Journal of Science and Technology
ISSN: 2456-5660 Volume 9, Issue 06 (June -2024)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2024.v9.i06.pp20- 32*

Development of an IoT-Based QR Code Access Control and Payment System using Arduino and ESP8266

G. Tejaswai[1], Chiruvella Manasa[2], Avadhanam Sandhya Sri[2], Amari Sravani[2], Challagundla Thanusree[2], Kandagaddla Lakshmi Akhila[2]

[1]AssistantProfessor, Department of ECE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh, India

[2]UG Scholar, Department of ECE, Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh, India

To Cite this Article

G. Tejaswai, Chiruvella Manasa, Avadhanam Sandhya Sri, Amari Sravani, Challagundla Thanusree Kandagaddla Lakshmi Akhila,“ **Development of an IoT-Based QR Code Access Control and Payment System using Arduino and ESP8266”** Journal of Science and Technology, Vol. 09, Issue 06,- June 2024, pp20-32

Article Info

Received: 28-04-2024 *Revised: 15-05-2024* *Accepted: 27-05-2024* *Published: 14-06-2024*

Abstract

In this research, we present the development and implementation of an IoT-based access control and payment system utilizing QR code technology, Arduino microcontroller, and ESP8266 Wi-Fi module. The system is designed to enhance security and streamline payment processes in various applications such as parking lots, public transport, and restricted access areas. The core components include an ESP camera for QR code scanning, a Liquid Crystal Display (LCD) for user feedback, and a pair of motors to control physical barriers. Upon scanning a QR code, the system verifies its validity and either grants access or denies it based on pre-set criteria. For valid QR codes, the system deducts a specified amount from the user’s balance, displays the updated balance on the LCD, and operates the motors to allow entry. Invalid QR codes trigger an audio alert via a buzzer. The system communicates transaction data to a remote server using the ESP8266 module, ensuring real-time logging and monitoring. The project highlights the integration of hardware components with software modules to achieve a robust and efficient access control solution. By leveraging IoT technologies, the system offers improved security, real-time data processing, and automated transaction handling. This research contributes to the field of IoT-based automation by demonstrating a practical application in access management and payment systems, providing a scalable and versatile solution for modern access control challenges.

Keywords: Automated payment system, Internet of Things, Arduino, ESP8266 WI-FI module, QR code access control.

1. INTRODUCTION

A QR code-based metro pass technology makes public transportation easy and frictionless for commuters. Online pass purchases create a QR code upon approval. Instead of tickets and lines, travelers scan their QR code to enter a station or board a vehicle. This solution streamlines pass

management and usage tracking, improves user experience, and integrates with digital platforms. The European Commission has promoted public transit (PT) as "a safe, efficient, affordable, and low-emission mobility solution for everyone" across Europe and beyond since 2002. To cope with PT limitations in urban areas, intelligent transportation systems (ITSs) will use ICTs to automate transportation data collection to make transport safer, more efficient, more reliable, and more sustainable. Modern ITSs for PT offer two spatiotemporal data classes:

- Automated vehicle location (AVL) systems, mostly using satellite localization techniques, provide real-time vehicle data, including location and speed.
- Automated passenger counting (APC) or automatic fare collecting (AFC) systems can provide passenger data, such as the number of passengers boarding a bus/train or entering a station.

Strategic, tactical, operational, and real-time PT system optimization and planning tactics often incorporate such data. In example, lack of passenger arrival information, especially real-time, limits accurate studies. In many ITSs, only cars have real-time location data for trip information and medium-to-long-term service management and monitoring. In smart cities, fine-grained and real-time passenger data collecting is possible with IOT technology. Indeed, the widespread usage of mobile and portable devices with sensors allows one to collect massive amounts of data in urban settings for many applications and jobs. The fifth generation (5G) of cellular networks can support massive IOT connections, where billions of smart devices are connected to the Internet and can be easily located and tracked. The sixth-generation (6G) networks will expand these features. Some researchers have indicated that congestion adversely impacts PT users' quality of service (QOS) and travel satisfaction/quality of experience (QOE).

To address this issue, real-time, reliable, and capillary information regarding the crowding state of PT rail or road vehicles (e.g., buses, trams, and trains) and their access infrastructures is needed. Yes, "the availability of real-time passenger demand data can significantly improve the performance of control models in the case of overcrowding." New modeling, planning, and management solutions that collect real-time crowding data and use them to improve QOS/QOE in PT systems are surfacing in the literature due to past needs. Crowd analysis/monitoring includes a network of physical sensors to detect crowds and estimate their parameters, while crowd control includes prediction, decision-making, and control strategies to manage crowd events. Crowd management is different from crowdsourcing/sensing. Crowdsourcing (also known as "sensing by the crowd") in PT systems involves passengers submitting suggestions, concerns, and resources or products, such as peer-to-peer services. PT firms collaborate with passengers to fix problems or plan public transit using crowdsourced data to research and build user-preferred solutions. Instead, crowd management is based on "sensing the crowd," where PT companies analyze environmental data collected through networks of IOT sensor devices and/or user terminals for forecasting, choosing among several alternative options, and ensuring robust and safe PT system operation. During the COVID-19 epidemic, crowd management in PT systems became a major issue (see Section II). Emergency measures like reducing bus and train capacity to 50% were essential to prevent overcrowding during the acute outbreak phase. Since they divert many people to private vehicles, these methods are unsustainable. Since many scientists expect recurrent pandemic outbreaks in the future, PT system overload must be addressed better and more structurally. Modern AVL/APC/AFC systems in ITS systems collect a lot of vehicle and passenger data, but they are not always suited for real-time crowd monitoring and control. Many ICT/IOT crowd monitoring sensing technologies are presently or soon will be accessible in smart cities. A recent special issue of this magazine discusses cutting-edge ICT technology for sensor integration with transportation

infrastructure. The contributions focus on private transportation system sensing technologies for autonomous driving, intelligent fault detection, and electric charging optimization. road condition monitoring, precise fleet management, speed detection, and accident avoidance: PT system sensing technology integration receives less attention. Additionally, crowd surveillance sensing methods are not mentioned.

2. LITERATURE REVIEW

K. T. Doss, D. A. O'Sullivan, and J. A. Slotnick (2020). In 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. D. Kim and M. G. Solomon ((2021), 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. A. Botha, C. Salerno, M. Niemand, S. Ouma, and I. Makitla (2014). 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 Wireless Communications and Mobile Computing 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.

I. Ali, S. Sabir, and Z. Ullah(2016). 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. Andaloussi et al. discussed access control and authentication mechanisms supporting the cryptography algorithms in constrained devices. 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. W. Ouyang, X. Zeng, X. Wang et al., IEE(2017). Voulodimos et al.'s work on deep learning for computer vision is relevant to the work we wanted to pursue in computational intelligence. Ouyang et al. presented object detection with deformable part-based convolutional neural networks. Verdhan presented learning hierarchical representations for face verification with convolutional deep belief networks. D. Chen, X. Cao, F. Wen, and J. Sun, IEE(2013). 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. M. I. A. Latiffi and M. R. Yaakub (2018). To propose an alternate low-cost solution for highperformance 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. 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.

J. Doherty (2021). 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 . 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. During the whole process, from obtaining the photo to delivering it to the programmed destination device, no human or machine direction is involved. Across the world, businesses are using the IOT for improving efficiency and decision-making for customer-oriented services.

E. S. Ali, M. K. Hasan, R. Hassan et al. (2021). 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.

N. M. Elfatih, M. K. Hasan, Z. Kamal et al (2022). 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.

M. Akhtaruzzaman, M. K. Hasan, S. R. Kabir, S. N. H. S. Abdullah, M. J. Sadeq, and E. Hossain, IEE(2020). "HSIC bottleneck based distributed 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.

S. Y. Siddiqui, A. Haider, T. M. Ghazalet, IEE(2021). 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.

A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang(2018).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). Suwarno & Kevin (2020).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 . A comparative study [34] between different classification techniques suggests that the DNN has better accuracy than other popular algorithms. We compared the published FRR percentage of 27.27% with obtained false. M. K. Hasan, M. Shafiq, S. Islam et al(2021). 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.

S. Amanlou, M. Hasan, and K. A. A. Bakar(2021). 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.

R. Terebes, O. Lahlou, and R. Enseirb(2008). Traditional methods developed for camera-based barcode detection can be found in the literature which make use of image processing methods based on predefined rules. A. Zamberletti, I. Gallo, and S. Albertini,(2013). "Robust angle invariant 1d barcode detection," in Proc. 2nd IAPR These methods are the first choice in case of carefully controlled situations, where the camera is directly pointed to the barcode in close proximity. These methods prove to be equally unreliable in the case of complicated scenes, which we encounter in most commercial applications. Recently, researchers have developed deep-learning-based methods to solve this problem. Zamberletti et al. A. Sharif, G. Zhai, J. Jia, X. Min, X. Zhu, and J. Zhang,(2021).As utilized the CNN model to directly predict the angle of alignment of barcode along with the localization box results. Redmon et al. utilized a general object detection Yolo to localize barcode and also used Darknet19 to output alignment angle. Sörös and Flörkemeier used a "barcodeness structure matrix. used a "barcodeness structure matrix"-based method to locate 1-D and 2-D barcodes, which is capable to detect blur samples as well. Dubská et al. used hough space for efficient detection and localization of 2-D barcodes. Xiao and Ming employed a line segment detection-based method for detecting arbitrarily aligned barcode. Such methods perform very well in public data sets, such as ArtLab and WWW Manchester data sets, but in the case of complex scenes still lack the desired accuracy. Jia et al. presented Faster RCNN based model which presents better results of 1-D and 2-D barcodes detection, but suffers from efficiency problem. Faster RCNN is an anchor-based method similar to Yolo-v2 , SSD , and RetinaNet . The anchor-based methods work on the old sliding window-based concept. Anchor boxes of predefined shapes, sizes, aspect ratios, and orientations work analogous to sliding windows. They suffer from the problem of too many hyperparameters for tuning during training. Specifically, localization of four vertices of barcode using anchor-based methods present the challenges mentioned above. Hence, anchor-based methods are not suitable to be adopted for our solution. In our previous work.

J. Redmon, S. Divvala, R. Girshick, and A. Farhadi,IEE (2016). "we proposed a 1-D barcode detector along with a model pruning method for efficient and accurate barcode detection. The work did not focus on the deblurring problem and also required an iterative model pruning approach to make it efficient. In this work, we propose an anchor-free method that is scaled and does not require model pruning. Anchor-free methods, such as Yolo-v. Z. Tian, C. Shen, H. Chen, and T(0ct 19,2020). He The EAST detector for arbitrarily aligned text also qualifies as an anchor-free method. These methods work by outputting a segmentation-based prediction map, utilizing pixel location inside the barcode locations to predict boundary boxes. Some of these methods typically have a rather complicated postprocessing step to output the final bounding boxes from output prediction maps. Recently, the anchorfree detector FCOS was introduced which also predicted.

A. Hiller and R. T. Chin,1990). Blurring is defined as the convolution of the blur kernel point spread function (PSF) with the original image. The inverse process given the PSF is called the deconvolution process. If the PSF function is completely unknown, and an attempt is made to deblur the image given only the blurry image, it is called blind deconvolution. Classical methods of kernel estimation-based deblurring include Wiener filter. S. Yahyanejad and J. Ström, IEE(2010). The K-L divergence to approach barcodes divergence. The results claimed are great but only synthetic barcode data is used for testing. Esedoglu [30] used a machine-learning-based method for 1-D barcode deconvolution, but the method suffers from an efficiency problem. Yahyanejad and Ström .

M. Tan and Q. V. Le(jun,2020).To build an accurate camera-based multiclass barcode decoding system, we must be able to localize as well as deblur the blur samples. In the first step, we train a customized object detector that outputs classification along with the correct localization result of the barcode. Localization results include the four vertices or 8-quadrilateral points of all categories of barcodes present in the scene. In the second step, barcodes are cropped out and fed to the barcode deblurring model. This model is trained in an adversarial manner using a GAN strategy. After training the deblurring model with adversarial loss, it takes blur barcodes as input and outputs the deblurred image. After the barcode deblurring, the barcode becomes able to be decoded which was otherwise undecodable because of blurring. Our localization model is an anchor-free, segmentation-based, FCN, which icccs inspired by the works. T. Lin, P. Dollár, R. B. Girshick, K. He, B. Hariharan, and S. J. Belongie(2016).Most of the recent state-of-the-art object detection models use FPN as feature fusion networks to merge the features of different scales in a top-down manner. Since our task of classifying and detecting multiple and multiclass barcodes is similar, we also design our model to have this capability. Multiscale feature fusion is required to achieve accurate barcode detection because it is important to combine high-resolution feature maps in CNN that have low semantic information with low-resolution feature maps, which have high-level semantic information. S. Liu, L. Qi, H. Qin, J. Shi, and J. Jia(2019).PANet tried to solve this issue by adding an extra bottom-to-top pyramid path aggregation network. NasFPN used deep reinforcement learning to optimize for the best connections for feature fusion, but the connections are very unstable and very difficult to interpret. Our best choice for a feature fusion network is BiFPN introduced in along with the weighted feature fusion method. BiFPN feature network provides the optimized crossconnections for the complete model to be efficient and accurate while being scalable for different application requirements. We employ EfficientDet-D3 as our feature fusion network, which contains five of these BiFPN feature fusion units.

3. PROPOSED SYSTEM

This project integrates multiple hardware components and software modules to create a functional and efficient QR code-based access control system as shown Figure 1. It showcases the practical application of IoT technology in improving security and automating payment processes. The system's ability to handle real-time data processing and network communication demonstrates a scalable solution for modern access control challenges. The system is designed for environments where secure access control and automated payment processing are essential, such as parking facilities, public transport systems, and entry points to secure areas. Users scan their QR codes using the ESP camera, and the system validates the codes to either grant access and process payments or deny access and provide feedback.

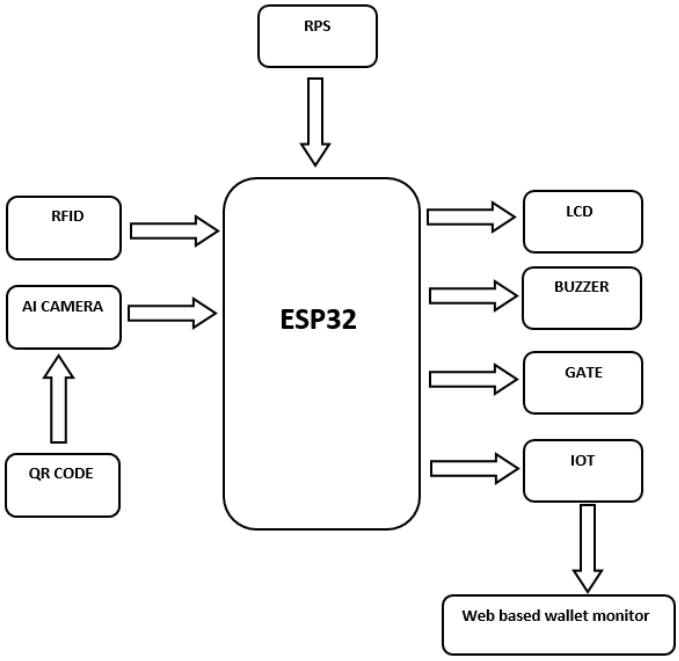

Fig.1: Block diagram of proposed system.

As shown in the above block diagram, the Arduino is interfaced with all the ESP camera which is used scan the QR code and sends the data controller. Once the microcontroller is powered up with the use of a 9v battery it is initialized and set to the basic settings, now the system is ready to proceed camera which scan the QR code of the product and display all the information of product in LCD display with the help of Arduino. Once the item is scanned user if authorized allow him to inside by opening dc motor if not it alerts with buzzer and automatically stops by closing dc motor all the data will display on lcd and send the same data into server. if the scanning process is successful the product details will be transferred to the microcontroller's memory and then will be transferred to the LCD module to be displayed on the LCD screen. The entire working process is implemented by the software called Arduino IDE. The Proteus simulation software is used to check the simulation results before the hardware implementations.

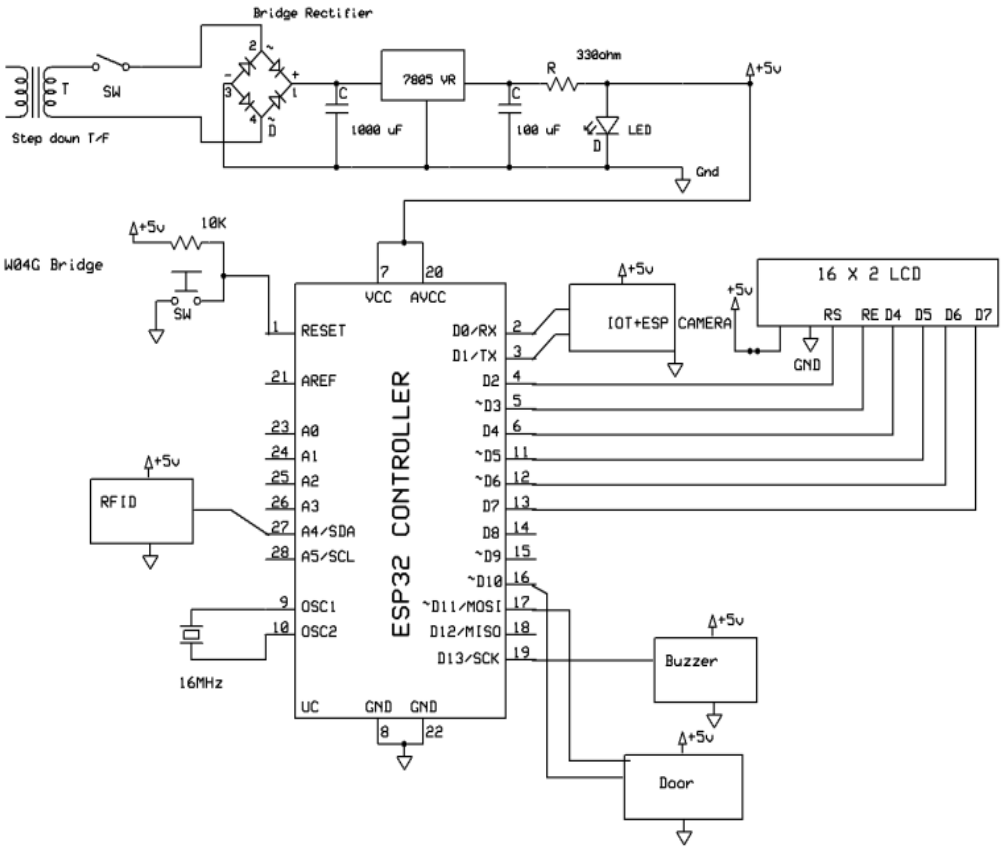

Figure 2. Schematic diagram of proposed system.

Here we are using this platform for the same. As we know that the java is a very powerful language which also rich in libraries so that to login, to balance check & to generate QR code we are using this language. First, we are creating a local server. At this server side, we create special identity like username & password for admin. For passenger only admin can fill a form which contain data like username, user ID, mobile number etc. and after registration profile and generating ID of a user, this system will automatically generate a QR code. After we register a particular user which will have users ID and QR code. User can add money to the wallet/ Add balance to a particular user ID. Whenever user will go by bus, they have to scan the QR code., thus here servo motor run motor smoothly. If exact condition matches then motor will driver and directly money will debit from users' wallet. The admin side (Transport Corporation) can keep track of traffic on the bus and can also track a particular user that on what day he/she is travelling etc.

4. RESULTS AND DISCUSSION

The circuit is powered on by providing a regulated power supply of 12V, which is then converted to 5V DC. The LED acts as an indicator for the 5V current; when 5V current is present, the LED lights up. This 5V DC current is distributed to every hardware component in the circuit.

When the reset button is pressed after providing the regulated power supply, the LCD displays "IOT QR Metro Pass System." The output can be seen on the LCD screen after the IoT module is connected as shown in Figure 4.

The EM-18 Reader Module is used to detect a card. If the card is valid, the balance is displayed on the LCD, and the DC Motor is controlled by the L293D motor driver. When the DC Motor moves forward, the gate automatically opens as shown in Figure 5(a). If the EM-18 Reader detects an invalid card, the output will be displayed on the LCD, the data will be posted to the server, and the buzzer will sound as shown in Figure 5(b).

The AI camera pins are connected to the ESP32, which scans the QR code. If the QR code is valid, the output is displayed on the LCD, and the DC Motor is controlled by the L293D motor driver. The gate automatically opens when the DC Motor moves forward.

Both valid and invalid data are uploaded to a website using the ESP8266 IoT module. The website displays details of valid and invalid cards/QR codes, the balance amount, and the time.

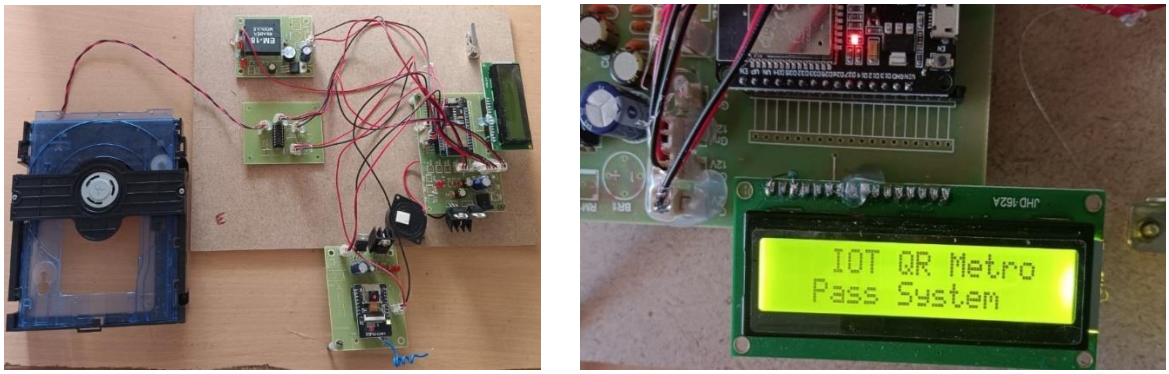

Figure 3. Hardware setup of proposed system.

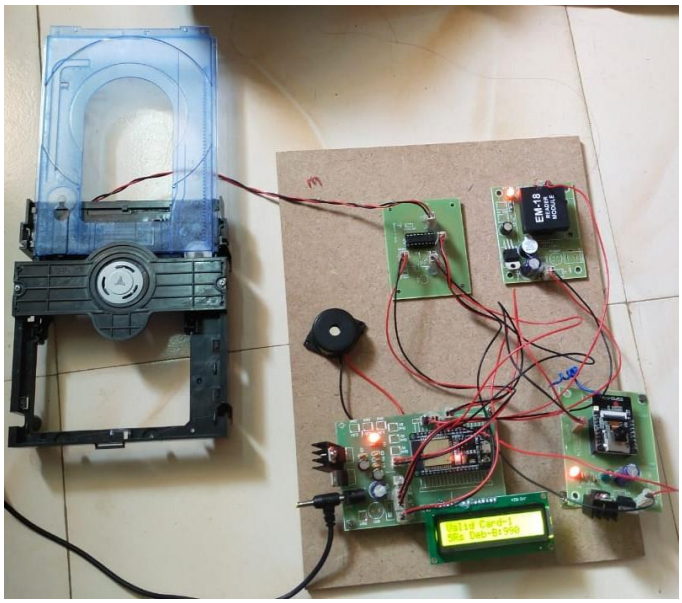

Figure 4. Output displaying on LCD.

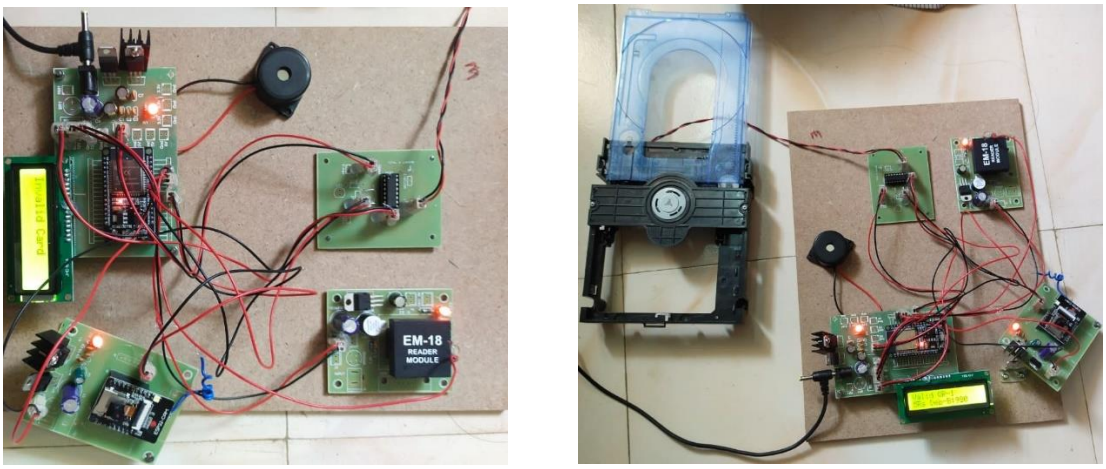

Figure 5. (a) EM-18 reader module with valid card. (b) EM-18 reader module with invalid card.

Page 1 of 2 Next

S.No	Pass_Status	Date
1	RFID_Card_5Rs_Debited_Blc:995	2024-02-16 12:19:03
2	Invalid_card	2024-02-16 10:20:17
3	RFID_Card_5Rs_Debited_Blc:995	2024-02-16 10:19:52
4	Invalid_card	2024-02-15 14:57:55
5	RFID_Card_5Rs_Debited_Blc:995	2024-02-15 14:48:45
6	QR1_Valid_5Rs_Debited_Blc:985	2024-02-15 14:47:08
7	QR1_Valid_5Rs_Debited_Blc:990	2024-02-15 14:46:54
8	Invalid_card	2024-02-15 14:44:01
9	RFID_Card_5Rs_Debited_Blc:995	2024-02-15 14:42:29
10	RFID_Card_5Rs_Debited_Blc:995	2024-02-15 14:38:25
11	RFID_Card_5Rs_Debited_Blc:990	2024-02-15 14:19:58
12	Invalid_card	2024-02-15 14:13:55
13	RFID_Card_5Rs_Debited_Blc:985	2024-02-15 14:12:35
14	QR1_Valid_5Rs_Debited_Blc:990	2024-02-15 14:11:45
15	QR1_Valid_5Rs_Debited_Blc:995	2024-02-15 14:11:31
16	QR1_Valid_5Rs_Debited_Blc:975	2024-02-15 14:05:23
17	QR1_Valid_5Rs_Debited_Blc:980	2024-02-15 14:03:51
18	QR1_Valid_5Rs_Debited_Blc:985	2024-02-15 14:03:37
19	QR1_Valid_5Rs_Debited_Blc:990	2024-02-15 14:03:06
20	RFID_Card_5Rs_Debited_Blc:995	2024-02-15 14:01:28

.

Figure 6. IoT cloud data.

5. CONCLUSION

In conclusion, the IoT-based QR Code Access Control and Payment System developed using Arduino and ESP8266 modules offers a robust and efficient solution for modern access management needs. By integrating QR code and RFID card scanning, real-time data processing, and automated transaction handling, the system enhances security and convenience in various applications such as parking facilities, public transport, and secure entry points. The successful implementation and functionality of this project demonstrate the practical applicability and scalability of IoT technologies in access control systems. Future improvements could focus on enhancing system security with advanced encryption techniques, incorporating biometric verification for multifactor authentication, expanding compatibility with various payment gateways, and optimizing the user interface for better accessibility and user experience. Additionally, integrating machine learning algorithms could improve the system's ability to detect and respond to fraudulent activities, further enhancing its reliability and effectiveness.

REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

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

[13] 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. cloud-of-things environments," Computers & Security, vol. 74, pp. 340 –354, 2018.

[14] 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.

[15] 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.

[16] 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.

[17] R. Terebes, O. Lahlou, and R. Enseirb, "Camera phone based barcode decoding system," ACTA Technica Napocensis, vol. 49, no. 3, pp. 57–62, 2008.

[18] A. Zamberletti, I. Gallo, and S. Albertini, "Robust angle invariant 1d barcode detection," in Proc. 2nd IAPR Asian Conf. Pattern Recognit., 2013, pp. 160–164.

[19] G. Sörös and C. Flörkemeier, "Blur-resistant joint 1D and 2D barcode localization for smartphones," in Proc. 12th Int. Conf. Mobile Ubiquitous Multimedia, 2013, pp. 1–8.

[20] A. Sharif, G. Zhai, J. Jia, X. Min, X. Zhu, and J. Zhang, "An accurate and efficient 1D barcode detector for medium of deployment in IoT systems," IEEE Internet Things J., vol. 8, no. 2, pp. 889–900, Jan. 2021.

[21] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 779–788.

[22] Z. Tian, C. Shen, H. Chen, and T. He, "FCOS: A simple and strong anchor-free object detector," IEEE Trans. Pattern Anal. Mach. Intell., early access, Oct. 19, 2020, doi.

[23] A. Hiller and R. T. Chin, "Iterative Wiener filters for image restoration," in Proc. Int. Conf. Acoust. Speech Signal Process., 1990, pp. 1901–1904.

[24] S. Yahyanejad and J. Ström, "Removing motion blur from barcode images," in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops, 2010, pp. 41–46.

[25] M. Tan and Q. V. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in Proc. ICML, 2020, pp. 6105–6114.

[26] T. Lin, P. Dollár, R. B. Girshick, K. He, B. Hariharan, and S. J. Belongie, "Feature pyramid networks for object detection," 2016. [Online]. Available: arxiv.abs/1612.03144.

[27] S. Liu, L. Qi, H. Qin, J. Shi, and J. Jia, "Path aggregation network for instance segmentation," 2018. [Online]. Available: arxiv.abs/1803.01534.