ISS: Intelligent Security System Using Facial Recognition

Rajesh Kumar Verma[1(✉)], Praveen Singh[2], Chhabi Rani Panigrahi[3], and Bibudhendu Pati[3]

[1] Infosys Limited, Hyderabad, India
Rajeshverma_chicago2004@yahoo.com
[2] HSBC Limited, Bengaluru, India
praveenhelp78@gmail.com
[3] Department of Computer Science, Rama Devi Women's University, Bhubaneswar, India
{panigrahichhabi,patibibudhendu}@gmail.com

Abstract. Security is mandatory and of utmost importance for all organizations. While the legitimate people should be allowed inside enterprises, the illegal ones should be barred from entering and this can be achieved using face recognition techniques. In this work, we have come up with a robust architecture using artificial intelligence and Internet of things that can be used across different enterprises. We have also derived the methodology and solution for implementing a more advanced security system. For proper demonstration, we have also considered one of the business use cases along with proposed processing work flow.

Keywords: Security · Face recognition · Artificial intelligence · Internet of things (IoT) · Big data · Mobile devices

1 Introduction

Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) technologies are broadly applied while developing any intelligent security system. In the past around 20 years back, people used to develop rule-based security system which was very much complex and there was hardly any intelligence. For every scenario, you need to define scenario and corresponding action.

In this work, we have proposed the architecture for modern intelligent security system, which comprises of Internet of things (IoT), cloud technologies and AI/ML/DL along with big data.

The rest of the paper is organized as follows. In Sect. 2, we will discuss about the related work, Sect. 3 discussed proposed architecture framework and steps taken to reach the solution discussed, business use case and work flow in Sect. 4 followed by conclusion in Sect. 5.

C. R. Panigrahi et al. (eds.), *Progress in Advanced Computing and Intelligent Engineering*, Advances in Intelligent Systems and Computing 1198, https://doi.org/10.1007/978-981-15-6584-7_10

2 Related Work

In this area of security using AI, a plethora of work has been done in designing the security system. In [1], the authors have proposed a car theft prevention system using face recognition in IoT-based home automation. They have used controller and RFID transmitter and receiver to secure the car in home along with controlling their home appliances through communication protocol. Face recognition system is being used to check the entered person in home and the person trying to drive a car is authorized or unauthorized.

Jose et al. [2] have proposed the device fingerprinting algorithm in order to improve the home automation security, and the paper highlights various security issues that are associated with modern smart homes. In the subsequent paper Jose et al. [3], have further improvised the smart home security system by introducing the behaviour prediction algorithm, which uses the required parameters to predict the behaviour of users. The proposed algorithm learns through several weeks of training data and is based on the knowledge it gains from the naïve Bayesian network.

In [4], author proposed a IoT-based SmartBots using MCC and big data technology, and the paper describes the architecture which is used as a base framework for building smart and advanced city using IoT devices. It provides the intelligent solution to the users in a real-time manner by use advanced tools available in the analytical market.

In Singh et al. [5], have proposed an architecture for running of resource intensive jobs on the cloud, in which off-loading to the cloud is the major feature used for faster computation. The integration of IoT devices and big data is highlighted in this paper wherein big data is used as the storage medium for the humongous data generated by the IoT devices over a period of time.

3 Proposed Architecture Framework

In this section, we present the proposed architecture framework for ISS using facial recognition, in order to discover the genuine people who work for the particular enterprise. The system then allows the person to enter into the premises of the enterprise.

In Fig. 1, the high-level architecture diagram of the proposed ISS has been depicted. The input to the system comes from either the IoT devices, like camera, or any user device, like mobile phones, and subsequently sent across to the cloud. The input images are further sent to the AI/ML/DL layer where the algorithms are hosted and help in identifying the similarity between the captured image and the original image stored in the system. The big data layer is used to store huge volumes of data and require parallel and distributed computing for further processing. The security team can monitor the entire process through the data which is being monitored.

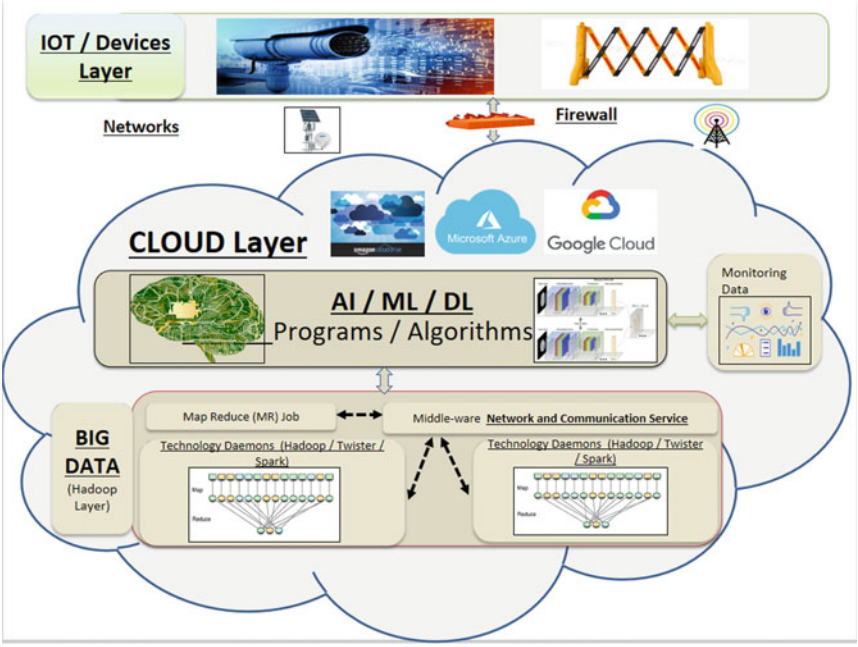

Fig. 1. Proposed intelligent security system architecture

3.1 SIAMESE Algorithm for Face Similarity Detection

SIAMESE neural network (SNN) [6] is an artificial neural network(ANN) which uses the measure of similarity for recognizing similar faces, handwritten checks, etc.

The most popular application of SNN is face recognition [8], wherein the images of people are pre-computed and subsequently compared to the image which comes from the IoT device at the security entrance of a particular company. SNN helps to recognize the legitimate person amongst a large number of persons. Popular example of SNN application is **DeepFace** [7] which is a deep learning facial recognition system created by Facebook and identifies the human faces in digital images. This system uses a neural network(NN) having 9 layers and 120 million weights and was trained on 4 million Facebook images. We have used SNN in our work for facial recognition and similarity comparison.

3.2 Solution Flow

Figure 2 shows the various modules in the architecture. Here, the related historical data is stored in the system and the new image is captured by the devices. Both the images are sent across the different layers and subsequently the similarity between them is detected.

Error correction system facilitates enterprises to ensure the level of security and advancement of the same by applying IoT, AI/ML/DL, facial recognition and big data.

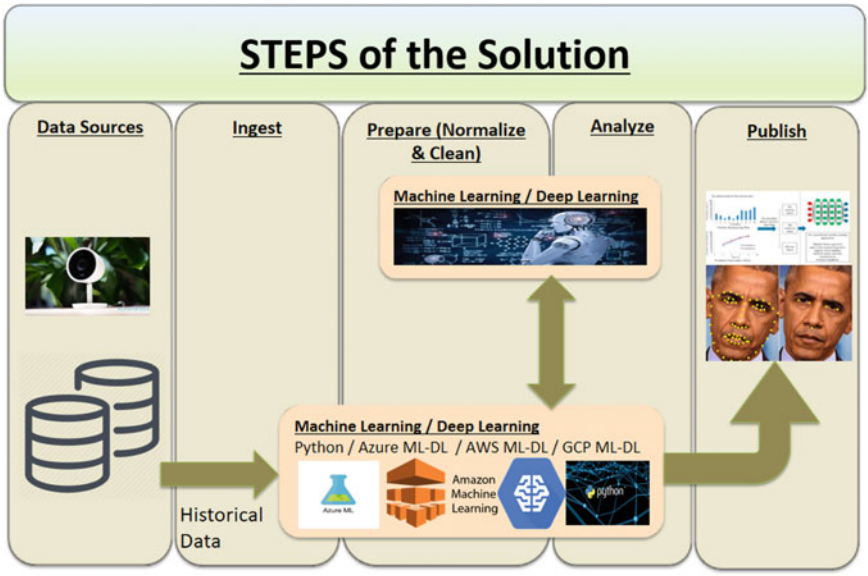

Fig. 2. Steps of solution

The different steps followed in execution of the ISS used in making ISS are explained below:

1. The current image of the person at security gate is captured using the cameras. Historical data is also used which was captured at an earlier date. Both the current and earlier data are passed to the next stage for further processing.
2. The data captured from the camera device as well as the historical data is now made available to the next module for the subsequent processing.
3. The images are now further processed (normalized) and the CNN-based algorithm is now applied to these images, which helps to detect the similarity between the edges of the faces.
4. The important features are extracted and help to recognize the person and the percentage of similarity is given by the system.
5. Identify the positive and negative signals.
   (a) find edges, coordinates of existing knowledge base to real-time object on the surveillance.
   (b) otherwise, find the similar pattern and their matching from the central repository present in the cloud.

6. fetch the coordinates and tag to each new object and to avoid the future load.

In this paper, we focus on the feature engineering based on historical data and IoT devices data. It can be categorized as a classification problem which helps to detect the similarity between faces.

4 Business Use Case and Work Flow

Figure 3 depicts the work flow for ISS starts with the particular person who arrives at the front security gate for entry into the premises of the company. Subsequently the IoT devices will take the photograph of the person for subsequent processing to detect the similarity with the reference image stored in the enterprise system. The intelligent module then analyses the captured image in reference to the image which is originally present in the repository. Upon successful identification of the captured image, the person is permitted entry into the premises of the enterprise. In case the person is detected as a fraud case, the entry is prohibited. At regular interval(can be daily, weekly or monthly), the monitoring report is generated and tracked by the security department.

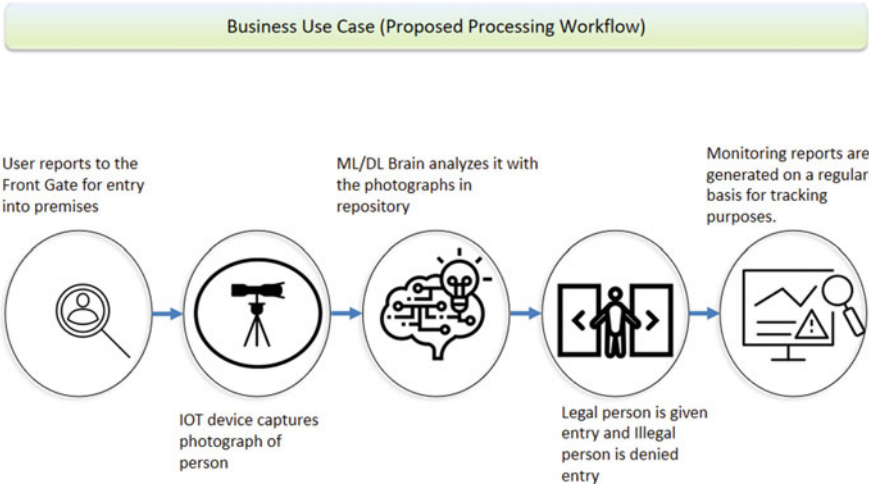

Fig. 3. Steps of solution for the business use case

5 Conclusion

Security systems using face recognition are being used at all places and are the emerging trend of the day. The uses of intelligent algorithms and big data enhance the approach of the applications for all types of organizations. The

architecture discussed in this paper is classified under the face recognition category, where the functioning of the system is mainly dependent on the image repository, applied intelligent algorithm, loading and off-loading to the cloud for processing. This architecture is robust as it can be modified and optimized based on the needs. We also provide the end-to-end process along with work flow of any security-based application.

References

1. Rajalakshmi S, Tharani R, Newlin Rajkumar M, Harshani PR (2017) IOT based smart home automation for car theft prevention using image processing. Int J Trend Sci Res Dev, pp 1307–1311
2. Jose AC, Malekian R, Ye N (2016) Improving home automation security; integrating device fingerprinting into smart home. IEEE Access 4:5776–5787
3. Jose AC, Malekian R, Letswamotse BB (2018) Improving smart home security; integrating behaviour prediction into smart home. IJSNet 28:253–269
4. Singh PK, Verma RK, Krishna Prasad PESN (2019) IoT-based smartbots for smart city using MCC and big data, smart intelligent computing and applications. In: Smart innovation, systems and technologies, vol 104. Springer, Singapore, pp 525–534
5. Singh PK, Verma RK, Sarkar JL (2019) MCC and big data integration for various technological frameworks., progress in advanced computing and intelligent engineering. In: Advances in intelligent systems and computing, vol 714. Springer, Singapore, pp 405–414
6. Koch G, Zemel R, Salakhutdinov R (2015) Siamese neural networks for one-shot image recognition. In: Proceedings of the 32nd international conference on machine learning, Lille, France
7. https://en.wikipedia.org/wiki/DeepFace
8. https://medium.com/swlh/advance-ai-face-recognition-using-siamese-networks-219ee1a85cd5