control of employees and perform monitoring while following security protocols. It presents multiple benefits such as fast facial recognition, automated entry logs and real-time security alerts which align well with Accenture's needs for efficiency, security and innovation. However, there may be some challenges during the implementation phase. Facial recognition is to be done under varying lighting conditions and for individuals with minor facial changes (e.g., glasses or facial hair). Achieving high accuracy may require fine-tuning, additional data and investment in specialized cameras that can handle low-light conditions. The use of biometric data, that is, facial recognition, may raise concerns about data storage, security and monitoring among employees if the latter are not clearly made aware of the data handling practices, security protocols and compliance with privacy regulations. As long as the project focuses on careful planning and clear policies, it has the potential to be highly successful by not only strengthening workplace security but also facilitating access control, creating a safer and more efficient environment for all employees in the organization.

6 References

1. Metz, C. (2019) 'Facial Recognition Tech Is Growing Stronger, Thanks to Your Face', International New York Times, 17 Jul, NA, available: https://link.gale.com/apps/doc/A595686848/AONE?u=anon~3679307e&sid=googleScholar&xid=60072740 [accessed 28 Oct 2024].

2. Kagona, E. (2022). Facial Recognition Attendance Scheme on CCTV Cameras Using Open Computer Vision and Deep Learning: A Case Study of International University of East Africa (IUEA). Advanced Journal of Science, Technology and Engineering, 2(1), pp.1–27. doi:https://doi.org/10.52589/ajste-hyvtcz9e. Available at: https://www.researchgate.net/publication/362584411_Facial_Recognition_Attendance_Scheme_on_CCTV_Cameras_Using_Open_Computer_Vision_and_Deep_Learning_A_Case_Study_of_International_University_of_East_Africa_IUEA

3. Alom, Z., Karim, N.T. and Rozario, S.P. (2014). Computer Vision Based Employee Activities Analysis . International Journal of Computer and Information Technology , Volume 03 – Issue 05 (ISSN: 2279 – 0764) Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=31e8054f53cf536bc32c9815d90d4d9b81cc451e.

4. Zhilenkov and Shumeyko (2021). Analysis of Computer Vision technologies in the field of face recognition in a digital video signal. [online] eLIBRARY.RU. Available at: https://www.elibrary.ru/item.asp?id=46140949 [Accessed 28 Oct. 2024].

5. Privacy Statement — Accenture (2024). Privacy Statement — Accenture. [online] Accenture.com. Available at: https://www.accenture.com/us-en/support/privacy-policy [Accessed 28 Oct. 2024].

6. www.accenture.com. (n.d.). Information Security — Accenture. [online] Available at: https://www.accenture.com/us-en/services/technology/information-security.

7. Narain, K. and Guan, L. (2022). A New Dawn for Dormant Data. [online] Accenture Cloud Data Value: A New Dawn for Dormant Data. Available at: https://www.accenture.com/content/dam/accenture/final/capabilities/technology/cloud/document/Accenture-Cloud-Data-Value-A-New-Dawn-for-Dormant-Da pdf [Accessed 25 Oct. 2024].

8. . www.accenture.com. (n.d.). Accenture and Amazon Web Services take you further, faster. [online] Available at: https://www.accenture.com/us-en/services/cloud/aws-business-group [Accessed 25 Oct. 2024].

9. www.accenture.com. (n.d.). Accenture Momentum. [online] Available at: https://www.accenture.com/us-en/services/consulting/accenture-momentum [Accessed 25 Oct. 2024].