Prototyping the QR Code-based pandemic guard system

Varsha Patil[1], M S Vanjale[2], V R Pawar [3], Abhishek Negi [4]

***Abstract*—The widespread spread of COVID-19 has made a significant impact on people's normal activities and routines in numerous ways. Institutions such as schools and offices must take measures to limit the spread of infectious diseases among their staff and students. Better preparation for future pandemic viruses and the use of technical solutions to improve the working environment during a pandemic are both essential. For the protection of the working professional, we have proposed a Pandemic Guard System. The proposed work takes advantage of contactless QR code scanning as a means of prevention. In this work, facial detection methods and QR code scanning replace the use of biometric fingerprint scanners for contactless scanning. Automatic scanning, preserving safe social distances, hand sanitisation, and other methods are used to take care of employees. There are two stages to implementation; the first one involves using implementing modules at the company bus, and the second one focuses on the implementation of the modules at the company or workplace entrance. Additionally, this work delivers many layers of authenticity through the use of face recognition and QR codes.**

Further, face recognition-based attendance and QR code-based technological hardware and software coexistence are connected to real-time data through the Firebase database for biometric attendance. Thus, we are proposing a more secure system to ensure e-contactless operations.

Keywords*—Face detection. QR code, Attendance monitoring system, COVID-19, Viruses (medical), Pandemics, Coronavirus, pandemic, global economic impact, disaster management, *Temperature sensing, Contactless sanitisation

I. INTRODUCTION

The global outbreak of the COVID-19 pandemic severely disrupted conventional modes of social interaction, communication, and workplace operation. High population density environments such as offices, educational institutions, and public transport hubs, faced unprecedented challenges in maintaining operational continuity while ensuring health and safety.

Experts have indicated that the social and organisational impacts of the pandemic are long-lasting, necessitating sustained preventive measures rather than short-term interventions. In such scenarios, ensuring workplace safety requires not only significant resources and coordinated task forces but also careful planning and adoption of intelligent technological solutions.

Importantly, during a pandemic, essential work activities cannot be suspended indefinitely, highlighting the need for safe and efficient operational mechanisms.

One of the critical challenges identified during the pandemic was the reliance on contact-based biometric systems, particularly fingerprint-based attendance and access control mechanisms. These systems pose a high risk of virus transmission due to repeated physical contacts and shared surfaces. Consequently, there is a growing need to replace such mechanisms with contactless, secure, and fraud-resistant alternatives that can ensure both user authentication and health safety.

The implementation of intelligent safety measures in workplaces presents a promising approach to mitigating infection risks while maintaining productivity. Contactless technologies, combined with automated verification and monitoring, can enable safe enforcement of social distancing and access control protocols. In this context, integrating multiple authentication layers improves system robustness and reduces the likelihood of unauthorised access or identity misuse.

This work proposes a Pandemic Guard System designed to support contactless operations in workplaces such as offices, colleges, schools, and other organisational premises. The proposed system replaces traditional fingerprint-based attendance systems with a contactless framework that combines QR code–based identity verification and face recognition to ensure authenticity and detect fraudulent entry attempts. Additionally, the system supports attendance tracking and sanitisation enforcement at entry points, including organisational entrances and transportation access points such as buses.

The primary contribution of this work lies in the design and prototyping of a multi-layer contactless authentication and attendance system that enhances workplace safety during pandemic conditions. By employing QR code scanning and face recognition, the proposed solution minimises physical contact, improves security, and supports safer operational practices. The system demonstrates how intelligent application of contactless technologies can serve as an effective preventive measure for safeguarding working professionals during global health emergencies.

II. Literature survey

The COVID-19 pandemic created an urgent demand for automated and contactless systems capable of enforcing access control, performing health screening, and maintaining digital records of human movement in public and institutional environments. Embedded gateway systems emerged as a practical foundation for such applications due

---

Varsha Patil[1], M S Vanjale[2], V R Pawar [3], Abhishek Negi [4]
Affiliations:
Authors [1,2,4] : AISSMS Institute of Information Technology,
Authors [3]: BVCOEW, Pune
Corresponding Author Email id: varshapatil101@gmail.com
Manuscript received December 4, 2025 ; Revised January 3, 2026
Accepted January 26, 2026

to their low cost, modularity, and real-time processing capability. Embedded gateway systems have been explored to overcome limitations of traditional access control mechanisms. Jiaxin et al. proposed a cloud-based smart gate system in which a Raspberry Pi serves as the embedded hardware controller to enable remote door unlocking and access management. Their architecture integrates a cloud management platform, mobile front end, and Raspberry-Pi-based control unit, demonstrating the feasibility of low-cost embedded gateways for real-time access control applications [1]. Subsequently, Hassan et al. evaluated the performance of Raspberry Pi. Their results demonstrated that Raspberry Pi can reliably support low-latency data processing and real-time decision-making at the edge, validating its suitability for time-critical IoT applications[2]. Beyond access control–oriented implementations, the suitability of Raspberry Pi for real-time IoT edge processing has been systematically evaluated. Hassan et al. analyzed the performance of Raspberry Pi as an IoT edge signal processing device in a real-time system. Their findings indicate that Raspberry Pi can support time-critical edge-level processing tasks, which is relevant for gateway-based systems requiring real-time decision-making [2]. Beyond gateway-centric access control systems, embedded platforms have also been explored as distributed sensor web nodes. Vujović and Maksimović investigated the use of Raspberry Pi as a sensor web node for home automation, demonstrating its capability to integrate sensing, local data processing, and network communication within a sensor web architecture. Their results showed that Raspberry Pi can reliably support real-time data acquisition and distributed monitoring tasks, reinforcing its applicability in IoT-based monitoring and smart environment systems [3]. However, these gateway-oriented works did not address pandemic-specific requirements such as health screening, digital traceability, or identity-bound access enforcement.

Biometric identification, particularly face detection and recognition, has been extensively explored for access control and attendance systems. Gupta *et al.* implemented a face detection and recognition framework on Raspberry Pi, demonstrating that classical computer vision techniques can achieve reliable performance on resource-constrained embedded platforms [4]. Additional studies confirmed that lightweight face recognition approaches remain suitable for embedded and IoT environments where computational resources are limited [5]. While biometric authentication effectively prevents impersonation, most pre-pandemic implementations focused solely on identity verification and did not integrate health-related data or epidemiological logging. As a result, biometric-only systems are insufficient for pandemic scenarios that require simultaneous health screening and traceability.

Non-contact body temperature measurement became a core component of COVID-19 screening strategies. Goh et al. presented the design of a low-cost non-contact infrared thermometer incorporating range compensation to reduce distance-dependent measurement errors. Their work showed that accurate temperature sensing can be achieved using inexpensive components, making the approach suitable for embedded and contactless screening application [6].

Infrared temperature sensors enable rapid and contactless screening, thereby reducing infection risk at entry points. Nevertheless, temperature-only screening systems operate in isolation and do not associate measurements with verified identities or maintain structured historical records, limiting their usefulness for access authorisation and long-term health analytics.

Several IoT-based solutions focused on mitigating virus transmission through hygiene automation and preventive mechanisms. Rusimamto et al. proposed an automatic hand sanitiser container designed to reduce surface contact and improve hygiene compliance during the COVID-19 pandemic. Their system employs sensor-based actuation to dispense sanitizer without physical contact, demonstrating the effectiveness of simple IoT-enabled automation as a preventive public-health measure in shared environments [7]. Although effective as a preventive measure, such systems function independently and do not provide authentication, access decision logic, or centralised monitoring. Broader IoT surveys emphasised that effective pandemic-response systems must integrate sensing, identity management, and data analytics rather than operating as isolated modules . Ndiaye et al. presented a comprehensive survey of Internet of Things applications deployed during the COVID-19 pandemic, covering areas such as health monitoring, access control, contact tracing, and smart infrastructure. The study analysed system architectures, communication technologies, and data management strategies adopted across different pandemic-response use cases with challenges emphasizing the need for integrated and resilient IoT frameworks for public health emergencies [8].

QR code–based digital identification gained widespread adoption during COVID-19 because of its simplicity, scalability, and ease of deployment. Nakamoto *et al.* presented a QR code–based contact tracing framework demonstrating how digital check-ins can support large-scale containment strategies and facilitate a gradual return to normal activities. Their approach enables digital check-ins at public locations, allowing efficient logging of human movement and rapid identification of potential exposure events. The evaluation demonstrated that QR-based tracing offers a scalable and practical alternative to proximity-based tracing methods, particularly in controlled entry environments [9].

Radhi further explored the use of QR codes combined with IoT-enabled mobile devices to reduce physical interaction and improve epidemic prevention. The study demonstrated that QR-based identification combined with mobile IoT platforms can effectively enhance compliance and traceability during pandemic scenarios.[10].

Large-scale reviews of digital contact tracing applications evaluated systems deployed after the initial phase of the COVID-19 pandemic, including QR-based and mobile app–based approaches. These studies confirmed the practical effectiveness of digital tracing while also identifying critical challenges related to user adoption, privacy preservation, interoperability, and public trust [11], [12].

Cross-disciplinary reviews and best-practice guidelines emphasised the importance of interoperability, transparency, and system-level integration in digital contact tracing solutions [13].

Analytical and epidemiological studies demonstrated that digital contact tracing can significantly reduce viral transmission when identity and interaction data are captured

rapidly and accurately. Ferretti *et al.* showed that timely digital tracing could play a decisive role in epidemic control when supported by efficient data collection mechanisms [14]. AI and IoT applications for combating COVID-19 identified integrated screening, monitoring, and access control systems as key research directions [15]. Studies on smart and sustainable cities further highlighted the role of IoT-enabled infrastructures and cities in managing public health emergencies[16]. International health organisations have also issued guidance on the responsible deployment of digital tracing and screening technologies. The World Health Organisation released technical guidance on digital tools for COVID-19 contact tracing, emphasising accuracy, scalability, and public trust [17]. Ethical considerations and privacy-preserving design principles were further articulated to guide the use of digital proximity tracking technologies [18]. Ethical governance and public acceptance are critical to the success of digital contact tracing systems. Studies highlighted the need for strong privacy safeguards, transparent data governance, and user trust to ensure responsible deployment and widespread adoption [19], [20].

III. Summary of Literature Survey

The rapid spread of COVID-19 highlighted the need for contactless, automated, and scalable pandemic prevention systems capable of screening individuals at public and institutional entry points.

Research Gap

From the reviewed literature, several research gaps are evident. Existing systems typically address only a single dimension of pandemic management, such as gateway automation[1], biometric identification[4], temperature screening[6], hygiene automation[7], or QR-base tracing[9],[10]. Weak identity binding remains a limitation in QR-centric systems, while biometric-only approaches lack epidemiological traceability. Moreover, relatively few studies present a unified embedded architecture that integrates identity verification, health screening, access control, and centralised analytics with quantitative performance evaluation.

Motivated by these gaps, this work proposes a QR Code-based Pandemic Guard System that integrates QR-based digital identity, face recognition, and non-contact infrared temperature screening within a unified embedded and IoT-enabled framework with an attendance facility.

IV. Methodology

A. Overall System Architecture

Figure 1 illustrates the proposed QR Code–based Pandemic Guard System architecture and data flow. The system follows a distributed architecture comprising edge devices, a mobile application, and two backend servers. Edge devices deployed at entry points perform QR code scanning, face detection, and non-contact temperature measurement, while backend servers manage authentication, data validation, and attendance records.

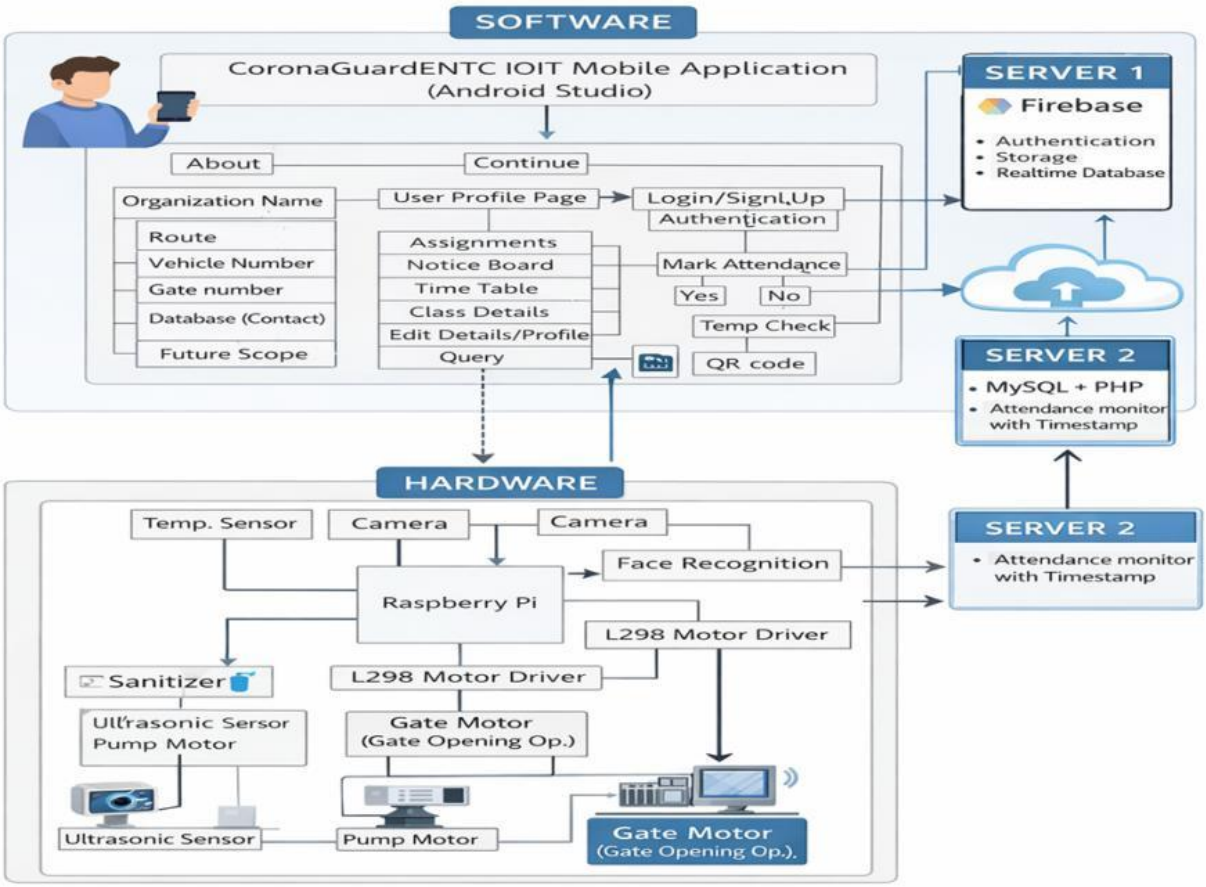

Figure 1: Proposed Pandemic Guard System Conceptual system architecture and data flow (hardware and software integration

A mobile application generates a unique QR code for each authenticated user. Figure 2 shows the screenshots of mobile app for students (available for institutional use and scope).

Figure 2: QR code generated for student from his login id on his mobile

This QR code is scanned at the edge device, where local verification is performed before access authorization. Attendance and event data are synchronised with backend servers in real time to ensure secure and consistent system operation.

QR Code Encoding and Decoding Mechanism

The system generates a unique QR code for each user by embedding a compact data payload that includes a user identifier, generation timestamp, and a health compliance flag. This structured representation enables precise identity association while ensuring that the QR code remains valid only within a defined time window. The encoded information is serialized into a lightweight textual format to support rapid decoding on embedded hardware. The payload structure can be represented as

$$\mathrm{QR}_{payload} = \{ID_u, T_s, H_s\} \quad \ldots 1$$

where ID_u corresponds to the registered user, T_s denotes the time of QR generation, and H_s indicates health clearance status.

QR codes are generated in accordance with standard specifications using a mid-range version and **error correction level Q**, which enhances tolerance to partial damage and environmental variations during scanning. At the entry point, the camera module captures the QR image, and the embedded processor decodes and validates the payload before forwarding it for server-side verification. This approach ensures dependable, low-latency QR processing while maintaining compatibility with resource-constrained embedded access systems.

B. System Design for Entry-Mounted Module

The entry-mounted module is installed at organisational entrances and exits. Integrated hardware includes a Raspberry Pi Zero W, camera module, infrared temperature sensor, gate motor, and sanitizer pump. Device interfacing is achieved using standard IoT communication protocols, enabling coordinated data exchange and control, as shown in Figure 3.

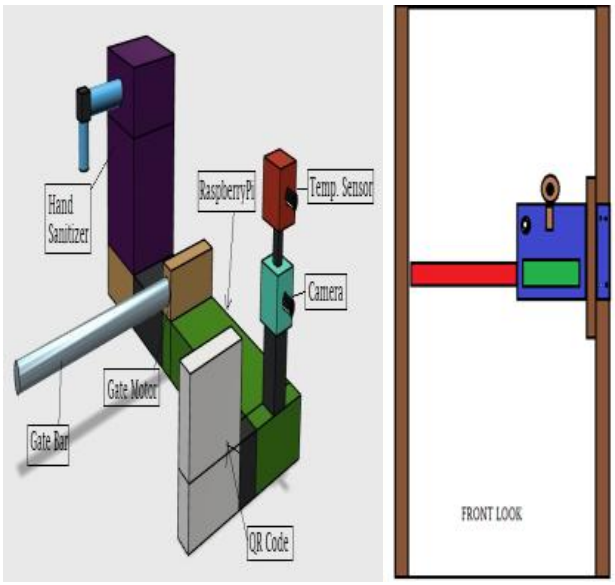

Figure 3: Interfacing of hardware for gate assembly

C. System Design for Bus-Mounted Module

The bus-mounted module is designed for public transport environments. A QR scanner installed near the bus entrance reads the user's QR code generated via the mobile application. Fare and user information entered in advance are transmitted to the backend server for ticket deduction and logging. The seating arrangement enforces physical distancing by keeping adjacent seats vacant. Figure 4 and 5 shows the prototype implementation of the bus-mounted module.

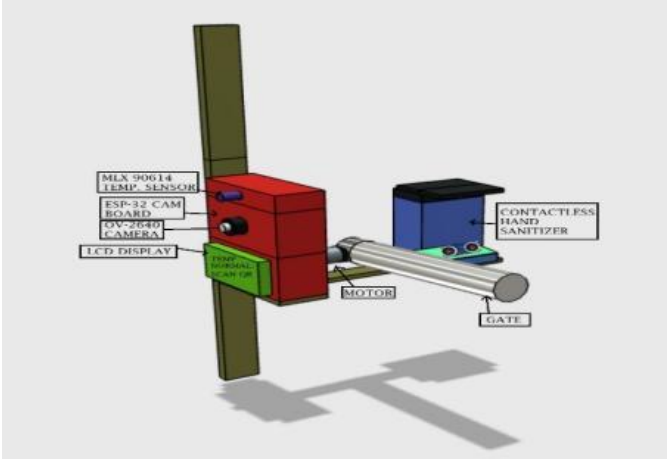

Figure 4: Integrated hardware attached to the bus door gate.

The alignment of the seats is done in such way that one seat will be kept vacant in the vicinity of the person. Figure 5 shows the prototype for the bus seating arrangement.

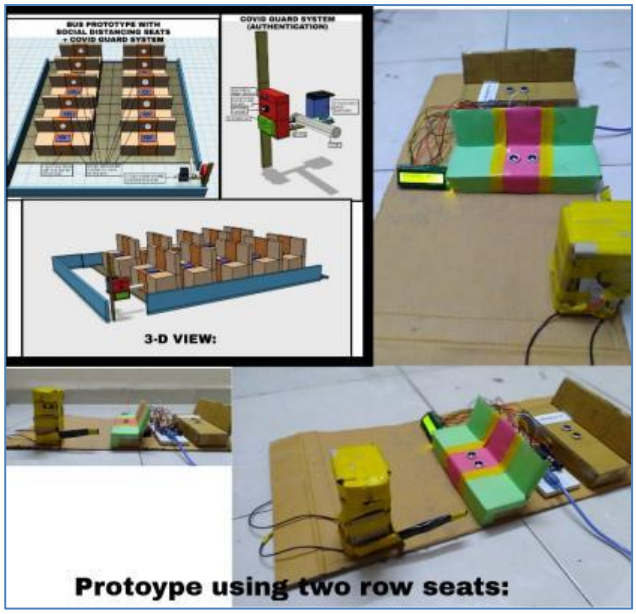

Figure 5: Prototype model for the bus seats with social distancing

.D. Hardware–Software Integration

The Raspberry Pi Zero W acts as the central edge controller, interfacing with the camera for QR detection and face capture, an infrared temperature sensor for contactless screening, and actuators for gate control and sanitiser dispensing. The assembly is arranged inside module as shown in figure 6.

Figure 6: Sanitizer battery and allied arrangement inside the module

QR codes are generated by encoding unique user-specific data into a matrix format, which is decoded at the edge device and validated by the backend server prior to access authorization.

E. Mobile Application (CGEI)

The Campus Gate Entry Interface (CGEI) mobile application supports user registration, secure login, and QR code generation. Access to the QR code is protected using device-level authentication (e.g., fingerprint verification) on the user's personal smartphone, eliminating the need for shared biometric devices. The application interfaces with backend servers for data synchronisation and attendance updates..Figure 7 shows various steps during QR code generation on mobile application and detection via Raspberry Pi Cam.

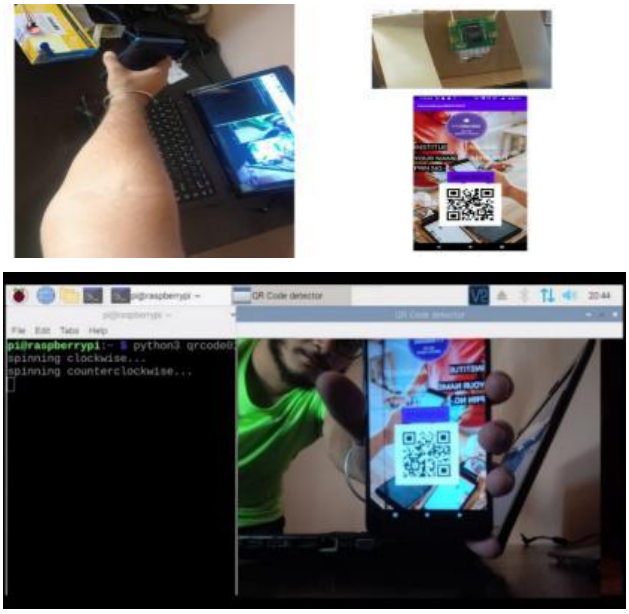

Figure 7: various steps during QR code generation on mobile application and detection via Raspberry Pi Cam

F. Backend Server Architecture

The backend infrastructure is divided into two servers to improve scalability and reliability. Server 1 manages user authentication, QR validation, and application data using a cloud-based NoSQL database (Firebase). Server 2 communicates with edge devices and maintains real-time attendance logs with timestamps. This separation of responsibilities reduces latency and improves system robustness.

G. Face Detection and Authentication

The method of face detection and attendance monitoring is similar to [4].Face detection is implemented using the Haar Cascade classifier on the Raspberry Pi. The registered uses are preregistered in the system with face files . When a registered user comes in front of the camera, detected facial regions are extracted using bounding boxes and compared with stored facial templates to verify identity. This additional authentication layer prevents QR code misuse while maintaining real-time performance on embedded hardware. Figure 8 shows face detection captured on the setup .

Figure 8: Face detection implemented

Proposed Face Detection Approach:

The proposed system employs a Haar Cascade–based approach for face detection to achieve efficient real-time performance on embedded hardware. The method relies on rectangular intensity features whose values are rapidly computed using an integral image representation, where the integral image $II(x, y)$is expressed as

$$II(x, y) = \sum_{x' \le x,\, y' \le y} I(x', y') \ldots 2$$

This method is allowing feature evaluation with constant computational cost. A cascade structure of weak classifiers, optimised through AdaBoost training, enables early rejection of non-facial regions, thereby minimising unnecessary processing.

This approach is selected in preference to HOG- or CNN-based techniques because it offers significantly lower computational and memory requirements, making it suitable for CPU-based platforms such as Raspberry Pi. While deep learning models provide higher robustness under complex conditions, their resource demands hinder real-time execution on low-cost gateways. The Haar Cascade method, therefore, ensures timely face detection with minimal overhead, supporting reliable authentication in access-controlled environments.

H. Database Management

A hybrid database architecture is employed. Facial images and extracted features are stored in a structured SQL database (MySQL), while QR data, attendance logs, and timestamps are stored in a real-time NoSQL database (Firebase). This combination ensures efficient storage, fast access, and scalability.

Figure 9 shows the mobile application screen during various steps, such as the QR code after passing temperature and fingerprint authentication checks. captured on the setup.

Figure 9: Mobile Application screen during various steps, such as QR code after passing temperature and fingerprint authentication checks.

V. RESULTS AND SYSTEM OPERATION

A. Operational Workflow

After system deployment, multiple users were registered through the CGEI application. Each user was assigned a unique QR code linked to their profile. The operational sequence is as follows:

1. User logs into the mobile application using credentials.
2. Device-level authentication enables QR code access.
3. QR code is scanned at the edge device.
4. Face detection and temperature measurement are performed locally.

5. Upon successful verification, access is granted and attendance is recorded.
6. Gate operation and sanitizer dispensing are triggered automatically.

B. Contactless Authentication and Access Control

The system successfully enabled contactless authentication using QR code scanning combined with face verification. Temperature screening was performed without physical contact, and access authorization occurred only after all checks were satisfied. The integration of these steps reduced physical interaction and improved operational safety.

C. Real-Time Attendance and Data Synchronisation

Attendance data and event timestamps were updated in real time on the backend servers. The dual-server architecture ensured reliable communication between edge devices and cloud services, enabling consistent data logging across multiple entry points.

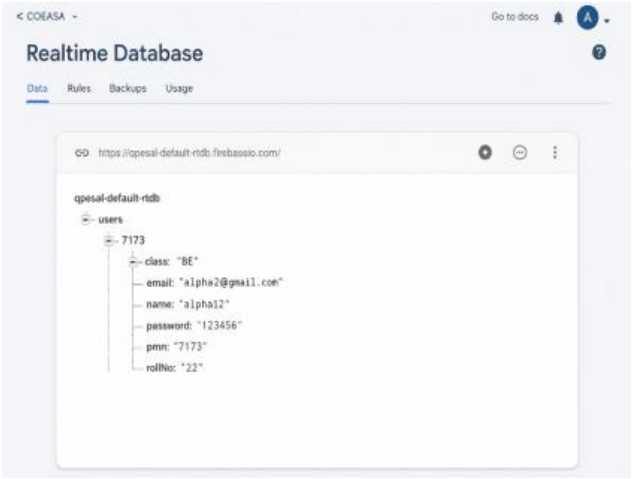

Figure 10: Real-time database collection

D. IoT-Based Device Coordination

All connected devices operated in a coordinated manner through IoT protocols. Upon successful authentication, gate motors and sanitizer pumps were activated automatically. This demonstrated effective integration of sensing, decision-making, and actuation within a single embedded system.

E. Deployment Validation

The system was validated across multiple deployment scenarios, including bus entrances, seating arrangements, and organisational entry and exit points. The results confirmed reliable QR detection, face recognition, temperature measurement, and automated access control under real-world conditions**.**

REFERENCES

[1] Y. Jiaxin, W. Zhong, and L. Hong, "Smart gate system design and implementation based on cloud platform," Procedia Computer Science, vol. 154, pp. 40–46, 2019, doi: 10.1016/j.procs.2019.06.008.

[2] A. Hassan, H. Nahar, and W. Md Shah, "Performance evaluation of Raspberry Pi as an IoT edge signal processing device for a real-time flash flood forecasting system," Int. J. Adv. Comput. Sci. Appl. (IJACSA), vol. 13, no. 10, pp. 1–10, 2022.

[3] V. Vujović and M. Maksimović, "Raspberry Pi as a sensor web node for home automation," Comput. Electr. Eng., vol. 44, pp. 153–171, 2015, doi: 10.1016/j.compeleceng.2015.01.019.

[4] I. Gupta, V. Patil, C. Kadam, and S. Dumbre, "Face detection and recognition using Raspberry Pi," in Proc. IEEE Int. WIE Conf. on Electrical and Computer Engineering (WIECON-ECE), Pune, India, Dec. 2016, pp. 83–86, doi: 10.1109/WIECON-ECE.2016.8009092.

[5] Patil, V.K., Pawar, V.R., Randive, S. *et al.* From face detection to emotion recognition on the framework of Raspberry pi and galvanic skin response sensor for visual and physiological biosignals. *Journal of Electrical Systems and Inf Technol* 10, 24 (2023). https://doi.org/10.1186/s43067-023-00085-2

[6] N. W.-J. Goh, J.-J. Poh, J. Y. Yeo, B. J.-J. Aw, S. C. Lai, J. J. W. Cheng, C. Y. L. Tan, and S. K. E. Gan, "Design and development of a low cost, non-contact infrared thermometer with range compensation," OSF Preprints, 2020, doi: 10.31224/osf.io/3fd7.

[7] P. W. Rusimamto, N. Nurhayati, E. Yundra, R. Rahmadian, A. Widodo, and M. A. Dermawan, "Automatic hand sanitizer container to prevent the spread of corona virus disease," in Adv. Eng. Res., vol. 196, Proc. Int. Joint Conf. on Science and Engineering (IJCSE 2020), Surabaya, Indonesia, Oct. 2020, pp. 63–68, doi: 10.2991/aer.k.201124.011.

[8] M. Ndiaye, S. S. Oyewobi, A. M. Abu-Mahfouz, G. P. Hancke, A. M. Kurien, and K. Djouani, "IoT in the wake of COVID-19: A survey on contributions, challenges and evolution," IEEE Access, vol. 8, pp. 186821–186839, Oct. 2020, doi: 10.1109/ ACCESS.2020.3030090.

[9] I. Nakamoto, S. Wang, Y. Guo, and W. Zhuang, "A QR code–based contact tracing framework for sustainable containment of COVID-19: Evaluation of an approach to assist the return to normal activity," JMIR mHealth uHealth, vol. 8, no. 9, Art. no. e22321, Sep. 2020, doi: 10.2196/22321.

[10] Radhi, A. A. (2022). Use QR Code and IoT Mobile Devices to Prevent the Spread of an Epidemic (COVID-19). *International Journal of Interactive Mobile Technologies (iJIM)*, *16*(12), pp. 127–136. https://doi.org/10.3991/ijim.v16i12.32125

[11] M. Shahroz, M. Ahmad, M. S. Younis, N. Ahmad, M. N. Kamel Boulos, R. Vinuesa, and J. Qadir, "COVID-19 digital contact tracing applications and techniques: A

review post initial deployments," Transportation Engineering, vol. 5, Art. no. 100072, Sep. 2021, doi: 10.1016/j.treng.2021.100072.

[12] A. Akinbi, M. Forshaw, and V. Blinkhorn, "Contact tracing apps for the COVID-19 pandemic: A systematic literature review," Health Inf. Sci. Syst., vol. 9, no. 1, Art. no. 18, 2021, doi: 10.1007/s13755-021-00147-7.

[13] World Health Organization, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing," WHO, Geneva, Switzerland, Tech. Rep., May 2020.

[14] Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science. 2020 May 8;368(6491):eabb6936. doi: 10.1126/science.abb6936. Epub 2020 Mar 31. PMID: 32234805; PMCID: PMC7164555.

[15] V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.

[16] A. Sharifi, A. R. Khavarian-Garmsir, and S. Kummitha, "Contributions of smart city solutions and technologies to resilience against the COVID-19 pandemic: A literature review," Sustainability, vol. 13, no. 10, Art. no. 5311, May 2021, doi: 10.3390/su13105311.

[17] World Health Organization, "Digital tools for COVID-19 contact tracing," WHO, Geneva, Switzerland, Tech. Rep., Jun. 2020.

[18] U. Gasser, M. Ienca, J. Scheibner, J. Sleigh, and E. Vayena, "Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid," Lancet Digital Health, vol. 2, no. 8, pp. e425–e434, Aug. 2020, doi:10.1016/S2589-7500(20)30137-0.

[19] U. Gasser, M. Ienca, J. Scheibner, J. Sleigh, and E. Vayena, "Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid," Lancet Digital Health, vol. 2, no. 8, pp. e425–e434, Aug. 2020, doi:10.1016/S2589-7500(20)30137-0.

[20] S. Altmann, L. Milsom, H. Zillessen, et al., "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study," JMIR mHealth uHealth, vol. 8, no. 8, Art. no. e19857, Aug. 2020, doi: 10.2196/19857.