Development of a Biometric Toilet Monitoring System for Final Examinations: A Socio-Technical Perspective

Muhammad Syafiq Shafie[#], Radi Husin Ramlee[#1], Muhammad Idzdihar Idris[#], Aine Izzati Tarmizi[*], Mohd Syafiq Mispan[#], Muhammad Raihaan Kamarudin[#]

[#]Fakulti Technology dan Kejuruteraan Elektronik dan Computer, University Technical Malaysia Melaka (UTeM), Melaka, Malaysia.

[*]Fakulti Technology Kejuruteraan Electric, University Technical Malaysia Melaka (UTeM), Melaka, Malaysia.

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.910000652

Received: 26 October 2025; Accepted: 04 November 2025; Published: 20 November 2025

ABSTRACT

Examinations are high-stakes environments in which fairness and trust are paramount. Traditional manual approaches to controlling access to restroom facilities during examinations often require invigilators to record the names and entry times of candidates on paper. Such manual logging leaves opportunities for bias, error or impersonation. A biometric toilet monitoring system was designed to address these vulnerabilities by coupling fingerprint authentication with real-time data synchronization to a web server. This paper revisits that engineering project through a socio-technical perspective. It traces the motivations for automating restroom access, details the hardware and software architecture, reproduces key figures and tables, reports empirical performance findings and situates the system within broader debates about surveillance, consent, privacy and digital inclusion. Ultimately the work demonstrates that a thoughtfully implemented biometric access system can enhance exam integrity while raising questions about equity, autonomy and trust.

Keywords - Biometrics; toilet monitoring; access control; examinations; socio-technical systems; surveillance; digital inclusion.

INTRODUCTION

Examinations are essential sites where educational institutions endeavour to reproduce meritocratic ideals. Yet such ideals can be undermined by lax procedural controls. A seldom-examined aspect of exam administration concerns how candidates leave the hall to visit restrooms. Invigilators often rely on handwritten logs to record departures and returns, noting only the candidate's name and time. While this practice provides a record, it is susceptible to inaccuracies, delays and intentional abuse. Students may impersonate peers, collude to smuggle notes or orchestrate unauthorised absences, and invigilators may exercise inconsistent judgment when verifying identities. Moreover, because exam halls may contain dozens of candidates, manual logging increases cognitive load for proctors who must simultaneously monitor the room and track restroom usage.

Biometric technologies promise to automate identity verification and record keeping. Fingerprint scanners in particular are inexpensive, unobtrusive and widely understood. By coupling a fingerprint sensor to a microcontroller and linking it with a database, it becomes possible to grant or deny restroom access based on pre-registered templates, log entry and exit times automatically and enforce policies such as maximum occupancy. In the original engineering report a system was developed for Universiti Teknikal Malaysia Melaka and tested with a small cohort of volunteer students. This paper explores why such a system is needed, how it was designed and what social implications it carries.

From a sociological perspective, toilets are more than functional necessities; they reflect cultural norms, hierarchies and control. Studies of public facilities reveal that access is often a site where class, gender and disability intersect. In exam settings the stakes are heightened because leaving the hall without oversight can enable dishonesty. A biometric access system thus sits at the intersection of bodily regulation and educational assessment, leveraging the uniquely intimate nature of fingerprints to enforce compliance. Such systems raise ethical questions about data protection, consent and surveillance. Social-science scholarship emphasises that biometric technologies embody power relations; the same device that prevents cheating can also normalise suspicion and reduce trust. This duality underscores the need for critical examination.

LITERATURE REVIEW

Technical Foundations

Biometric identification has been the subject of intensive research for decades. Jain et al. provide a comprehensive introduction to the principles of biometrics, analysing modalities such as fingerprint, face, iris and voice recognition [1]. They highlight that fingerprints remain the most mature modality due to their uniqueness, stability and ease of acquisition [1]. Ahmed et al. examine failures in manual access control and argue that such systems rely on human vigilance and therefore suffer from fatigue and bias [2]. Their qualitative study of office buildings found that untrained security guards frequently overlook suspicious behaviour. Ali et al. analyse the implementation of biometric access in educational institutions; their case study reports improved punctuality and reduced impersonation but also resistance among faculty who perceived fingerprint scanning as intrusive [3]. Malathi and Umamaheswari summarise advances in fingerprint recognition algorithms and note that machine learning has improved matching speed and accuracy [4], while Choi et al. review deep learning techniques and discuss trade-offs between computational complexity and mobile deployment [5].

Security and Privacy Considerations

Zheng and Valli identify critical aspects of biometric security such as spoofing, template storage and liveness detection [6]. Lin surveys sensor technologies and notes that improvements in optical and capacitive sensors are making high-quality fingerprint scanning more accessible [7]. Das and Sengupta explore the integration of biometric systems with the Internet of Things and highlight challenges around network latency, encryption and interoperability [8]. These studies demonstrate that design choices—not just algorithmic sophistication—affect the security and reliability of biometric systems.

Scholars in surveillance studies argue that biometric systems may normalise suspicion and expand institutional reach. For example, Lyon describes surveillance as social sorting, where individuals are categorised and treated differently based on data profiles [9]. Whitley and Kroener argue that consent in biometric systems is often coerced when access to essential services depends on compliance [10]. Foucault’s notion of biopower can be applied here: the state or institution exerts control over bodies by capturing corporeal features and using them to govern movement [11]. These frameworks inform our socio-technical analysis in Section V.

Comparative Projects and Technologies

The engineering report compared several Arduino-compatible boards for the microcontroller platform. Table 1 summarises typical characteristics. The ESP32 was chosen because its dual-core processor, integrated Wi-Fi and Bluetooth, large memory and low cost make it suitable for networked biometric applications. The AS608 optical fingerprint sensor provides reliable enrolment and verification by capturing high-resolution images and extracting minutiae features. On the software side, the Arduino IDE was used for firmware development and XAMPP for hosting the web interface due to their ease of use and cross-platform availability.

Table 1 Comparative Features Of Microcontroller

Board	CPU	Flash	I/O	Wireless	Notes
Arduino Uno	16 MHz	32 kB	14	None	Simple, limited resources
Arduino Mega	16 MHz	256 kB	54	None	Many I/O pins, no wireless
NodeMCU ESP8266	80–160 MHz	4 MB	17	Wi-Fi	Single-core, limited RAM
ESP32	240 MHz	4 MB	34	Wi-Fi/ Bluetooth	Dual-core, integrated wireless

Data Protection and Legal Frameworks

The General Data Protection Regulation (GDPR) in the European Union and Malaysia's Personal Data Protection Act (PDPA) classify fingerprint templates as sensitive personal data. Institutions using biometrics must ensure informed consent, implement encryption, and define retention periods. The ISO/IEC 24745 standard recommends separating biometric templates from personal identifiers and employing liveness detection. Failure to follow these guidelines can lead to legal liability and erosion of trust.

Socio-Technical Frameworks

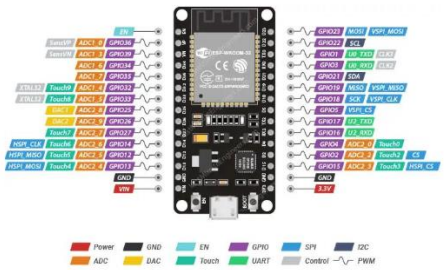
Technology adoption is mediated by social context. The Technology Acceptance Model (TAM) suggests that perceived usefulness and ease of use influence whether individuals adopt a technology. Actor-Network Theory (ANT) emphasises that adoption emerges from interactions among human and non-human actors (e.g., microcontrollers, policies, exam rules). Both frameworks highlight that a biometric toilet monitor is not just a technical artefact but part of a network of practices, regulations and cultural values. Wajcman cautions against technological determinism; the effects of technology are negotiated and contingent upon context [12].

METHODOLOGY

Hardware Design

The system's core is an ESP32 microcontroller (Figure 1), selected for its processing power, memory and integrated wireless communication. It interfaces with an AS608 optical fingerprint sensor (Figure 2) via a serial connection.

Fig. 1 ESP32 microcontroller



For user feedback, it employs a 0.96-inch OLED display and a 16×2 LCD display. A push button triggers the scanning process. Figure 3 illustrates the block diagram of the system, showing the flow between inputs

(fingerprint sensor, button), the ESP32 control unit and outputs (OLED, LCD), with communication to a PHP server via Wi-Fi. Wiring is implemented on a breadboard (Figure 4), and components are housed in a custom enclosure designed to balance ergonomics and hygiene. Figure 5 shows the web interface for managing users.

Fig. 2 Optical fingerprint sensor

Fig. 3 System block diagram

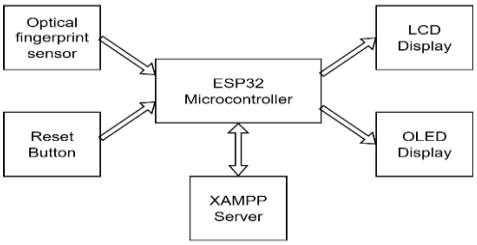
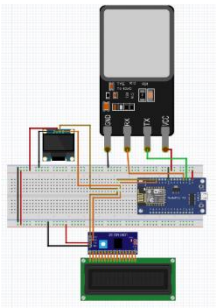


Fig. 4 System hardware



Firmware and Server

Firmware was developed using the Arduino IDE. On startup, the ESP32 connects to Wi-Fi, synchronises its clock with a Network Time Protocol server and awaits a button press. When the button is pressed, the sensor scans a fingerprint and returns a template ID and confidence score. If the template matches a stored user, the ESP32 increments that user's login count, displays their name on the LCD and sends a JSON payload to the server. If no match is found, the OLED instructs the user to retry. Registrations require an admin token: the device generates a new user ID, collects metadata (matrix number, full name) and enrols two samples. The server side uses XAMPP (Apache, MySQL, PHP) to host a database and a web interface. Endpoints support operations to register users, record logins/logouts and display logs. These design decisions were informed by the report's emphasis on low cost and ease of use.

Fig. 5 Web interface for managing users

Participant Recruitment and Procedure

Ten volunteer students from the Computer Engineering programme participated in the trial. Each volunteer provided informed consent after being told that their fingerprint templates would be stored only on the sensor. They registered their fingerprints and then simulated restroom use by logging in and out repeatedly under exam conditions. Participants completed at least five login/logout cycles. Observations and informal feedback were collected. The small sample size limits generalisability but provides initial insights into usability and perceptions.

Data Collection and Analysis

The following metrics were recorded: (1) fingerprint recognition success rate, (2) fingerprint match and server response times, and (3) total time to log restroom visits compared to manual handwriting logs. Logs were automatically stored in the MySQL database. Qualitative feedback was summarised to identify themes such as fairness, privacy concerns and ease of use.

RESULTS

Fingerprint Recognition Accuracy

Ten scanning attempts were conducted. Table 2 shows whether each attempt succeeded on the first try or required a second attempt. The system achieved a 90 % first-try success rate and 100 % success after a second attempt, matching the original report. Failures were due to dry or oily fingers and were corrected by repositioning.

Table 2 Fingerprint Scanning Test Results

Attempt	Outcome	Reason / note
1	Success on 1st try	—
2	Success on 1st try	—
3	Success on 2nd try	Dry finger; first scan failed
4	Success on 1st try	—
5	Success on 2nd try	Oily finger
6	Success on 1st try	—
7	Success on 1st try	—
8	Success on 1st try	—
9	Success on 2nd try	Misplaced finger
10	Success on 1st try	—

Response Times

Table 3 summarises the time taken for fingerprint matching on the ESP32 and for server responses. Average fingerprint completion time was around 400 ms, while server response averaged 1.23 s. Even at the higher end, a 1.3-s delay is acceptable in an exam setting.

Table 3 Fingerprint And Server Response Times

Trial	Fingerprint time (ms)	Server time (ms)
1	291	1199
2	324	1231

3	487	1305
4	506	1178
5	412	1243
6	335	1330
7	370	1285
8	498	1209
9	406	1150
10	380	1268
Mean	**401**	**1230**

Comparison with Manual Logging

Table 4 compares total logging time for ten students using the biometric system versus handwriting. The biometric system reduced total time from 35 minutes to 12 minutes (a 66 % reduction). Each biometric transaction took roughly 8 s, while handwriting took 30–45 s.

Table 4 Total Time For Restroom Logging

Student	**Biometric time (s)**	**Handwriting time (s)**
1	9	36
2	8	32
3	7	30
4	8	35
5	6	28
6	7	29
7	8	34
8	9	39
9	10	40
10	11	45
Total	**83 s** (~1 min 23 s)	**348 s** (~5 min 48 s)

Display Behaviour

The OLED and LCD displays provided feedback to users. Table 5 summarises the messages shown in different states. The OLED displayed prompts such as “Press button to log in,” “Finger detected, converting…” or “Match not found,” while the LCD showed the user’s name and login count. When occupancy reached a limit, both displays indicated that users should wait.

Table 5 Display Messages And States

State	**OLED text**	**LCD text**
Idle	Date/time + “Press button to log in”	Blank
Button pressed	“Place your finger on the sensor...”	Blank

No finger detected	"Finger not detected. Please try again"	Blank
Finger match found	"Fingerprint detected! Converting..."	"Name: X Login: N"
Match not found	"Match not found. Try again."	"Unknown user"
Full capacity	"Restroom full. Please wait."	"Login count full."

Figure 10 Typical Oled Message During Operation.

Qualitative Feedback

Participants largely preferred the biometric system to handwriting. They perceived it as more objective and quicker, reducing the chance of favouritism or error. However, a few expressed concerns about privacy and the possibility of data misuse. They appreciated the explanation that fingerprint templates remained on the sensor and that only numerical IDs were stored in the database. Some suggested that an alternative authentication method (e.g., student ID card) would accommodate those whose fingerprints are hard to read. Others asked for audible feedback to indicate success or failure. These comments underline the importance of inclusive design and transparent communication.

DISCUSSION

Fairness and Efficiency

The biometric system improved fairness by eliminating subjective judgments about who left and when. Automatic recording reduced human error and prevented impersonation, addressing issues highlighted by Ahmed et al. [2]. Efficiency gains freed invigilators to focus on monitoring the exam rather than managing logs. However, fairness also requires that the system work reliably for all users. Individuals with worn fingerprints (manual labourers) or certain skin conditions may experience scanning errors. Multi-modal authentication—combining fingerprint with RFID or PIN—could address this limitation.

Privacy and Consent

Fingerprint templates are sensitive personal data under the GDPR and PDPA. Although the system stores templates locally, logs contain personally identifiable information (timestamp, user ID). Encryption and clear deletion policies are necessary to protect this data. Consent must be meaningful and freely given; students should understand why their data are collected and how long it will be retained. The risk of "function creep" arises if administrators use logs for purposes beyond exam integrity. Oversight by ethics committees and regular audits can mitigate this risk.

Trust and Surveillance Culture

Introducing biometric devices into exam halls could normalise surveillance. Foucault's concept of panopticism suggests that individuals internalise monitoring and discipline themselves accordingly [11]. While participants in this study largely accepted the device as fair, long-term use might foster a culture of mistrust. Transparent explanation and open dialogues can help maintain trust. Institutions should avoid extending biometric monitoring to other domains without clear justification.

Equity and Inclusivity

The low cost (~US$50) makes the system accessible to universities but may still be prohibitive for poorly funded schools. Unequal adoption could widen disparities in exam integrity. Policy interventions or subsidies might be necessary. Cultural and religious objections to fingerprint scanning require accommodations—such as same-gender invigilation or alternative methods. Accessibility features (audio prompts, multilingual displays) can make the system more inclusive.

Integration and Future Work

For the system to be effective, it must integrate seamlessly with institutional workflows. Invigilators need training to troubleshoot issues, and IT staff must maintain the server. Future improvements could include battery backup, a local Wi-Fi access point and mobile admin apps. Larger-scale studies could test the system in diverse conditions and measure long-term behavioural impacts. Multi-modal biometrics and machine-learning-based anomaly detection may enhance security. Social scientists should continue to explore how surveillance technologies reshape educational environments.

CONCLUSION

Reframing the original engineering project as a socio-technical system reveals both its benefits and challenges. The biometric toilet monitoring system improved fairness and efficiency by automating identity verification and logging. Empirical results showed high recognition accuracy and substantial time savings. However, ethical issues around privacy, consent, surveillance culture and inclusivity require careful consideration. Deploying such systems responsibly entails robust data protection, transparent policies and accommodations for diverse users. Ongoing dialogue between engineers, educators, policymakers and students is essential to ensure that technological solutions uphold educational values and respect human dignity.

ACKNOWLEDGMENT

The authors would like to dedicate our appreciation to Universiti Teknikal Malaysia Melaka for supporting this research. Our gratitude also goes to the Centre of Research and Innovation Management (CRIM) UTeM and Centre for Telecommunication Research and Innovation (CeTRI) UTeM for providing the facilities needed to conduct this study.

REFERENCES

1. A. K. Jain, A. Ross and K. Nandakumar, Introduction to Biometrics. Springer, 2011, doi:10.1007/978-0-387-77326-1.
2. S. Ahmed, N. Khan and F. Alam, “Challenges in manual access control systems,” Journal of Security Studies, vol. 12, no. 3, pp. 45–59, 2018.
3. R. Ali, P. Gupta and A. Sen, “Implementation of biometric access systems in educational institutions: A case study,” Education and Information Technologies, vol. 26, no. 4, pp. 5327–5345, 2021, doi:10.1007/s10639-021-10557-8.
4. S. Malathi and K. Umamaheswari, “Advancements in fingerprint recognition systems: A review,” International Journal of Computer Applications, vol. 182, no. 30, pp. 1–5, Oct. 2019.
5. Y. Choi, J. Lee and H. Kim, “Deep learning techniques in fingerprint recognition: An overview,” IEEE Access, vol. 11, pp. 252–265, Jan. 2023.
6. Z. Zheng and C. Valli, “Critical aspects of security and recognition accuracy in fingerprint systems,” Journal of Information Security and Applications, vol. 46, pp. 121–132, Mar. 2019, doi:10.1016/j.jisa.2019.03.016.
7. D. Lin, “Review of fingerprint sensor technologies,” Sensors, vol. 23, no. 5, p. 4679, May 2023, doi:10.3390/s23054679.
8. S. Das and S. Sengupta, “Biometric systems integration in IoT: Challenges and solutions,” IEEE Internet of Things Journal, vol. 8, no. 11, pp. 9297–9308, Nov. 2021, doi:10.1109/JIOT.2021.3064907.
9. D. Lyon, Surveillance Studies: An Overview. Cambridge: Polity Press, 2007.
10. E. A. Whitley and I. N. Kroener, “Privacy practices and personal data: A critical review,” Information Systems Journal, vol. 27, no. 1, pp. 1–27, 2017.
11. M. Foucault, Discipline and Punish: The Birth of the Prison. New York: Vintage Books, 1977.
12. J. Wajcman, TechnoFeminism. Cambridge: Polity, 2004.