Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8750840, 11 pages
https://doi.org/10.1155/2022/8750840

Research Article

Artificial Intelligence-Powered Contactless Face Recognition Technique for Internet of Things Access for Smart Mobility

Nirmala Hiremani,[1] Mohammad Kamrul Hasan,[2] T. G. Basavaraju,[3] Shayla Islam,[4] Dabiah Alboaneen,[5] Entisar Alkayal,[6] Nesreen M. Alharbi,[7] Zulkefli Mansor,[2] and Sanaz Amanlou[2]

[1]*Department of Computer Science and Engineering, Visvesveraya Technological University, Karnataka, India*
[2]*Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia*
[3]*Department of Computer Science and Engineering, Government Engineering College, Karnataka, India*
[4]*Institute of Computer Science and Digital Innovation, UCSI University, 56000 Kuala Lumpur, Malaysia*
[5]*Computer Science Department, College of Sciences and Humanities, Imam Abdulrahman Bin Faisal University, P.O. Box 31961, Saudi Arabia*
[6]*Department of Information Technology, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Rabigh 21911, Saudi Arabia*
[7]*Information System Department, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Rabigh 21911, Saudi Arabia*

Correspondence should be addressed to Mohammad Kamrul Hasan; mkhasan@ukm.edu.my and Shayla Islam; shayla@ucsiuniversity.edu.my

Received 4 April 2022; Revised 21 July 2022; Accepted 26 August 2022; Published 16 September 2022

Academic Editor: Kuruva Lakshmanna

A contactless system became necessary for smart mobility during the COVID-19 pandemic. There are many touchpoints in private and public areas where contact is essential, such as intelligent transportation systems for vaccine carriers, patient ambulances, elevators, metros, buses, hospitals, and banks. A secured contactless device reduces the chances of COVID-19 infection spread. Several devices use smart cards, fingerprint identification, or code-based access. Most of these devices require some form of touch. The cost of such devices varies, depending on their capability and intended use. Sensors developed by using artificial intelligence (AI) to provide secured access are an emerging area. This paper presents an AI-powered contactless face recognition system. The solution has the Internet of Things (IoT) enabled access system. To identify a person, it uses AI assistance for face recognition with the help of Python Dlib's facial recognition network. Dlib offers a wide range of functionality across several machine learning sectors and is open-source. The Arduino Uno (ATmega328P) and STK500 protocol has been used for communication to testify and validate the performance of the proposed technique. The objective is to detect and recognize faces by the proposed contactless approach. The obtained result shows 92% accuracy, 94% sensitivity, 96% precision and FRR 6% for face detection. There is a significant improvement in FRR in our work compared to the published 27.27%. The implemented solution in this paper provides accurate and secure contactless access to conventional, readily available techniques in public health safety.

1. Introduction

Paper ticket-based access has been for decades, and then came smartcards.

A smartcard comes with embedded memory and microprocessor chips with data storage. At the touchpoint, the chip on the card reads signals. The data transmission separation for smartcard systems is up to 15-30 cm.

One of the risks of the smart mobility for daily living in public places, and organizations, workplaces is the possibility of exposure to infection of the COVID-19 virus.

To prevent this risk, an initiative to remove the challenges of infection is required. Essential steps to make safe mobility, return employees to the workplace, and maintain standard health and safety involve contactless interaction.

These comprise the contact tracing application to provide organizations with a rapid COVID-19 identification and response system. The solution uses data from the patient, vaccine transportations, and workplaces–such as meeting participants, badge scans, on-location WiFi access points, and other sources–to help employers rapidly identify that may have been exposed to an infected person while onsite. Several contact tracers are employed thru case management to reach out to all potentially impacted employees. But this is costly and is an afterthought once the infected person has already contacted a touchpoint. So, touchpoints like the door lock, as shown in Figure 1, or badge access, as shown in Figure 2, are vulnerable.

Technological advances enabled access badges to identify the person who owned the badge. The commonly adopted technologies in access badges are magnetic stripes, smart cards, proximity barcodes, and biometric devices. There is an urgent need to enable the touchpoint to be contactless.

Therefore, this paper intends to propose an alternate technique and evaluate the advantages of such a solution regarding the current state-of-the-art contactless system. Targeted users will be using IoT-based identity validation for easy access. With a smartphone, users will be able to get access to a facility's remote control with the help of a secured digital identity.

In particular, the work relies on AI and IoT, two leading-edge technologies. The solution is good for home, office, and public place access applications and is contactless identity access. The motivation for the work is the adverse impact of touch-based systems during the COVID-19 era in public places where the contact person who previously used the system is unknown. In the present work, the proposed access system has three features; AI-based deep learning system uses the smart contactless camera. This system allows us to detect a person without any contact. Once the system detects the person, it looks for the access rights for the identified person. This is a system background validation process. Based on the access rights, an access code is generated and provided to the IoT-based lock for validation. In parallel, a one-time password (OTP) is sent to the mobile phone of the registered matching user.

Once the system blinks the green light, the user must enter the OTP to the devices using the IR code using the smart application. The advantage of the process is that at no point is there any contact or touch required. The OTP will be sent to the registered mobile phone only. OTP-based access can be an optional feature for the low-security area. The key advantage of this proposed design is that it is portable and easy to deploy.

Figure 1: Electronic keypad combination lock, La Gard, USA [1].

Figure 2: Access badge [2].

In this work, special attention was paid to identifying the person using an IoT smart camera. Further analysis was carried out on the OTP transmission for the validation of the person. The whole process involves no public touchpoints, thereby reducing the risk of COVID-19 spread.

The remainder of this paper is as follows: Section 2 presents related work on contactless access devices. Section 3 highlights the importance of contactless access devices; Section 4 describes the methodology; Section 5 put forward the proposed design of the system; Experimental settings and results with analysis are discussed in Sections 6, 7 and 8; Finally, Section 9 concludes and sets future work.

2. Literature Survey

Recently, many places, such as offices, parking, public transportation, etc., use an access control system for smart mobility where the access badges are programmed with a number called the facility code that is read by the card reader. The number read by the card reader is sent to the access control system that makes access-control decisions based on information about the credential. If the supplied credentials match those in the access control list, then the access control is unlocked [3]. High-quality professional badges with an easily identifiable photo and equipped with customizable digital information (barcode, magnetic tape, electronic chip, RFID chip) are readily available on the market [4].

Since we aimed to search for contact with less access, we explored the origin and current state of the art of contactless access devices [5, 6]. Botha et al. outlines the extensions for digital badging in a resource-constrained environment in the Nciba district in the Eastern Cape, South Africa. The

initial implementation was aimed at using Mozilla open badges but ended up with alternative methods. In conclusion, a case for an alternative mechanism was used to include end-users in a resource-constrained environment [7].

Quaddah et al. presented the difficulties of IoT-enabled security. In IoT access control systems, these systems communicate via wireless. An authorization-compliant smartphone could access electronically and control [8]. Andaloussi et al. discussed access control and authentication mechanisms supporting the cryptography algorithms in constrained devices [9].

Another interesting paper from Ali et al. presents challenges to traditional security solutions such as cryptographic solutions, authentication mechanisms, and key management in the IoT. The authors provide the threats at different layers and layer-wise security [10].

Voulodimos et al.'s work on deep learning for computer vision is relevant to the work we wanted to pursue in computational intelligence [11]. Ouyang et al. presented object detection with deformable part-based convolutional neural networks [12]. Verdhan presented learning hierarchical representations for face verification with convolutional deep belief networks [13]. Chen et al. discussed a high-dimensional feature and its efficient compression for face verification is a great motivation [14].

3. Key Issues of Existing Solutions

With our literature survey, the problem statement derived as motivation for the work is to have a secured contactless-access system. The technology is still in its early stages of adoption and can be improved as the system's learning progresses. The proposed system should have a solution to the following key issues:

(i) Contactless accessibility

(ii) Using smartphones instead of any other touchpoints

(iii) Secured identity access credentials with the simplest method to update without a touch point

(iv) Access only on a line of sight to avoid hacking, proxy

(v) Real-time validation of access requests

(vi) No physical smart card to minimise the risk of impersonation

4. Related Works

4.1. Transportations. In today's urban environment, smart infrastructure deployment and a touch-free transportation system are required to facilitate by eliminating the costly part of public-facing ticketing devices. This could involve minimizing ticketing windows, which in turn helps cut costs on staff and ticket devices, or operating different methods required to provide travelers with a travel token.

4.2. Office Environment. Now, more than ever, we need innovative solutions through partnerships, and our ability to scale innovations will require unprecedented coordination and communication. For the safety of employers, companies need to invest in contactless technologies to stay away from disease transmission. Also, through technology, it is possible to alert employees via mobile phones regarding social distancing and employee movement tracking.

4.3. Public Places. A touch-free system eliminates the requirement to line up to access a public place and provides an improved experience. The public will take this as more beneficial for the use of public facilities if a touchless approach is introduced.

4.4. Home. During the pandemic, contactless delivery of goods, medicines, and other services is done to reduce the risk of infection. In this process, a customer does not have to be in the pharmacy or other facilities at any point to avail these services. During delivery, the messenger will place the products at the door, step back to a safe two-meter distance, and wait for the customer.

4.5. Retails. The retail industry is using checkout-free retail with technologies such as Scan-and-Go mobile and artificial intelligence. Visitors can visit the retail outlet, use smart cells, scan QR codes or bar codes, put the purchase in a basket, and make the payment using mobile applications. The abovementioned area of contactless needs engineering implementation of AI and IoT. In the current work, we proposed one implementation with the addition of an innovative approach for Infra-Red (IR) based access code validation.

Table 1 shows the prevailing techniques for smart access systems and its main features and weaknesses. As can be seen from the table, most of the existing techniques have a limitation of image-based KYC validation and poses a chance of spreading infection because of the use of public touchpoints.

5. Materials and Method

To propose an alternate low-cost solution for high-performance face detection, we have considered using Arduino for IoT implementation and deep learning AI for image detection. The following two subsections will provide a brief overview of IoT and AI for face recognition. Since the scope of the work is on secured access using face detection, only the relevant theoretical background is included in these sections.

5.1. IoT. The IoT is a system of interrelated devices (mechanical, electrical, digital, computer, mobile), living and nonliving objects that are supplied with unique identifiers (UIDs), and possess the capability to transmit data over a network without the need for a human or machine command to initiate the transfer [15].

An IoT-enabled device is programmed in such a way that it can initiate data transfer through an IoT gateway in the event of the onset of a scheduled event [16]. For example, an IoT camera may capture a moment when there is movement around the premises and send it to the desired device, such as a mobile phone (Figure 3). During the whole process, from obtaining the photo to delivering it to the programmed destination device, no human or machine direction is involved.

Table 1: Summary of related existing techniques.

Techniques	Features	Weakness
Barcode	Contactless	Copied easily, security issue
Magnetic tape	Touchpoint needed	Can spread infection
Electronic chip	Touchpoint needed	Can spread infection
RFID chip	Contactless	Image verification not possible
OTP authentication	Contactless	Image verification not possible
Biometric	Touchpoint needed	Can spread infection

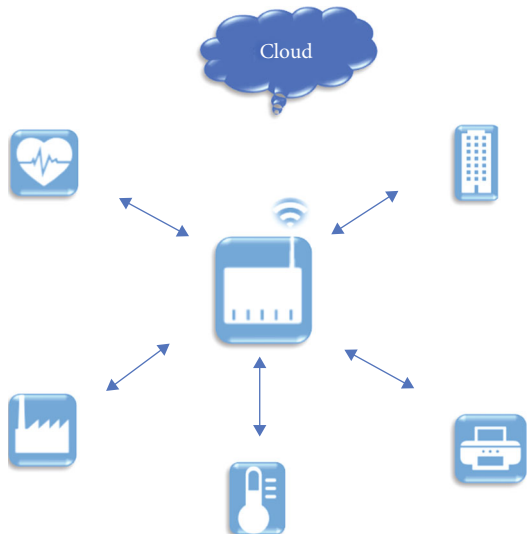

Figure 3: IoT applications.

Across the world, businesses are using the IoT for improving efficiency and decision-making for customer-oriented services [17, 18].

For some time, several IoT standards for communication have been in use, such as IPv6, ZigBee, and OneM2M. However, the most used OneM2M is a machine-to-machine service protocol for devices to communicate with each other. An open-source advanced message queuing protocol (AMQP) is also in use for IoT devices. Commercial off-the-shelf IoT frameworks for IoT enablement of services are Amazon Web Services (AWS), Google's Brolo/Weave, Arm Mbed, and Microsoft's Azure IoT Suite. An open-source IoT platform, Calvin from Ericsson, also provides required development and runtime libraries [19–27].

5.2. AI and Deep Learning. AI-powered technologies are behind recent innovations such as self-driving cars running on roads, online retail e-commerce sites recommending products, and speech recognition in smartphones [28].

It has been demonstrated that machine learning and deep learning, a subset of AI, are extensively used to resolve issues with superior performance.

Deep learning algorithms mimic the capabilities of the human brain. The important aspect of deep learning is that it learns from large amounts of data. Deep learning uses a hierarchy in its capability to learn [1, 2, 20, 29–37]. The word "deep" signifies the use of several steps in the process of learning and interpreting data to get the expected outcome. Figure 4 shows the schematic of a deep learning neural network.

As shown in Figure 4, a neural network is a network of neurons mimicking human brains. An AI architecture consists of an input layer, an output layer, and multiple hidden layers, such as layer 1, layer 2, and layer 3 [31]. The number of hidden layers varies depending on the purpose of use. For example, an automated vehicle AI model may have millions of hidden layers. A deep neural network (DNN) in general contains several hidden layers. DNN helps explore an identified region of an image rather than analysing the full captured picture and, consequently, is far better equipped for face identification. The algorithm popularly known for DNN-centric identification is convolution. The detection of a particular facial feature, such as a mole, can be done with a high probability using DNN in comparison to other algorithms. There are many areas of investigation in image recognition systems where DNN is extensively in use. Face recognition includes feature extraction, segmentation, and use in face detection. The following are the key reasons for choosing DNN for the current system:

(i) The developed algorithm needs to support big data when used for a retail chain. With IoT, big data, and the cloud, this is possible

(ii) The processing capability can be supplemented by edge computing or by cloud sourcing

(iii) DNN implementation can be performed in a segregated manner

It is a modification in the algorithm with the Rectified Linear (ReLU) function that is superior to using a SIGMOID while training a DNN. This is primarily because it comes with a vanishing gradient.

6. Proposed Design

Figure 5 shows the implementation design for the AI-powered contactless IoT access system. The proposed system consists of the following tiers:

6.1. External Interface. This is the interface through which the user interacts. This tier consists of an IoT camera and an IR sensor. The camera is to capture the image of the visitor, and the IR sensor is to receive an access code from a smartphone.

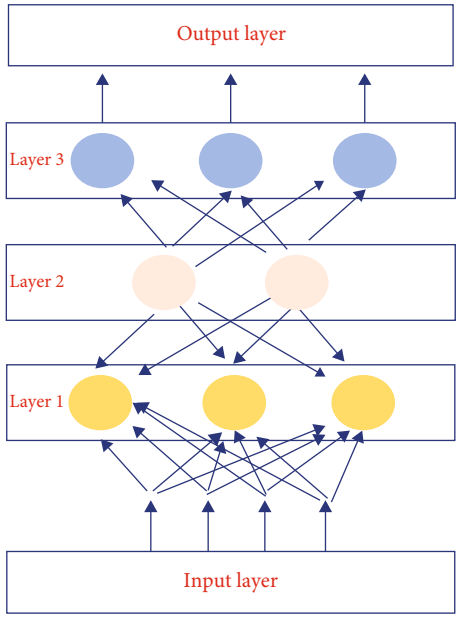

Figure 4: Deep learning neural network [30].

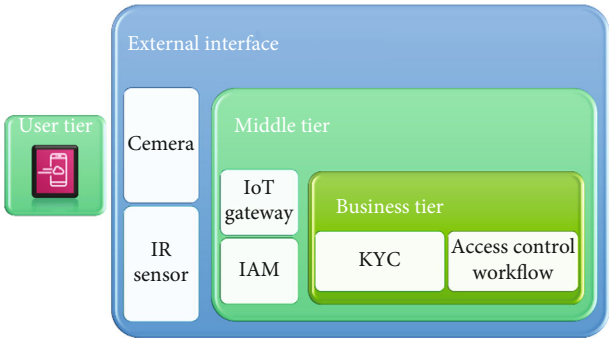

Figure 5: AI-powered contactless IoT access system.

6.2. Middle Tier. This tier consists of an IoT gateway for data transfer between the IoT devices and the internet. To have proper security credential validation and access, the identity access management (IAM) module is placed in this tier. IAM acts as a secured gate for access to business information and transactions.

6.3. Business Tier. This tier includes business information processing and business databases. Know your customer (KYC) information with digital photographs and personal access credentials is kept in this layer. Depending on the intended visit requirement, the access control workflow is called, and the necessary access code is generated. The generated code via the internet is dispatched to the registered user's smartphone after KYC verification.

6.4. User Tier. This tier consists of a smartphone with or without internet connectivity. The business tier-generated access code is received as an OTP on the used smartphone. To complete the validation, the user must click on the IR app to transfer the received OTP to the IR sensor at the interface tier.

The key benefits of the design compared to available similar technologies are as follows:

(i) The face detection uses the latest deep learning technology, so even if there is a change in some of the facial features like spectacles, moustaches, etc. from the stored KYC photo, the system will be able to recognize the face

(ii) The whole identity access process, from start to finish, is contactless. There is no need to use a figure print or a smart card

(iii) The smartphone can receive the OTP as SMS, so there is no need to remain connected to the internet during validation

(iv) The input from the smartphone is using IR using a line of sight so there is no chance of wrong use of the OTP

7. Experimental Setup

7.1. System Architecture. Cloud-based technologies enable users to easily monitor and control IoT devices in real-time. The proposed system setup is based on a combination of IoT and AI. Figure 6 shows the architecture of the proposed AI-p contactless IoT access system.

The roles of each component shown in Figure 6 are:

(1) *Mobile.* The mobile will be used to receive the OTP for secured access. The mobile needs to be connected to a mobile network to receive SMS. In the proposed system, to minimize internet data dependency, the OTP is generated as an SMS

(2) *IR lock.* This is an electronic lock equipped with an IR sensor and can operate through IR transmission. IR has chosen to make it a line-of-sight access and prevent unauthorized hacking

(3) *CCTV.* This can be any off-the-shelf CCTV to capture the image of the visitor. Send this to the IoT gateway

(4) *Monitor.* This is a commercial monitor to display a visitor's image and access status/notification

(5) *IoT gateway.* The IoT gateway can be any edge-based gateway. A capability of local processing for authenticated access and data exchange to the cloud/internet

(6) *Server.* The server is primarily the server catering to the customer relationship management (CRM) needs with the KYC information and workflow for visitor access authorization

7.2. Flow Chart of Implementation. Figure 7 shows the flowchart of the implementation of AI-powered contactless IoT access. The starting point for the system access is a visitor standing in front of the CCTV and requesting access to the facility.

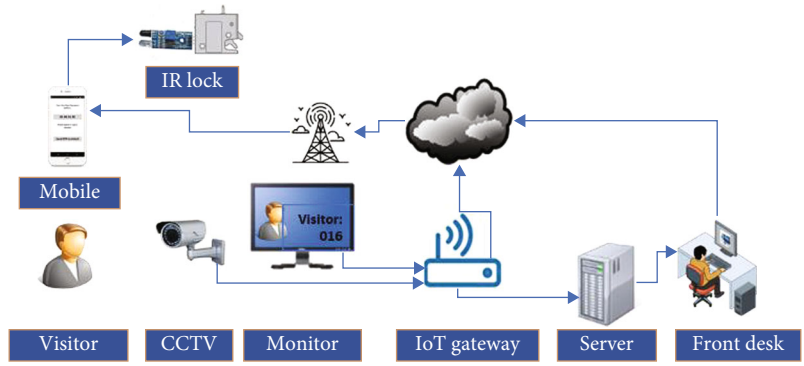

Figure 6: AI-powered contactless IoT access architecture.

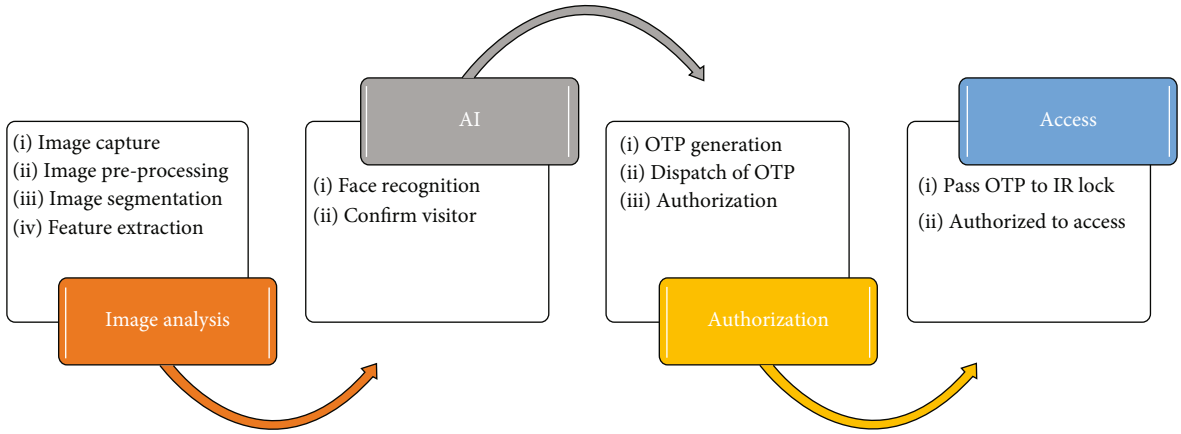

Figure 7: AI-powered contactless IoT access flowchart.

The final step of the process is to open the electronic lock for the facility using the system-provided access code. During designing of the proposed system, we have taken security and contactless access into consideration as the highest priorities. Since the security aspect details are beyond the scope of current work, the details about the IAM are not included as part of the architecture diagram in Figure 6. We have assumed standard IAM will be available along with CRM.

7.3. IoT System. IoT has been all around us for quite some time now, and it has almost revolutionized the way machines communicate among themselves. In the current system, the IoT implementation consists of an Arduino-based system.

This includes an IR sensor, a display panel, and the Arduino Uno, a microcontroller built on the ATmega328P and is open-source hardware. The ATmega328 on the Arduino Uno allows you to upload C code. It communicates using the original STK500 protocol. The ESP8266 is an economical Wi-Fi chip that provides a wireless connection to the Arduino Uno. Using Wi-Fi, the device's data transfers to the Internet shown in Figure 8.

7.4. Face Recognition Using AI. The face recognition using deep learning-based AI implementation is inspired by Project Gurukul [32]. The implementation of the algorithm helps to identify the human face in a live video. This is implemented with the help of Python Dlib's facial recognition network. Dlib is a general-purpose software library. The image analysis process as shown in Figure 7 is done using standard Python Dlib functions such as preprocess image (*input_path, output_path, crop_dim*). The system needs to call the appropriate function and pass the required parameters to do the image analysis (preprocessing, segmentation, and feature extraction).

To start with, we have created a link list of KYC numbers and image numbers as shown in Table 2. This is required to map each image with the associated KYC information in the CRM database. So that when DNN recognizes a person from a video stream, the system can trace the related KYC.

Table 3 shows the number of images used to train the DNN. For security reasons, each image is given a number instead of a name.

The proposed AI system is trained with KYC images. The main contribution of using AI with Python Dlib's facial recognition network is to recognize a registered user using a camera. The AI system gets trained with KYC images used during registration of the user. This removes the need of human being to identify a registered user. The AI based approach offer better and more effective processing models. Its ability to learn unsupervised drives continuous improvement in accuracy and outcomes. Further the proposed AI approach provides alarm for impersonation and anomaly detection.

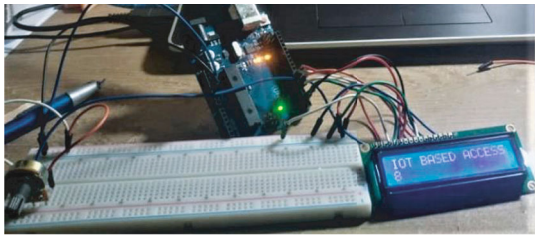

Figure 8: Arduino-based IoT system.

Table 2: Image link list table format.

No.	Image#	KYC#
1	01	2020_05_20_01
2	02	2018_07_10_04
3	03	2019_06_04_03

Table 3: Image classifications.

No.	Classification	Count
1	KYC images	80
2	Non-KYC images	20

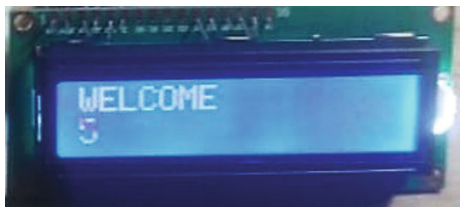

Figure 9: Display for image number 5.

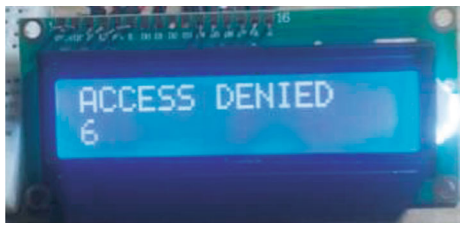

Figure 10: Display for image number 6.

8. Results

The system can identify the person whose photo is associated with number 5 (Figure 9).

Figure 10 shows that the system is unable to identify the person whose photo is associated with number 6.

Figure 11 shows that the system has dispatched the OTP to the person's mobile, whose photo is associated with number 7. Figure 12 shows how the OTP is received in a person's mobile.

Figure 11: Display for image number 7.

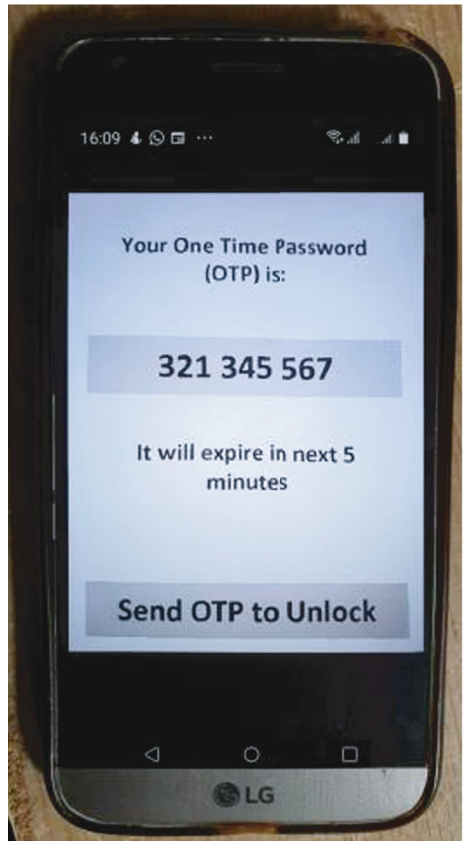

Figure 12: OTP received in mobile.

Figure 13 shows how it will display on the monitor at the front desk. This shows the live video of the person at the gate and the associated KYC photo, with the result showing the video feed and "Matched with KYC" image.

9. Analysis of Result

To assess the outcome obtained during the experiment, a confusion matrix as shown in Figure 14 is used for analysis. This is used to get the efficiency of the classifier.

As per the confusion matrix, "Matched" refers to DNN's trained algorithm's recognition of an image. "Actual" refers to the known KYC's as referred to in Table 2. The parameters in Figure 14 mean True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) [33]. Table 3 shows the obtained result, indicating the accuracy of 92% and precision of 96% with a FP rate of 13%.

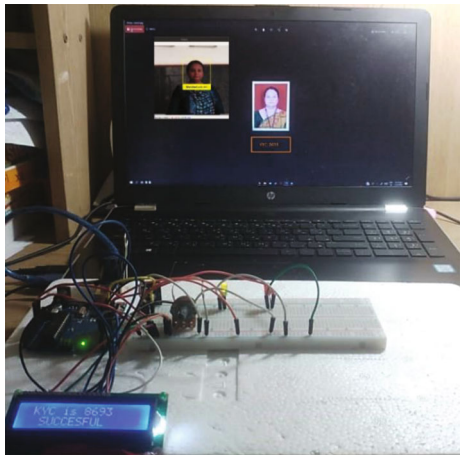

Figure 13: Matched KYC image number 8693 with terminal display.

	Matched No	Matched Yes	
Actual No	TN = 20	FP = 3	23
Actual Yes	FN = 5	TP = 72	77
	25	75	

Figure 14: Confusion matrix for KYC image recognition.

Table 4: The performance of algorithm.

No.	Performance metric	Value
1	Known KYC	80%
2	Accuracy	92%
3	Error rate	8%
4	Sensitivity	94%
5	FP rate	13%
6	Specificity	87%
7	Precision	96%
8	Prevalence	77%

Table 4 provides the standard performance indicators computed based on obtained result as per standard definition. For example, sensitivity and specificity can be calculated as the following:

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \quad \text{Obtained Sensitivity} = \frac{72}{72 + 5} = 94\% \tag{1}$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}}, \quad \text{Obtained Specificity} = \frac{20}{20 + 3} = 87\% \tag{2}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}}, \quad \text{Obtained Accuracy} = \frac{72 + 20}{72 + 20 + 5 + 3} = 92\% \tag{3}$$

$$\text{Error Rate} = \frac{\text{FP} + \text{FN}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}}. \quad \text{Obtained Accuracy} = \frac{3 + 5}{72 + 20 + 5 + 3} = 8\% \tag{4}$$

The chances of error are 8%. The algorithm's recognition sensitivity is highest at 94%. The FP rate is a complex metric. This implies that even though the algorithm identifies a face as correct, it is false. In the current algorithm, the FP rate is only 13%. With a large number of samples, the deep learning system will learn more. In such a condition, the FP rate will improve. Specificity drives the missed identification of a real image. In the current algorithm, it is at 87%. This implies that the algorithm will be able to match the actual faces in 87% of cases.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}. \quad \text{Obtained Accuracy} = \frac{72}{72 + 3} = 96\% \tag{5}$$

Precision is a significant metric that forecasts how many times its prediction is correctly linked to the actual KYC. The obtained precision is 96%, which is very precise, and this can be improved with a larger data set.

$$\text{Prevalence} = \frac{\text{FN} + \text{TP}}{\text{TP} + \text{TN} + \text{FN} + \text{FP}}. \quad \text{Obtained Accuracy} = \frac{5 + 72}{72 + 20 + 5 + 3} = 77\% \tag{6}$$

The prevalence result is 77%, which indicates the 100 images used are associated with 77% KYC. This is fairly close to 80% of the actual number of known KYC images (Table 3).

A comparative study [34] between different classification techniques suggests that the DNN has better accuracy than other popular algorithms. We compared (see Figure 15) the published FRR percentage of 27.27% [34] with obtained false rejection rate (FRR) of 5 out of 77 (that is 6%). The proposed algorithm has significant improvement in FRR from 27.27% to 6%. This indicates the present approach is more reliable.

Table 5 shows comparison of the obtained result with other published similar work using AI. From the comparative analysis, we can observe that the key performance parameters for present AI based approach are significantly higher.

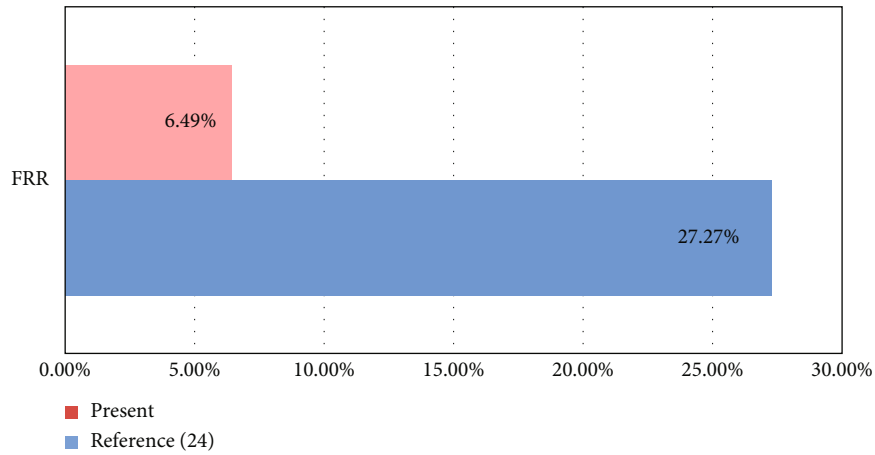

Figure 15: Comparison between reference FRR % vs. present work FRR %.

Table 5: Comparison of performance with other published similar work.

Contribution	Image partitioning %	Key parameters %
Wu et al. [1]	Validation - 80 Training - 10 Testing - 10	Accuracy - 76 Sensitivity - 81.1 Specificity - 61.5
Xu et al. [2]	Validation & Training - 85.4 Testing - 14.6	Accuracy - 86.7 Sensitivity - 81.5 Precision - 80.8
Javaheri et al. [35]	Training - 90 Validation - 10	Accuracy - 91.66 Sensitivity - 87.5 Specificity - 94
Present work	Validation - 80 Testing - 20	Accuracy - 92 Sensitivity - 94 Precision - 96 Specificity - 87

10. Conclusion

Smart mobility by contactless IoT access system can curve the COVID-19 pandemic growth. At present, there are many touchpoints in private and public vehicles, transportations, and areas where contact is essential, and there is a need for secured contactless access to reduce the spread of COVID-19. Devices such as smart cards, figure print identification, and code-based access require touch, hence risks for COVID-19 spread are possible. The motivation for the current work was to use AI to provide contactless and secure access. In this paper, we have proposed a design for an AI-powered contactless and IoT-enabled access system. AI is used for face recognition to identify a person. The IoT is used for validation and to provide an access code. AI identified 77% associated with KYC, while actual known KYC is 80%, which is fairly close to the actual number. In comparison with the published FRR percentage of 27.27% [34], the obtained false rejection rate (FRR) in current work is 6% (5 out of 77). The proposed algorithm has significant improvement in FRR from 27.27% to 6%. Furthermore, a comparison is done for the key performance indicators such as accuracy, sensitivity, and precision with published result in Table 5. The result shows 92% accuracy, 94% sensitivity, and 96% precision for face recognition and is significantly higher than reference work [25, 26, 27]. The AI and IoT combination provide more accurate and secure contactless access than conventional, readily available devices. This result concluded that AI with IoT can increase health safety without compromising security. The performance of the system is encouraging.

There is tremendous potential to use the proposed system in future. This can be extended to the implementation of the Arduino web server; this will help to open the doors to more IoT-based user-friendly implementations. The new technique can also further improve retina-based access. To make the system compact, the Raspberry Pi, a fully functional computer, can replace the Arduino. With COVID-19 pandemic impact still ongoing, a contactless system is the need of the hour, and proposed smart system can be helpful in minimizing the spread of COVID-19 through contacts in public facilities.

Data Availability

Data are available in the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

All authors have the similar contributions.

Funding

This work has been supported in part by the Universiti Kebangsaan Malaysia, under research grant GGPM 2020-028.

References

[1] X. Wu, H. Hui, M. Niu et al., "Deep learning-based multi-view fusion model for screening 2019 novel coronavirus pneumonia: a multicentre study," *European Journal of Radiology*, vol. 128, p. 109041, 2020.

[2] X. Xu, X. Jiang, C. Ma et al., "Deep learning system to screen coronavirus disease 2019 pneumonia," (2020), http://arxiv.org/abs/2002.09334.

[3] K. T. Doss, D. A. O'Sullivan, and J. A. Slotnick, "Chapter 37 - physical security concepts and applications," in *The Professional Protection Officer (Second Edition)*, S. J. Davies and L. J. Fennelly, Eds., pp. 409–432, Butterworth-Heinemann, 2020.

[4] D. Kim and M. G. Solomon, *Fundamentals of Information Systems Security*, Jones & Bartlett Learning, 4th Edition edition, 2021.

[5] R. Anderson, *Security Engineering*, Wiley, 3rd Edition edition, 2020.

[6] S. Bisser, *Microsoft Conversational AI Platform for Developers: End-to-End Chatbot Development from Planning to Deployment*, 9781484268377, Apress, ISBN, 2021.

[7] A. Botha, C. Salerno, M. Niemand, S. Ouma, and I. Makitla, "Disconnected electronic badges in resource constrained environments: a use case from the rural Nciba district in the Eastern Cape," *Proceedings of the Second International Conference on Advances in Computing*, , pp. 202–207, Communication and Information Technology (CCIT), 2014.

[8] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[9] Y. Andaloussi, M. D. El, Y. Ouadghiri, J. M. Maurel, and H. C. Bonnin, "Access control in IoT environments: feasible scenarios," *Procedia Computer Science*, vol. 130, pp. 1031–1036, 2018.

[10] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 8, 2016.

[11] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadak, "Deep learning for computer vision: a brief review," *Computational Intelligence and Neuroscience*, vol. 2018, Article ID 7068349, 13 pages, 2018.

[12] W. Ouyang, X. Zeng, X. Wang et al., "DeepID-net: object detection with deformable part based convolutional neural networks," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 7, pp. 1320–1334, 2017.

[13] V. Verdhan, *Computer Vision Using Deep Learning: Neural Network Architectures with Python and Keras*, Apress, 2021.

[14] D. Chen, X. Cao, F. Wen, and J. Sun, "Blessing of dimensionality: high-dimensional feature and its efficient compression for face verification," *Proceedings of the 26th IEEE Conference on Computer Vision and Pattern Recognition (CVPR '13)*, pp. 3025–3032, 2013.

[15] M. I. A. Latiffi and M. R. Yaakub, "Sentiment analysis: An enhancement of ontological-based using hybrid machine learning techniques," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 7, no. 2, pp. 61–69, 2018.

[16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[17] J. Doherty, *Wireless and Mobile Device Security*, Jones & Bartlett Learning, 2nd Edition edition, 2021.

[18] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of things and its applications: a comprehensive survey," *Symmetry*, vol. 12, no. 10, p. 1674, 2020.

[19] K. Jaskolka, J. Seiler, F. Beyer, and A. Kaup, "A Python-based laboratory course for image and video signal processing on embedded systems," *Heliyon*, vol. 5, no. 10, 2019.

[20] E. S. Ali, M. K. Hasan, R. Hassan et al., "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications," *Networks*, vol. 2021, article 8868355, pp. 1–23, 2021.

[21] M. K. Hasan, S. H. Yousoff, M. M. Ahmed, A. H. Hashim, A. F. Ismail, and S. Islam, "Phase offset analysis of asymmetric communications infrastructure in smart grid," *Elektronika ir Elektrotechnika*, vol. 25, no. 2, pp. 67–71, 2019.

[22] T. M. Ghazal, M. K. Hasan, M. T. Alshurideh et al., "IoT for smart cities: machine learning approaches in smart healthcare—a review," *Future Internet*, vol. 13, no. 8, p. 218, 2021.

[23] I. Memon, R. A. Shaikh, M. K. Hasan, R. Hassan, A. U. Haq, and K. A. Zainol, "Protect mobile travelers information in sensitive region based on fuzzy logic in IoT technology," *Networks*, vol. 2020, article 8897098, pp. 1–12, 2020.

[24] N. S. Nafi, M. K. Hasan, and A. H. Abdallah, "Traffic flow model for vehicular network," in *2012 International Conference on Computer and Communication Engineering (ICCCE)*, pp. 738–743, IEEE, 2012.

[25] M. K. Hasan, M. Shafiq, S. Islam et al., "Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications," *Complexity*, vol. 2021, Article ID 5540296, 13 pages, 2021.

[26] M. K. Hasan, A. F. Ismail, S. Islam, W. Hashim, and B. Pandey, "Dynamic spectrum allocation scheme for heterogeneous network," *Wireless Personal Communications*, vol. 95, no. 2, pp. 299–315, 2017.

[27] S. Amanlou, M. Hasan, and K. A. A. Bakar, "Lightweight and secure authentication scheme for IoT network based on publish- subscribe fog computing model," *Computer Networks*, vol. 199, article 108465, 2021.

[28] N. M. Elfatih, M. K. Hasan, Z. Kamal et al., "Internet of vehicle's resource management in 5G networks using AI technologies: current status and trends," *IET Communications*, vol. 16, no. 5, pp. 400–420, 2022.

[29] M. Akhtaruzzaman, M. K. Hasan, S. R. Kabir, S. N. H. S. Abdullah, M. J. Sadeq, and E. Hossain, "HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey," *IEEE Access*, vol. 8, pp. 222977–223008, 2020.

[30] D. Matthew, K. Diego, and B. Jin, *Implementing Deep Neural Networks for Financial Market Prediction on the Intel Xeon Phi*, 2015.

[31] S. Y. Siddiqui, A. Haider, T. M. Ghazal et al., "IoMT Cloud-based intelligent prediction of breast cancer stages empowered with deep learning," *IEEE Access*, vol. 9, pp. 146478–146491, 2021.

[32] D. Estrada, L. Tawalbeh, and R. Vinaja, "How secure having IoT devices in our homes?," *Journal of Information Security*, vol. 11, no. 2, pp. 81–91, 2020.

[33] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," *Computers & Security*, vol. 74, pp. 340–354, 2018.

[34] Suwarno & Kevin, "Analysis of face recognition algorithm: Dlib and OpenCV," *JITE (Journal Of Informatics And Telecommunication Engineering)*, vol. 4, no. 1, pp. 173–184, 2020.

[35] T. Javaheri, M. Homayounfar, Z. Amoozgar et al., "CovidCT-Net: an open-source deep learning approach to identify COVID-19 using CT image," (2020), http://arxiv.org/abs/2005.03059.

[36] M. K. Hasan, S. Islam, R. Sulaiman et al., "Lightweight encryption technique to enhance medical image security on internet of medical things applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021.

[37] S. Islam, A. H. Abdalla, and M. K. Hasan, "Novel multihoming-based flow mobility scheme for proxy NEMO environment: a numerical approach to analyse handoff performance," *ScienceAsia*, vol. 43S, no. 1, pp. 27–34, 2017.

[38] M. K. Hasan, S. Islam, I. Memon et al., "A novel resource oriented DMA framework for internet of medical things devices in 5G network," *IEEE Transactions on Industrial Informatics*, vol. 1, 2022.

[39] M. K. Hasan, A. Alkhalifah, S. Islam et al., "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9065768, 26 pages, 2022.

[40] M. K. Hasan, T. C. Chuah, A. A. el-Saleh et al., "Constriction factor particle swarm optimization based load balancing and cell association for 5G heterogeneous networks," *Computer Communications*, vol. 180, pp. 328–337, 2021.

[41] K. Choi and G. E. Sobelman, "Optimized face detection and alignment for low-cost and low-power IoT systems," in *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, pp. 129–135, IEEE, 2021.

[42] N. Mostakim, R. R. Sarkar, and M. A. Hossain, "Smart locker: IoT based intelligent locker with password protection and face detection approach," *International Journal of Wireless and Microwave Technologies*, vol. 9, no. 3, pp. 1–10, 2019.

[43] M. Kolhar, F. Al-Turjman, A. Alameen, and M. M. Abualhaj, "A three layered decentralized IoT biometric architecture for city lockdown during COVID-19 outbreak," *Ieee Access*, vol. 8, pp. 163608–163617, 2020.

[44] V. Sharmila, N. R. Paul, P. Ezhumalai, S. Reetha, and S. N. Kumar, *IOT Enabled Smart Assistance System Using Face Detection and Recognition for Visually Challenged People*, Materials Today: Proceedings., 2020.

[45] A. Barnawi, P. Chhikara, R. Tekchandani, N. Kumar, and B. Alzahrani, "Artificial intelligence-enabled internet of things-based system for COVID-19 screening using aerial thermal imaging," *Future Generation Computer Systems*, vol. 124, pp. 119–132, 2021.