

Robot-Mediated Attendance Verification in Higher Education: A Socio-Technical Evaluation

Fuad Budagov*, Tarmo Robal, Mohammad Tariq Meeran,
and Ali Atakan Basaran

School of Information Technologies, Tallinn University of Technology,
Ehitajate Street 5, Tallinn, 19086, Estonia

fuad.budagov@taltech.ee, tarmo.robal@taltech.ee, mohammad.meeran@taltech.ee,
albasa@taltech.ee

Abstract. Attendance tracking remains an essential administrative task in higher education, particularly in large classes and examination settings where accurate identity verification and time efficiency are critical. Traditional manual methods are time-consuming, prone to error, and difficult to manage in high-volume scenarios, motivating the need for automated and reliable solutions. This study evaluates a robot-mediated multi-factor attendance verification system through a socio-technical perspective, considering the interaction of its technical components, users, and institutional workflows. The proposed system was tested in a real classroom environment and compared with traditional manual attendance methods to evaluate time efficiency, accuracy, usability, and user acceptance. The results indicate a lower estimated average attendance-processing time when using robot-assisted verification compared with manual attendance under experimental conditions, while also demonstrating reliable identity verification for supported ID cards. Student and lecturer feedback highlighted the system's efficiency and ease of use, with lecturers reporting perceived reductions in administrative workload. The multi-factor verification approach supports stronger identity assurance and attendance-record integrity.

Keywords: Socio-Technical Evaluation, Attendance Check, Face Recognition, ID Verification, Robot Assistant, Higher Education.

1 Introduction

Efficient and accurate attendance tracking remains a challenge in higher education (HE), particularly in large classes with more than 100 students [1]–[3]. Lecturers face an administrative burden associated with repetitive academic management tasks [4]. Manual attendance tracking is one such task, often described as exhausting and time-consuming, which detracts from valuable

* Corresponding author

© 2026 Fuad Budagov, Tarmo Robal, Mohammad Tariq Meeran, and Ali Atakan Basaran. This is an open-access article licensed under the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>).

Reference: F. Budagov, T. Robal, M. T. Meeran, and A. A. Basaran, "Robot-Mediated Attendance Verification in Higher Education: A Socio-Technical Evaluation," *Complex Systems Informatics and Modeling Quarterly*, CSIMQ, no. 48, pp. 1–32, 2026. Available: <https://doi.org/10.7250/csimq.2026-48.01>

Additional information. Author ORCID iD: F. Budagov – <https://orcid.org/0000-0003-1762-2263>, T. Robal – <https://orcid.org/0000-0002-7396-8843>, M. T. Meeran – <https://orcid.org/0000-0002-8567-7285>, and A. A. Basaran – <https://orcid.org/0009-0007-8471-5044>. PII S225599222600267X. Received: 18 June 2026. Accepted: 28 October 2026. Available online: 31 October 2026.

teaching time [1], [5], [6]. While traditional attendance methods, such as paper sign-ins and manual digital entry, are commonly used, they are often slow [1], unautomated, and error-prone [7]. Although simple digital alternatives such as Moodle-based attendance with button clicks, passwords, or QR codes [4], [7] exist, these methods still require active student participation and are susceptible to misuse or falsification (e.g., proxy attendance, signing in for absent peers) [4], [5], [8]. Additionally, paper-based attendance tracking is not environmentally sustainable, contributing to unnecessary paper waste and inefficiencies in record-keeping [8]–[10].

The socio-technical perspective views system outcomes as arising from interactions between technical and social-organizational components and emphasizes their joint consideration rather than treating technology as the sole determinant of work practices [11]–[13]. A socio-technical system can be defined as a work system composed of interrelated technical and social subsystems whose joint interaction produces system outcomes [14]. The attendance verification system discussed in this article is a socio-technical system as it brings together a semi-autonomous robot platform, national identity cards, multi-factor identity verification, facial recognition, biometric models, and institutional workflows in a complete system that students and lecturers can interact with.

In this article, we propose and evaluate a robot-mediated multi-factor attendance verification system within this socio-technical framing. As the robotic platform, we use the Temi version 3 semi-autonomous service robot, a mobile assistant equipped with navigation, touchscreen interaction, and camera-based recognition capabilities suitable for classroom environments. We compare the proposed robot-assisted method with traditional manual attendance procedures in terms of processing time and operational performance, while separately evaluating robot-assisted identity-verification performance and user acceptance. In addition, we assess the usability and acceptance of robot-assisted attendance checking among both students and lecturers using targeted surveys and the System Usability Scale (SUS) [15], [16] to determine the practicality of our approach in academic settings. This research is guided by the following three research questions:

RQ1: *To what extent does an automated robot-assisted attendance check system reduce the administrative workload for lecturers while ensuring accurate and reliable attendance tracking of students compared to manual attendance tracking?* To answer RQ1, we compare robot-assisted attendance against the baseline manual process across multiple class sessions. We assess performance using the genuine verification success rate and false-rejection rate, alongside attendance processing time and perceived workload ratings. We then compare the procedural efficiency of both methods and report the observed verification outcomes.

RQ2: *How do students perceive the usability, efficiency, and privacy implications of an automated robot-assisted attendance check system based on a national identity document and facial recognition in a higher education setting?* To answer RQ2, we conducted in-class attendance-check sessions where students used the robot-assisted attendance check (ID document and face verification) under realistic teaching conditions. Immediately after participation, students completed a structured questionnaire measuring usability, perceived efficiency, and privacy perceptions. We performed a quantitative analysis of the survey items using descriptive statistics.

RQ3: *How do lecturers perceive the usability, efficiency, and privacy implications of an automated robot-assisted attendance check system based on a national identity document and facial recognition in a higher education setting?* To answer RQ3, lecturers observed and operated the robot-assisted attendance process during their teaching sessions and evaluated it afterward. We collected lecturer feedback via a targeted survey and semi-structured interviews focusing on perceived usability, time efficiency, privacy implications, and adoption barriers. We performed a quantitative analysis of survey items and a thematic analysis of qualitative feedback to identify recurring concerns and improvement requirements. Altogether, RQ1 examines the technical and operational dimensions, while RQ2 and RQ3 examine the human and organizational dimensions of the socio-technical evaluation.

This study contributes to existing research by introducing a robot-mediated multi-factor identity verification approach that combines national ID-card authentication with facial recognition on a

mobile semi-autonomous robot platform in HE. We also envision using the system beyond classroom settings, for instance, accepting participants to events (e.g., conferences, workshops). While prior studies typically explore robotic systems and ID-card-based authentication methods such as RFID, QR or barcode verification separately, this research uniquely integrates both methods into a unified automated solution. By embedding facial recognition functionality into a mobile robot assistant that reads national ID cards, the system enables secure, minimal-contact, and efficient attendance verification. This hybrid system addresses key limitations of manual and single-technology systems, offering a practical and scalable framework for automating attendance checks while improving accuracy, reducing administrative burden, and enhancing attendance management. The results of our study show that the proposed robot-assisted approach improves time efficiency and provides reliable identity verification compared to traditional manual attendance methods. Furthermore, both students and lecturers reported positive usability and acceptance, indicating the practicality of the system for real classroom environments.

The remainder of this article is organized as follows. Section 2 presents related work on attendance tracking technologies, including robot-assisted and ID card-based systems in educational contexts. Section 3 introduces the robot-assisted system for attendance check. Section 4 describes the experimental setup. Section 5 presents the results of both manual and robot-assisted attendance experiments, along with survey and interview findings. Section 6 discusses the key outcomes, implications, and broader relevance of the findings. Finally, Section 7 concludes the article by outlining limitations and proposing directions for future research.

2 Related Work

Socio-technical research treats information systems as work systems in which technical artifacts, users, work practices, and organizational conditions are interdependent [11]–[13]. Mumford [11] argues that technical and human factors should receive comparable attention, and that socio-technical design seeks the joint optimization of the social and technical subsystems. Baxter and Sommerville [12] extend this perspective to systems engineering by emphasizing that technical development, stakeholder needs, and organizational change should be considered together. Clegg [13] similarly presents socio-technical principles for designing systems that incorporate information technology and changing work practices. Following this perspective, robot-mediated attendance verification should be evaluated not only through processing time and biometric reliability but also through usability, privacy perceptions, lecturer workload, workflow compatibility, and institutional readiness.

Attendance tracking in HE has attracted growing research interest as institutions seek to replace manual methods with more secure, efficient, and scalable alternatives [17]. Two primary technological approaches have emerged in recent studies: the use of robot-assisted systems [1] and ID card-based solutions [18]. While robotic platforms increasingly incorporate biometric technologies such as facial recognition to automate attendance [19], ID-based systems often combine RFID or QR codes [18], [20] with backend databases for verification and reporting. We continue by first discussing the existing works using robot-assisted attendance check systems in HE, followed by the application of ID cards to this problem.

The use of robot-assisted attendance checks is not novel to HE. Alali et al. [1] developed a multipurpose robotic assistant called Cognito to support academic workflows in HE through a range of smart features. One of its functions is automated attendance tracking using facial recognition and fingerprint verification. This was enabled through Python-compatible biometric sensors and machine learning models such as Histogram of Oriented Gradients (HOG) and Support Vector Machines (SVM). The system allows students to check in to classes via touchscreen, reducing time spent on manual procedures. While not focused solely on attendance, Cognito demonstrates the value of robotic assistants for classroom automation by additionally integrating lecture transcription, automated multiple-choice question (MCQ) exam correction, emotion detection with motivational feedback, and fingerprint-based biometric verification, thereby

positioning the robot as a multipurpose academic support system rather than a single-function attendance tool.

In a separate initiative, Mohyiddeen et al. [21] developed SARA, a college virtual receptionist system that uses facial recognition to automate staff attendance recording. The assistant combines voice recognition, intent classification, and a K-Nearest Neighbors (KNN)-based facial recognition module to identify employees and log their attendance. While its primary function is to answer queries and guide visitors through speech interaction, the integrated attendance module marks daily sign-in and sign-out times and generates reports for administrative use. Although focused on staff attendance rather than student tracking, SARA demonstrates how AI-driven virtual receptionist systems can integrate biometric verification into institutional workflows through the combination of facial recognition, intent classification, and database-backed attendance logging. This reinforces the feasibility of embedding automated biometric attendance functions within service-oriented systems in educational environments.

In contrast to mobile robotic platforms, several recent attendance systems adopt fixed architectures, where identity verification is performed through stationary camera infrastructures rather than mobile or interactive platforms. Darshan et al. [6] developed a Raspberry Pi-based facial recognition attendance system that uses a fixed camera and embedded device setup to capture facial images in real time and match them against a pre-registered attendance dataset for automated logging. Similarly, the IoT-based system developed by Nguyen et al. [22] and the Attendify platform presented by Srivastava et al. [23] use closed-circuit television (CCTV) or Raspberry Pi-connected cameras installed in institutional environments to continuously capture student images for real-time processing and attendance logging. Mardiana et al. [24] similarly integrated a YOLOv5-based facial recognition module with an existing library automation system through an API, face-recognition, and visitor-identification subsystems. In these implementations, the hardware remains static within the physical environment, and students or users passively appear within the camera's field of view. While such systems show scalability and ease of infrastructure integration, they rely solely on single-biometric facial authentication and do not incorporate mobile interaction, official identity document verification, or multi-factor identity assurance mechanisms.

Beyond classroom attendance, recent studies have begun to explore biometric technologies specifically for examination attendance scenarios. Olojido and Oladimeji [25] propose a system that employs a fixed camera and computer setup to perform Convolutional Neural Network (CNN)-based facial recognition, matching students' faces against a pre-registered database prior to entry into the examination hall. The system operates in real time and aims to automate identity verification to reduce impersonation and administrative workload. It compares unimodal and enhanced camera configurations within a controlled examination environment but relies entirely on single-factor facial authentication, without incorporating official identity documents or additional verification layers. Similarly, Rukhiran et al. [26] present an IoT-based facial recognition solution deployed on a Raspberry Pi platform and evaluate unimodal (single-camera) and multimodal (dual-camera) configurations. Its primary contribution lies in assessing student acceptance through an extended Technology Acceptance Model (TAM) framework, emphasizing perceived usefulness, ease of use, and trust. While the findings indicate positive user perceptions and highlight the importance of trust and security factors, the system remains limited to single-biometric authentication and does not address multi-factor identity assurance, national ID integration, or operational benchmarking.

Several other approaches have been explored for attendance checking, either alone or in combination with ID cards. Nagendra et al. [27] developed a biometric and RFID-based student attendance system that combines fingerprint authentication with RFID tag scanning for secure verification. Students are first required to scan their fingerprint, and upon successful match, must then authenticate with their RFID-embedded ID card. Tested in real-world classroom scenarios, the implementation demonstrated improved security, accuracy, and efficiency over manual methods, while preventing proxy attendance through dual-layer authentication. Similarly, Üçgün

et al. [28] introduced a two-stage student attendance system for HE that combines RFID card scanning with fingerprint verification. The system first checks student identity via an RFID-embedded ID card and then activates fingerprint authentication to complete the attendance process. This dual-verification design enhances security and minimizes proxy attendance, offering a practical and cost-effective model for biometric-based classroom management.

An alternative low-cost method was developed by Mustafa and Jawad [29] who developed an electronic student attendance management system using QR codes embedded on ID cards, scanned via a standard webcam. Designed for HE, the system logs attendance in real time and allows lecturers and administrators to view, edit, and generate attendance reports. Despite the lack of biometric or robotic components, the solution illustrates how low-cost ID card technology can modernize attendance tracking.

Hakim et al. [30] proposed an IoT-based attendance tracking system specifically designed for college library environments. By integrating barcode scanners with Raspberry Pi devices and linking student ID cards to a centralized web-based platform, the system enables students to check in at the library via barcode scans of their ID cards and record the purpose of their visit. Although focused on library visits rather than classroom attendance, the system demonstrates how ID card-based automation can enhance institutional efficiency and user experience (UX) in HE contexts.

Sathishkumar et al. [31] developed a real-time classroom attendance system in which students scan RFID-enabled cards using a fixed reader installed at the classroom entrance. The system validates card identifiers, prevents duplicate entries, stores attendance records in a centralized database, and provides real-time feedback and attendance reports. Although the system lacks biometric verification, it demonstrates how a stationary RFID-based architecture can automate attendance recording and administrative reporting.

Near Field Communication (NFC) has also been investigated as an alternative approach for attendance management in HE. Benyo et al. [32] explored NFC-based student attendance monitoring in university environments, while Chiang et al. [33] developed a smartphone-based attendance system combining NFC with GPS-based location verification. In such implementations, students can register attendance using an application installed on their NFC-enabled mobile devices by interacting with a nearby NFC tag or compatible reader. Compared with conventional QR-code or password-based methods, NFC-based approaches can reduce opportunities for proxy attendance by requiring short-range interaction and access to a student's personal device, which is generally less likely to be shared. Nevertheless, NFC-based registration does not independently establish the user's identity, as a lost, stolen, or borrowed mobile device could potentially be used for proxy attendance if additional authentication mechanisms are absent. Therefore, identity assurance depends on the authentication mechanisms implemented alongside NFC. In contrast, the proposed robot-assisted system combines national ID-card validation with live facial verification to authenticate the student's identity.

The reviewed literature reveals two broad directions in automating attendance checks in HE: robot-assisted systems incorporating biometric recognition and non-robot attendance solutions employing RFID, QR codes, barcodes, or NFC-enabled mobile devices. Robot-assisted systems provide mobility and interactive interfaces but often require more advanced infrastructure and technical integration. By comparison, card-based and mobile-device-based solutions can offer simpler and potentially more cost-effective attendance registration, although their ability to prevent proxy attendance depends on the authentication and identity verification mechanisms implemented. In our previous pilot study [34], conducted over one week in May 2024 with 67 students, we implemented a Temi-based attendance system that used facial recognition as the sole verification method and stored encoded facial-feature representations locally on the robot after deleting the captured photographs. Although the pilot study reported positive student usability and acceptance, participants also raised privacy concerns. The pilot did not systematically compare manual and robot-assisted attendance methods or investigate lecturers' perspectives. Moreover, existing systems typically rely on a single authentication method and rarely combine robotic mobility with multi-factor identity verification. Building on our previous work and addressing this

gap, the present study integrates national ID card authentication and live facial recognition with liveness detection within a multi-factor identity verification approach, without requiring persistent biometric enrollment profiles. The current study also extends the experimental evaluation to 32 classroom sessions (11 manual and 21 robot-assisted), incorporating student and lecturer surveys and semi-structured lecturer interviews. The socio-technical evaluation considers multi-factor identity assurance alongside time efficiency, verification reliability, usability, privacy perceptions, lecturer workload, and institutional integration.

3 Robot-Mediated Attendance Check System

This section provides a detailed technical overview of the robot-mediated multi-factor identity verification system for attendance, including how the system interacts with ID cards, processes biometric verification, and communicates with the backend Attendance Check Database (ACD). These components form the technical subsystem, while the broader socio-technical system also includes students, lecturers, consent and manual fallback procedures, privacy requirements, and institutional attendance workflows.

3.1 Temi Robot Platform

In this study, we use the Temi v3 robot as the robot assistant to perform the automated attendance verification process. The robot platform serves as the physical interface between students and the attendance verification system. Temi is an advanced, AI-powered mobile robot equipped with a touchscreen, camera, microphone, speaker, and autonomous navigation capabilities, designed for interactive assistance in various industries, including healthcare, retail, and education. In this study, Temi was utilized to assist students and lecturers in HE by automating the attendance check process through ID card authentication and facial verification. Figure 1 illustrates a student using the attendance check application (ACA) on the Temi v3 robot to verify attendance by inserting a national ID card and undergoing facial verification through the robot's camera.

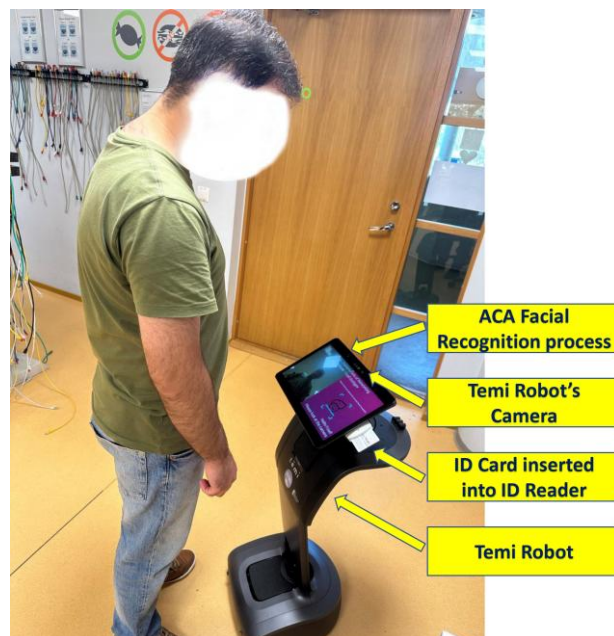


Figure 1. Student verifying attendance through national ID card authentication and facial verification using the ACA on the Temi v3 robot

3.2 ID Card Data

Identity verification in the proposed system relies on reading personal data stored on the electronic chip of national ID cards rather than maintaining a separate database of user information. This approach allows the system to access trusted identity data directly from the official document when needed. In order to verify the user's identity without permanently storing their data on the robot or an external database, the image from their ID card is used, as it is a trusted and reliable source. The image is accessible from the ID cards that support the International Civil Aviation Organization (ICAO) Doc 9303 [35] standard. As of August 2021, ID cards issued in Estonia support this standard under Regulation (EU) 2019/1157 [36].

Interfacing with the ICAO document in the ID card allows us to fetch the document number, expiration date, and date of birth of the cardholder [37]. This data is stored on the card and must be manually entered or scanned with optical scanner solutions if the process is not automated.

However, Estonian ID cards also support the EstID standard [38]. The EstID standard has the document number, expiration date, and birth date of the document holder as well as their name and their public key, which can be used for further verification of the ID card's validity. It is possible to use the data returned from the EstID component of the card to obtain the information required to interface with the ICAO component and retrieve the user's biometric image for verification. For our robot-assisted system, we take advantage of both the ICAO Doc standard and the EstID standard and combine them for a streamlined automated attendance check process.

3.3 Attendance Check Application

Building upon the ID card standards described, the application layer retrieves identity data, performs biometric verification, and coordinates communication with the backend system. The application runs locally on the Android-based Temi v3 robot and uses the robot's touchscreen, camera, processor, memory, and connected ID card reader. Figure 2 presents the main user interface displayed on the robot's screen, including the consent statement and ID card insertion prompt.

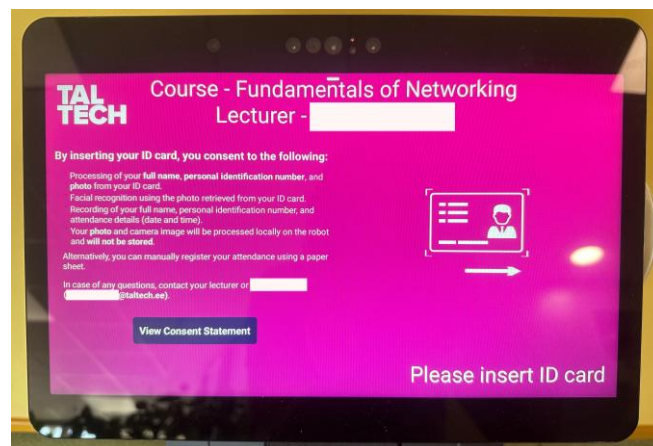


Figure 2. The main page of the ID ACA interface displayed on the Temi robot screen

After receiving data from the ID card reader, the application searches for the EstID document on the card. If the document is not found, the card is rejected as a non-Estonian ID card, and the user is notified. Otherwise, the application retrieves the cardholder's first name, last name, ID code (national identifier), date of birth, expiration date, document number, and authentication certificate details. The expiration date and public authentication certificate are checked for validity before proceeding. The system applies two-factor identity verification through (1) possession of a validated national ID card and (2) biometric verification by comparing the cardholder's live facial image with the photograph stored on the ID card.

To access the ICAO document, the application resets the ID card connection and mounts the ICAO interface using the retrieved EstID data. If the ICAO document cannot be accessed, the card is rejected as unsupported, including old-generation Estonian ID cards. Otherwise, a biometric photograph is retrieved from the card, and the user is instructed to look into the robot's camera for facial verification.

Face detection is performed using the Multi-task Cascaded Convolutional Neural Network (MTCNN) model [39] that incorporates three stages: P-Net, R-Net, and O-Net. P-Net identifies potential face regions, R-Net refines the detections and removes unsuitable candidates, and O-Net produces the final detections and estimates five facial landmarks. The detection thresholds were set to 0.60, 0.70, and 0.70, respectively. Non-maximum suppression removes overlapping detections, and if multiple faces are detected, the largest face is selected and prepared as a square crop for recognition. The biometric models are executed locally using TensorFlow Lite and multithreaded processing. Smaller model configurations and limited image dimensions are used to accommodate the computational and memory constraints of the Temi robot.

Following face detection, the ID card photograph and live camera image are resized and normalized for processing by the FaceNet model [40]. FaceNet converts both images into numerical facial representations, known as embeddings, which are compared using a distance-based similarity calculation. The resulting application-level similarity score is evaluated against a threshold of 80%. Scores equal to or greater than 80% are accepted as facial matches, while lower scores result in identity mismatches. This threshold is an application-specific decision criterion and does not represent an 80% statistical probability that the images belong to the same person.

After successful facial recognition, the live camera image undergoes liveness verification using the FasNet model [41]. A compact model is used to accommodate the robot's computational limitations, with a 50% confidence threshold applied as the experimental decision criterion. Scores below this threshold are classified as possible spoofing attempts, while scores equal to or above the threshold satisfy the liveness requirement. The mechanism is intended to detect basic presentation attacks involving printed photographs or facial images displayed on another device. However, its effectiveness against advanced attacks, such as three-dimensional masks, manipulated videos, injected camera streams, and synthetic facial images, has not been established by the reported evaluation. A failed liveness check indicates unsuccessful verification but does not establish intentional impersonation.

The application handles unsuccessful verification attempts without creating a successful attendance record. Failure conditions include expired or unsupported ID cards, invalid authentication certificates, inaccessible ICAO documents, unreadable biometric images, unsuccessful face detection, camera or model processing errors, facial recognition scores below 80%, and liveness scores below 50%. Students are notified of unsuccessful verification and may repeat the procedure. If verification remains unsuccessful, the lecturer's manual attendance procedure is available.

The application also manages structured event logging through the Attendance Check Database (ACD). Unsuccessful attempts are recorded with corresponding status labels, including "Non-Estonian ID card," "Old-generation ID card," "Expired document," "Invalid certificate," "Face not detected," "Identity mismatch," "Liveness check failed," and "Technical processing error." Successful attempts are recorded as verified attendance. The application transmits the verification outcome, failure category where applicable, interaction timestamps, performance measurements, robot identifier, and required attendance information to the ACD.

To minimize biometric data exposure, the ID card photograph, live camera image, facial embeddings, and liveness input are processed temporarily in the robot's memory and discarded after each verification attempt, regardless of its outcome. Raw biometric images and facial embeddings are not transmitted to the ACD or permanently stored. Figure 3 illustrates the complete ACA workflow, including ID card validation, biometric verification, failure handling, and backend event logging.

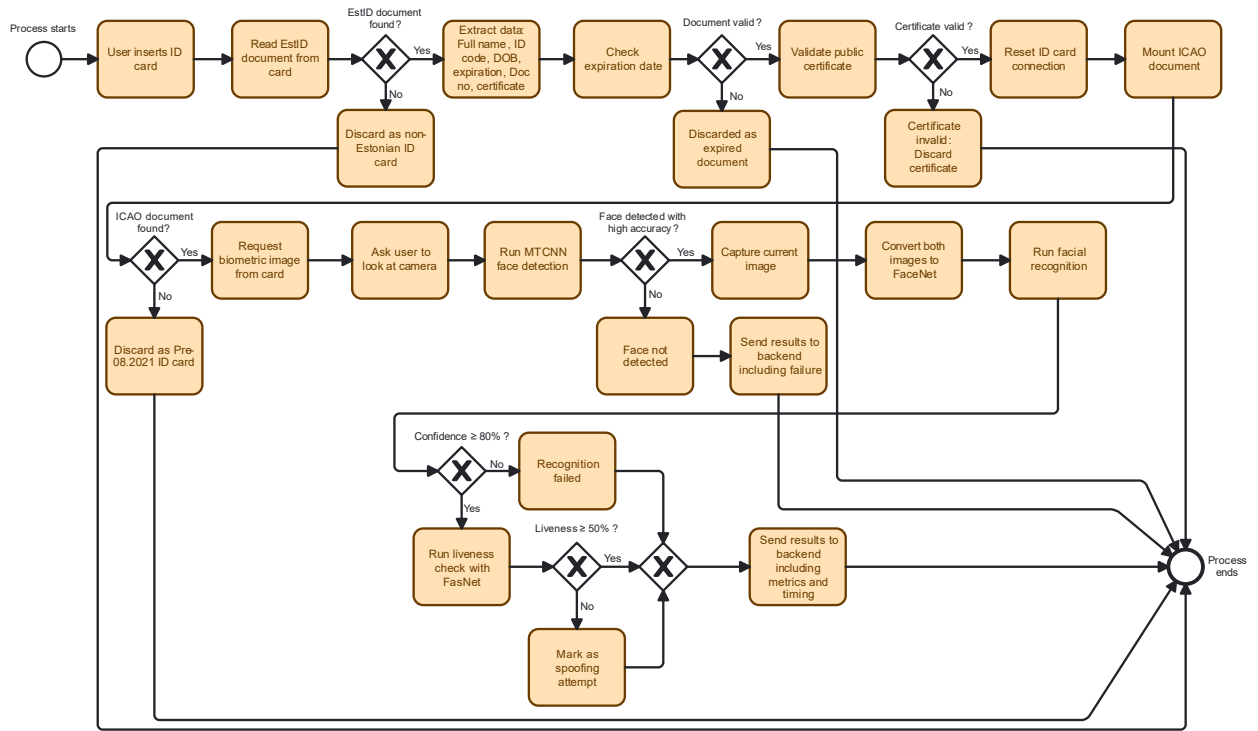
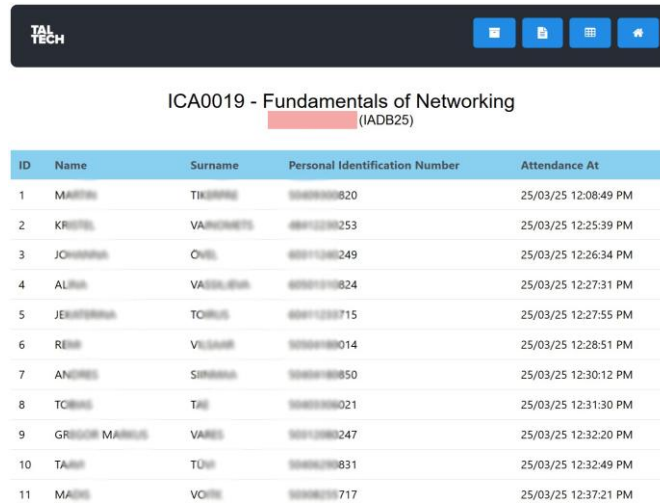


Figure 3. Workflow of the ACA using an Estonian ID card and facial recognition for attendance checking

3.4 Attendance Check Backend and Database

The Attendance Check Backend and Database (ACD) is a centralized digital system used to securely manage and store student attendance records, ensuring accurate tracking while maintaining compliance with the General Data Protection Regulation (GDPR) [42]. The ACD functions as the primary data repository, receiving verification results from the robot application and making them accessible to lecturers through a web-based interface. The system features secure storage of attendance details such as full name, personal identification number, date, and time of attendance for each student. It also maintains records of student consent agreements, ensuring adherence to ethical research guidelines. All data, except biometric images, is securely stored on university servers, with access limited to research personnel, participating lecturers, and the authors, and is set to be retained for up to three years before permanent deletion. The three-year data retention period was selected to align with the planned duration of the PhD research project entitled “Applicability of Robot Assistants in Higher Education,” of which this experiment forms a part. Attendance and consent records will be retained to support the doctoral research and will be deleted after the required analysis, no later than three years after the experiment. This retention period does not apply to biometric images, which are processed temporarily in the robot’s memory and deleted immediately after verification. The ACD also supports student data deletion requests; if a lecturer removes a student’s consent agreement, all related attendance records are automatically erased from the system. During the experiment, the ACD supported attendance registration as part of the research evaluation, with identifiable records collected for the specified research purposes. These purposes require consideration of data-controller responsibilities, access authorization, and restrictions on subsequent use of personal information. In particular, institutional governance must address who authorizes access to attendance records, handles data-subject requests, and ensures that exported attendance reports remain subject to appropriate data protection requirements. Wider deployment of biometric attendance verification also requires an assessment of privacy risks, including whether a Data Protection Impact Assessment (DPIA) is necessary under GDPR Article 35 [42]. Additionally, lecturers have administrative functions such as creating and editing courses, updating course information, viewing archived records, and

downloading attendance and consent lists in PDF or Excel formats for reference. Figure 4 shows an archived course view presented to the teacher in the ACD interface, with student and course information blurred for privacy.



ID	Name	Surname	Personal Identification Number	Attendance At
1	MAIRIA	TRINIDAD	XXXXXXXXXX820	25/03/25 12:08:49 PM
2	KRISTIN	VAN DER MEETS	XXXXXXXXXX253	25/03/25 12:25:39 PM
3	JENNIFER	OWEN	XXXXXXXXXX249	25/03/25 12:26:34 PM
4	ALBA	VAN DER MEETS	XXXXXXXXXX824	25/03/25 12:27:31 PM
5	JENNIFER	OWEN	XXXXXXXXXX715	25/03/25 12:27:55 PM
6	RILEY	VAN DER MEETS	XXXXXXXXXX014	25/03/25 12:28:51 PM
7	ANDREW	SIMPSON	XXXXXXXXXX850	25/03/25 12:30:12 PM
8	TONY	TAYLOR	XXXXXXXXXX021	25/03/25 12:31:30 PM
9	GRACE MARCUS	VALENTI	XXXXXXXXXX247	25/03/25 12:32:20 PM
10	TAHAR	TUNALI	XXXXXXXXXX831	25/03/25 12:32:49 PM
11	MARIA	VAN DER MEETS	XXXXXXXXXX717	25/03/25 12:37:21 PM

Figure 4. An archived course view of the ACD

The backend infrastructure supports both the ACD web interface and the robot-based attendance application. The backend service is developed using Node.js, while MongoDB is used for data storage. The backend exposes two sets of APIs: one for teachers and another for robot devices. The application layer runs completely on the robot platform to ensure privacy, and none of the personal biometric data (images) is shared with systems external to the robot assistant (Figure 5). Each robot has a unique ID assigned for tracking and assignment to interface with the IoT APIs where it can retrieve the current course they are assigned to and report the attendance check results it obtained. The teacher APIs provide the ability to view the results of both successful and unsuccessful attendance attempts, including the reason for any failures. The teacher can also modify the current course information with the robots assigned to them. This data is displayed to the teacher on a web interface in real time.

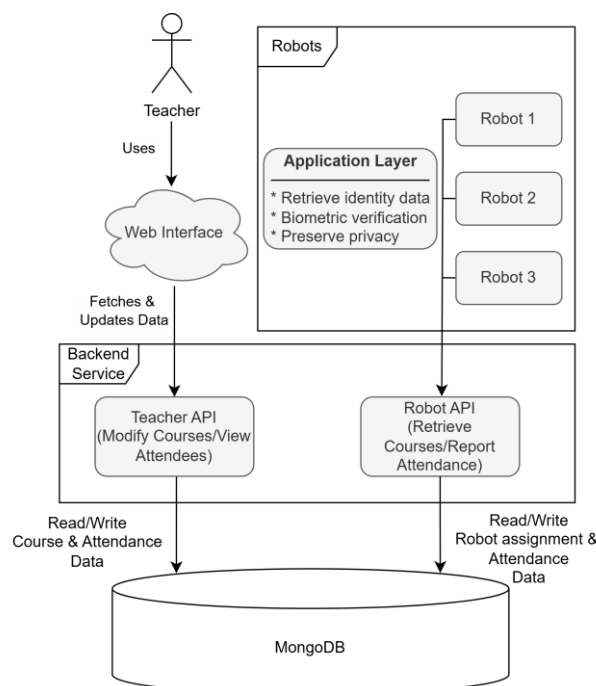


Figure 5. Overview of the ACD backend architecture

4 Experimental Setup

This section presents the experimental setup designed to evaluate the proposed robot-assisted ID card-based attendance system in real classroom environments. The section first describes the research methodology and data collection approach, followed by the design of the attendance check experiment and the procedures used to measure efficiency, accuracy, usability, and user experience in comparison with the traditional manual attendance method.

4.1 Methodology of the Study

To conduct the socio-technical evaluation of the robot-mediated attendance system, a mixed-methods approach [43] was employed to combine technical measures with human and organizational evidence. The technical dimension included processing time, verification reliability, and document compatibility. The human dimension included usability, acceptance, and privacy perceptions, and the organizational dimension included lecturer workload, workflow compatibility, reporting functions, and institutional readiness. Attendance-processing duration was measured through observer timing and system logs, whereas lecturer workload was assessed through survey responses and interviews. Lecturers' active time spent on attendance-related tasks was not directly measured. The research design combined quantitative measures, including time efficiency, accuracy metrics, Likert-scale survey responses, and the SUS, with qualitative data derived from open-ended survey responses and semi-structured interviews. The interpretation examined relationships between technical performance and participant experiences, including differences between measured processing efficiency and perceived workload benefits, as well as the influence of ID card compatibility and existing institutional workflows on system adoption. In order to address RQ1 (administrative workload and accuracy comparison), classroom sessions using both manual and robot-assisted attendance methods were observed by a designated observer during each session, who monitored the attendance process and recorded timing and performance data for comparison in terms of procedural efficiency and operational performance. Furthermore, to address RQ2 (student perceptions), a Likert-scale questionnaire including a free-form comment section was administered to students after they had experienced both attendance methods. The questionnaire captured perceptions of usability, efficiency, reliability, and privacy implications. Similarly, to address RQ3 (lecturer perceptions), a questionnaire was distributed to participating lecturers, followed by semi-structured interviews to obtain deeper insights into perceived workload impact, integration challenges, and classroom applicability. In addition, to assess overall system usability, the standardized 10-item SUS [15], [16] was administered to both students and lecturers using the same anonymous questionnaire. The combined SUS results are presented in Section 5.4. Questionnaires were distributed to participants immediately after exposure to both attendance methods using the Microsoft Forms platform, where QR codes linking to the survey were displayed on the classroom screen for students to access using their personal devices. Participation was voluntary, and responses were collected anonymously.

4.2 Attendance Check Experiment

The attendance check experiment was designed as a controlled classroom comparison between manual attendance procedures and the robot-assisted ID-card-based system (Section 3) in real teaching environments. Specifically, the experimental setup enabled the assessment of attendance-processing duration (RQ1), student perceptions of the robot-assisted attendance system (RQ2), and lecturer perceptions of workload, usability, and integration (RQ1 and RQ3) through exposure to both attendance methods. The experiment was integrated into five different courses. During the first session, the manual attendance method was applied, where students wrote their full names and signed a printed paper form. This was followed by two sessions in which the same group experienced the robot-assisted attendance check. During the robot-assisted sessions, the Temi

robot was positioned at the classroom entrance, while an alternative manual attendance procedure remained available in parallel. As the robot-assisted method was newly introduced, the experimental procedure considered the initial technology adoption process. Students could approach the robot voluntarily at any point during the 90-minute class session to become familiar with its operation, ID card requirements, and identity verification procedure. Since students experienced the robot-assisted method during only two sessions, a mandatory queue at the beginning of the class was not imposed. The experimental design enabled a comparison of attendance-processing efficiency between both methods, alongside an evaluation of robot-assisted identity-verification performance and participant UX.

4.3 Manual Attendance Check

The manual attendance check was conducted during the first session using a pre-printed attendance sheet containing a structured table with the following columns: student full name and signature. The procedure began with the lecturer circulating the attendance sheet to students in the classroom. Each student was instructed to write their full name and signature, after which the sheet was passed along to the next student and eventually returned to the lecturer upon completion.

To measure time efficiency, the duration of the manual attendance process was recorded using a digital stopwatch operated by an independent observer. The timer was started when the first student received the attendance sheet and stopped when the completed sheet was returned to the lecturer. No individual student times were recorded; only the total duration per session was measured. The number of participating students was determined by the lecturer and recorded on the attendance sheet, and the total count was verified based on the number of student signatures collected during the session. Students who arrived late were excluded from the time measurement. The average time per student was calculated by dividing the total recorded duration by the number of participating students for that session.

4.4 Robot-Assisted Attendance Check

The robot-assisted attendance check was conducted during the second and third sessions with the same student groups that participated in the manual attendance sessions. Participation in the robot-assisted method was voluntary. Students who did not wish to use the robot or had missing or incompatible ID cards could register their attendance manually without attempting robot-assisted verification. Students whose identity verification was unsuccessful could also complete their registration manually. Both attendance methods operated in parallel, and alternative manual registrations were excluded from the robot-assisted processing-time analysis. The Temi robot was placed at the classroom entrance. Initially, the Temi robot displayed a GDPR consent statement (Figure 2). Students were required to read the statement and choose whether to participate. If a student disagreed, they were redirected to the lecturer for manual registration. If the student accepted, they proceeded with the ID card-based attendance procedure.

The student inserted their Estonian national ID card into the reader and followed the on-screen instructions. In cases where consent had not been recorded, consent acceptance was stored in the ACD before proceeding. If the identity verification was successful, the robot displayed a confirmation message including the student's name and informed them that attendance had been recorded. If an identity mismatch occurred, the student was prompted to reinsert the ID card. Persistent mismatches resulted in redirection to manual attendance registration. The interaction sequence of the ID card-based attendance process during classroom execution is shown in Figure 6.

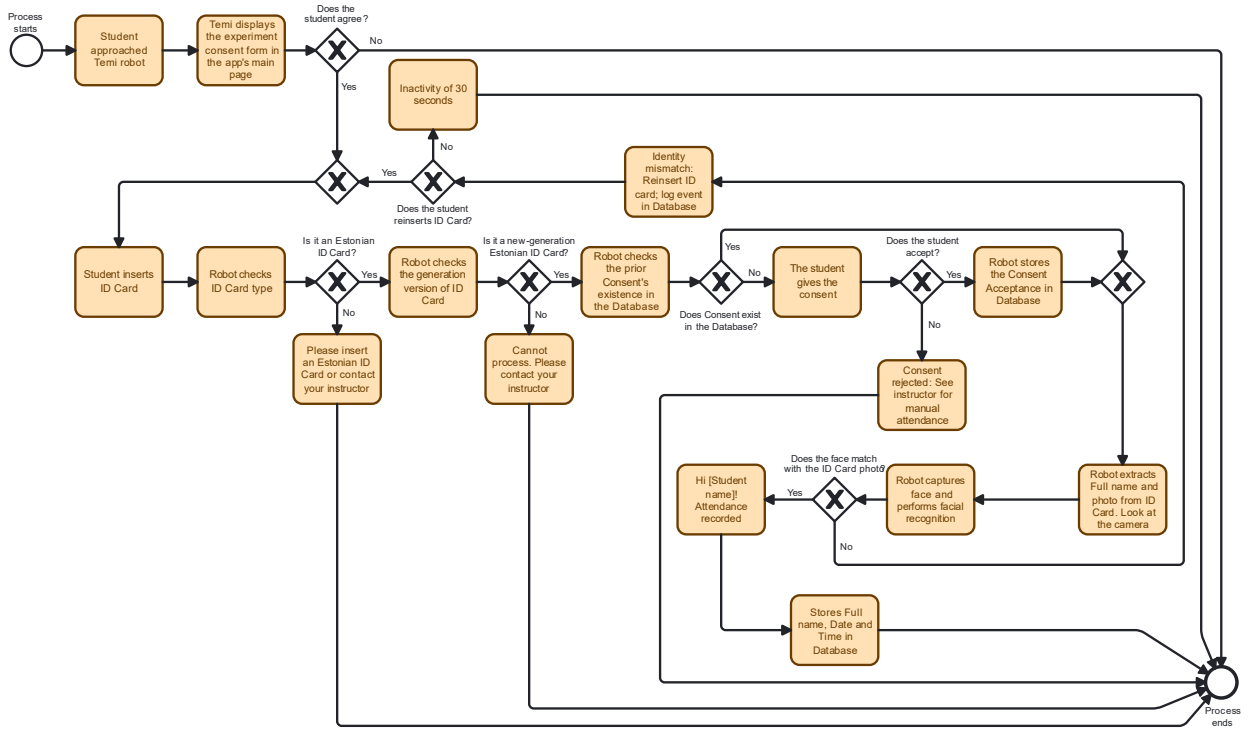


Figure 6. ID card-based ACA workflow

For the time-efficiency analysis, the system automatically recorded the internal processing duration of 162 robot-assisted verification attempts, including two unsuccessful identity matches. Processing time was measured from ID card detection until the verification outcome was recorded in the backend database. Attempts involving incompatible ID cards (non-Estonian and old-generation Estonian ID cards) that could not proceed through verification were excluded from the processing-time analysis. The estimated interaction duration was calculated by adding the maximum observed approach and start-use time of 7 seconds to the average system-recorded processing time. Individual waiting times were not measured separately.

In addition to survey and interview data, quantitative system logs and attendance records were stored to enable analysis of operational performance and system reliability. Attendance records, including student names, ID codes, timestamps, and session details, were securely stored on a GDPR-compliant server hosted at the university.

The experiment received ethical approval from the Ethics Committee of the Tallinn University of Technology (TalTech) for the project titled “Attendance Check of Students in Higher Education” (decision reference: Committee minutes 25.03.2025 nr 1-16/3; approval number: 1-33/23). The research ethics application identified participant consent for specified research purposes as the lawful basis for processing identifiable attendance data, corresponding to GDPR Article 6(1)(a) [42]. All participants were informed about the purpose and procedures of the study and provided their informed consent digitally before participation by confirming acceptance within the ACA. Participation in the study was entirely voluntary, and participants had the right to withdraw from the experiment at any time without penalty. Students were assured that their data would be handled in accordance with GDPR guidelines and stored securely on university servers. No biometric images were stored during the attendance check process, and all responses and attendance records were anonymized for analysis.

5 Results

In this section, the results are presented in alignment with the research questions guiding this study (RQ1–RQ3). First, in Section 5.1, we examine quantitative comparisons of attendance-processing

duration, procedural efficiency, and verification outcomes between manual and robot-assisted methods (RQ1). Next, in Section 5.2, student perceptions of usability, efficiency, and privacy implications are reported (RQ2). Section 5.3 presents lecturer perceptions and qualitative insights regarding system integration, workload impact, and adoption considerations (RQ3). Finally, Section 5.4 presents the combined SUS results from both participant groups.

The study was conducted over a time period of six weeks (weeks 6–11) of the 2025 Spring semester (March and April) at TalTech. It involved 1st- and 2nd-year Bachelor's students enrolled in multiple study programs in engineering and information technology. A total of 7 lecturers teaching 5 courses volunteered to participate in both the manual and robot-assisted attendance check experiments. In total, 32 regular class sessions were included in the study – 11 sessions using manual attendance and 21 sessions using robot-assisted attendance. According to the experimental design (Section 4.2), each group of students participated in three consecutive sessions: one session using manual attendance, followed by two sessions using robot-assisted attendance. However, one planned robot-assisted session was canceled due to scheduling conflicts, resulting in 21 rather than 22 robot-assisted sessions.

5.1 Robot-Assisted Attendance Check

To address RQ1, a comparative evaluation of manual and robot-assisted attendance procedures was conducted to assess attendance-processing duration, procedural efficiency, and identity verification performance under real classroom conditions. Lecturer workload was evaluated separately through self-reported feedback, as presented in Section 5.3.

The study included a comparative analysis of manual and robot-assisted attendance methods using timestamp data recorded in the Attendance Check Experiment Data Sheet developed for this study. Metrics such as total processing time per session and average time per student were analyzed to assess time efficiency. Identity-verification performance was evaluated using the genuine verification success rate (SR) and false-rejection rate (FRR) of robot-assisted attendance attempts. These data points provided a quantitative basis for evaluating attendance-processing efficiency for both methods and identity-verification performance for the robot-assisted method. The analysis used descriptive statistics to examine attendance processing durations across individual classroom sessions. Session-level averages were used to describe variation between sessions, while the overall averages were calculated from the total recorded durations and corresponding numbers of registrations or verification attempts.

The manual attendance check experiment was conducted over a total of 11 classroom sessions, involving 7 lecturers and 192 students who were physically present in the classroom during the sessions in which the manual attendance procedure was implemented. Of these, 184 students (96%) actively participated in the manual attendance check, while 5 students (3%) refused to participate. Participation was voluntary, and no reasons for declining were collected. An additional three (1%) students arrived late and were excluded from the experiment to ensure consistent time measurement.

The total manual attendance time recorded across all 11 sessions was 74 minutes, covering 184 students, averaging 24.1 seconds per student. The average time per student was calculated by dividing the total recorded duration by the number of participating students. The shortest attendance session lasted 2 minutes and 50 seconds ($n = 11$, $\text{avg} = 15\text{s}$), while the longest session lasted 17 minutes and 34 seconds ($n = 43$, $\text{avg} = 25\text{s}$). The minimum average attendance time per student in a single session was 15.4 seconds, observed in a session with 11 students. The maximum average time recorded was 28.8 seconds per student in a session with 16 participants (Figure 7). The variation in average time across sessions may be attributed to contextual factors such as classroom layout, sheet circulation delays, or brief pauses during the signing process.

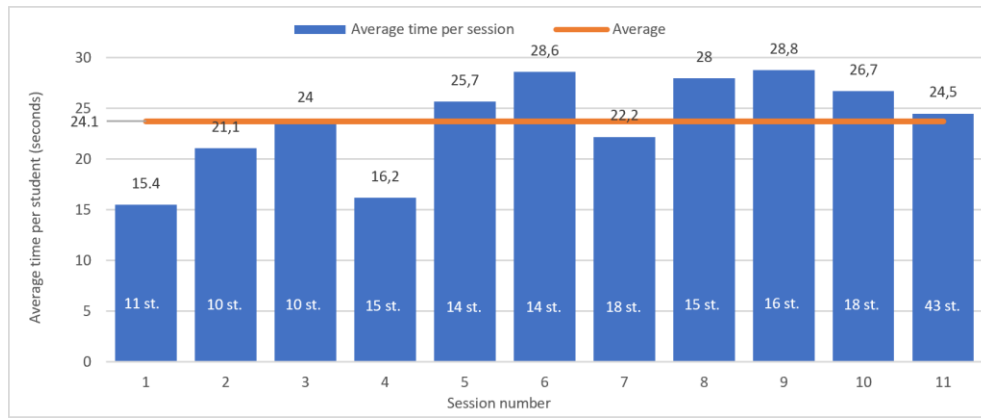


Figure 7. Results for manual attendance check – average time per student per session

We now turn to discuss robot-assisted attendance checking. The robot-assisted attendance check was carried out over 21 classroom sessions, involving 7 lecturers and a total of 171 students. As participation in the experiment was voluntary, students who did not wish to use the robot, or did not have their ID cards with them, or presented non-Estonian ID cards were directed to an alternative manual attendance check process. In total, 97 of the 171 students exposed to the robot-assisted attendance option (57%) used the robot at least once. These students generated 162 recorded verification attempts across 21 sessions, including 160 successful verifications and two identity mismatches. The difference between unique participants and recorded attempts reflects repeated attendance verification across the experimental sessions. Observer-collected data recorded that 70 students (41%) were unable to complete robot-assisted verification due to missing or incompatible identification documents. This group included 35 students (20%) who did not have their ID cards with them, 33 students (19%) using old-generation Estonian ID cards, and 2 students (1%) presenting non-Estonian ID cards. As the system required ICAO-compliant Estonian ID cards issued since August 2021, these documents were not supported. Two (1%) identity-mismatch cases occurred, in which the robot failed to match the student's live image with the photo on their ID card, although both students were correctly identified by the lecturer. This corresponds to a genuine verification success rate of 99% and a false-rejection rate of 1% among the recorded attempts. Throughout the robot-assisted attendance sessions, 138 alternative manual attendance registrations involving 72 students (42%) were recorded. This group included the two students whose robot-assisted identity verification was unsuccessful. Their processing times were included in the 162 robot verification attempts, while their subsequent attendance registrations were recorded through the alternative manual procedure. Seven (4%) refusals to participate in the robot-assisted process were recorded from four (2%) students; two opted for manual attendance, while the remaining two declined both attendance methods. No late arrivals were detected during robot-assisted sessions. The descriptive statistics for manual and robot-assisted attendance checks are presented in Table 1.

Table 1. Descriptive statistics for manual and robot-assisted attendance check

Description	Manual	Robot-assisted
# classroom sessions per attendance check method	11 (34%)	21 (66%)
# total students exposed for the attendance check option	192	171
# unique students participating in attendance check methods	184 (96%)	97 (57%)
# unique students refused to perform the attendance check methods	5 (3%)	4 (2%)
# records for attendance method	184	162
Total recorded time [minutes]	74	27.5
Average time/student for attendance check [seconds]	24.1	17.1

The manual duration represents attendance-sheet circulation, whereas the robot-assisted duration represents logged verification processing. The estimated robot-assisted duration includes an additional 7 seconds for approaching and initiating verification.

To explore the time it takes per student to register using the robot-assisted attendance check, we relied on system logs. A limitation of our approach is that we do not have direct measurements of the complete per-student interaction time. The system logs contain only the processing time from ID card insertion until the verification outcome is recorded and exclude the time required for a student to approach and start using the system. Therefore, we rely on classroom observations indicating that this additional interaction takes approximately 5–7 seconds per student, and we further use the maximum observed value of 7 seconds as the estimated additional interaction time.

According to the system logs, the shortest robot-assisted attendance session was 18 seconds ($n = 2$), while the longest session was 1 minute and 49 seconds ($n = 11$). Across all 21 sessions, the total robot-assisted attendance time was 27 minutes and 28 seconds, based on 162 uses of the system by 97 students (Figure 8).

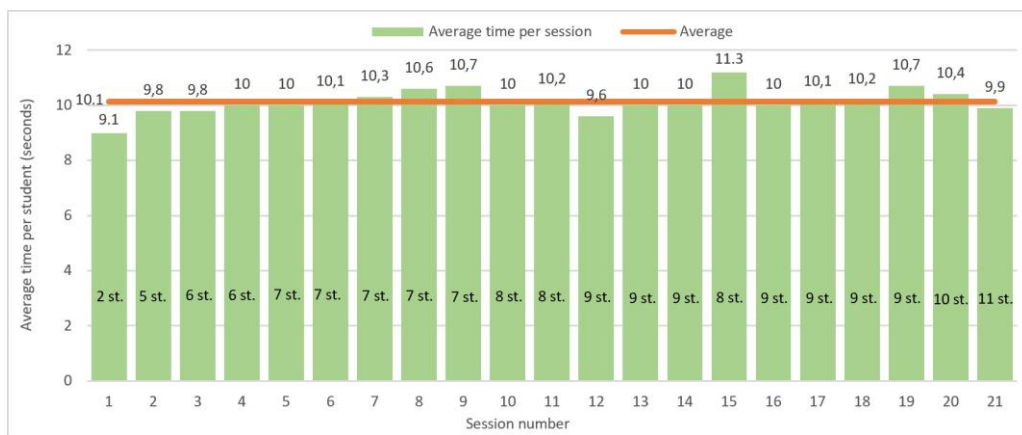


Figure 8. Results for robot-assisted attendance check – average time per student per session

Figures 7 and 8 present session-level results for 11 manual and 21 robot-assisted attendance sessions, respectively. To assess variability across classroom sessions, the standard deviation of session-level average processing times was calculated separately for both attendance methods. Based on the rounded session averages, the standard deviation was approximately 4.7 seconds for manual attendance and 0.5 seconds for robot-assisted internal processing, indicating greater variability across manual attendance sessions.

The minimum average internal processing time per student recorded in a robot-assisted session was 9.1 seconds, while the maximum was 11.3 seconds. Across all 162 uses, the average internal processing time was 10.1 seconds. As the robot-assisted and manual measurements covered different components of the attendance process, their direct comparison is limited. Therefore, we use the interaction time of 7 seconds as the maximum value of the observed 5–7-second range to estimate additional interaction time in the robot-assisted attendance check. This gives an estimated robot-assisted interaction duration of 17.1 seconds per verification attempt on average, with estimated minimum and maximum values of 16.1 and 18.3 seconds, respectively (Figure 9). Based on these measurements, the estimated robot-assisted attendance duration was 17.1 seconds per verification attempt, approximately 29% lower than the observed manual attendance average of 24.1 seconds per student. Both methods used total recorded duration divided by the corresponding number of registrations or verification attempts to calculate average recorded time. However, the manual method measured attendance-sheet circulation, whereas the robot-assisted estimate combined system-recorded processing time with an additional 7 seconds for approaching the robot and initiating verification.

As the experiment considered initial technology adoption, students could use the robot voluntarily throughout the 90-minute class session without a mandatory queue. Individual waiting

times were not measured separately for either attendance method, as the evaluation focused on attendance processing duration. Furthermore, alternative manual registrations operated in parallel and were excluded from the robot-assisted timing analysis. Therefore, the estimated 29% difference reflects the average attendance processing duration under the experimental conditions, focusing on robot-assisted verification attempts compared with manual attendance registration. Overall, the findings suggest that robot-assisted verification offers promising processing efficiency while providing automated identity verification and digital attendance recording.

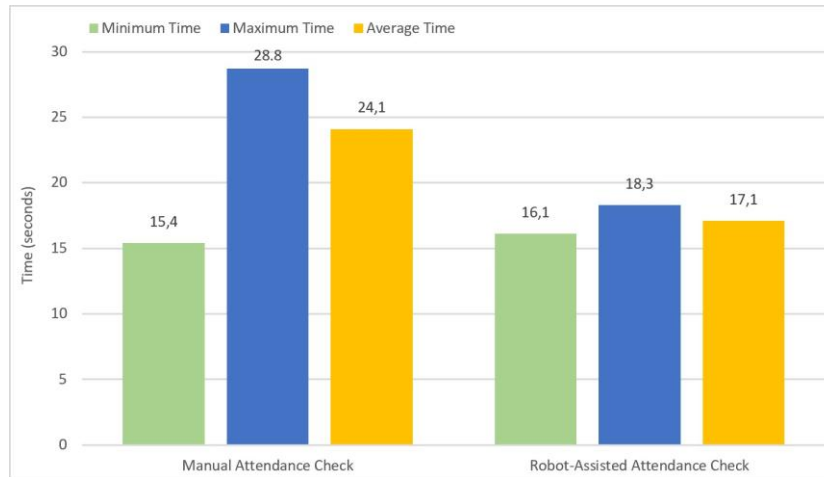


Figure 9. Manual vs. robot-assisted attendance check – average time per student

As part of the automated process, the robot recorded detailed timing data for three key steps: name reading (the time taken to extract the student’s full name from the ID card), image reading (the time taken to extract the ID card photo for facial recognition), and facial recognition (the time taken to compare the extracted image with the student’s live facial image). Time measurement started when the ID card was detected by the system and ended when the verification outcome was recorded in the backend database. The average time for name reading was 0.5 seconds, for ID image reading 9.3 seconds, and for facial recognition 0.3 seconds (Table 2). These values represent internal processing times recorded by the system and sum to 10.1 seconds, which corresponds to the measured average interaction time per student shown in Table 2. The majority of the processing time (92%) is spent on reading data from the ID card, while facial verification itself consists of two steps: retrieving the ID card image and capturing the live camera image followed by face comparison.

Table 2. Timing data for robot-assisted attendance check

	Min	Max	Avg.
Name read [seconds]	0.4	0.6	0.5
Image read from ID card [seconds]	8.4	10.3	9.3
Face recognition [seconds]	0.3	0.4	0.3
Interaction time [seconds]	9.1	11.3	10.1

This analysis highlights the robot’s ability to process attendance efficiently and reliably, while also drawing attention to limitations related to ID card compatibility and biometric verification accuracy.

Lastly, we examine the performance of the robot-assisted multi-factor identity verification process using genuine verification attempts. The evaluation considers the genuine verification success rate (SR), defined as the proportion of genuine attempts resulting in successful verification (Equation 1), and the false-rejection rate (FRR), representing the proportion of genuine verification

attempts incorrectly rejected (Equation 2), consistent with biometric performance evaluation terminology [44].

$$SR = \frac{\text{Successful genuine attempts}}{\text{Total genuine attempts}} \times 100\% \quad (1)$$

$$FRR = \frac{\text{Rejected genuine attempts}}{\text{Total genuine attempts}} \times 100\% \quad (2)$$

A total of 162 genuine verification attempts were recorded, of which 160 were successful and two resulted in identity mismatches. Both rejected students were correctly identified by their lecturers and subsequently registered their attendance manually. Accordingly, the genuine verification success rate was 99% (160/162), while the false-rejection rate was 1% (2/162). These results reflect verification performance for recorded attempts involving supported ID cards; students with missing or incompatible documents were excluded from this analysis. As no controlled impostor attempts were conducted, false-acceptance performance, precision, and F1 scores could not be reliably evaluated.

Overall, the findings provide a qualified answer to RQ1. The estimated robot-assisted attendance duration was 17.1 seconds per verification attempt, compared with an observed average of 24.1 seconds per student during manual attendance, representing a difference of approximately 29% under the experimental conditions. The findings suggest promising attendance processing efficiency, although the two methods were evaluated using different timing procedures. At the same time, the identity verification component achieved a genuine verification success rate of 99% and a false-rejection rate of 1% among the recorded attempts. Although incompatible or missing ID cards limited participation in robot-assisted attendance, identity mismatches were infrequent among the recorded verification attempts. Furthermore, lecturer feedback indicated perceived reductions in administrative workload, as discussed in Section 5.3. Together, these findings suggest that robot-assisted attendance offers promising processing efficiency and identity verification performance, alongside potential benefits for attendance-related administrative workload.

5.2 Socio-Technical Evaluation from Students' Perspective

To address RQ2, which examines student perceptions of usability, efficiency, and privacy implications of the robot-assisted attendance system, a structured user experience survey was conducted following students' exposure to both attendance methods.

Of the 97 students who participated in robot-assisted attendance verification, 94 (97%) completed the ID ACA user experience survey. As participation in the robot-assisted procedure was voluntary, the survey findings primarily reflect the experiences of students who used the system and may not fully represent those who did not participate. The demographic data indicate that the majority of participants (69%) were male ($n = 65$), 26% ($n = 24$) identified themselves as female, and 5% ($n = 5$) preferred not to disclose their gender. In terms of age distribution, the largest group of respondents was aged 18 to 24, accounting for 72 students (77%) of the total participants. This was followed by 11 students (12%) in the 35 to 44 age group, 6 students (6%) aged 25 to 34, and 4 students (4%) aged 45 and over. Only one student (1%) was under the age of 18. These demographics suggest that the survey predominantly reflects the perspectives of young adult students in a university setting (Table 3).

All 94 student respondents completed a survey of eight questions, which used the Likert scale to assess usability, perceived efficiency, reliability, privacy perceptions, comfort with biometric authentication, overall experience, and preference compared to manual attendance (Appendix A).

The student survey results shown in Figure 10 reveal generally positive experiences with the robot-assisted attendance system. A strong majority (91%, $n = 86$) of students found the system easy to use (Q1). While 45% ($n = 42$) of students agreed that the system was faster than traditional

manual attendance methods (Q2), 32% (n = 30) remained neutral, and 23% (n = 22) disagreed, suggesting some variability in perceived efficiency.

Table 3. Student demographic distribution (n = 94)

Category	Subcategory	N (%)
Gender	Male	65 (69%)
	Female	24 (26%)
	Prefer not to say	5 (5%)
Age Group	Under 18	1 (1%)
	18-24	72 (77%)
	25-34	6 (6%)
	35-44	11 (12%)
	45+	4 (4%)

In terms of comfort with using national ID cards and facial recognition, 56% (n = 53) of students responded positively (Q3), while 27% (n = 25) were neutral and 16% (n = 16) expressed discomfort. When asked about personal data privacy concerns, the responses were more divided: 37% (n = 35) disagreed with having concerns, 24% (n = 23) remained neutral, and a slightly higher 39% (n = 36) reported privacy concerns (Q4), highlighting a significant area for improvement in transparency and trust.

Regarding facial recognition performance, 70% (n = 66) of students agreed that the facial recognition process was quick and efficient (Q5), and 72% (n = 68) expressed trust in the accuracy of the attendance records (Q6). The overall experience of using the system was rated positively by 75% (n = 70) of students (Q7), while 21% (n = 20) remained neutral and only 4% (n = 4) responded negatively. Finally, when asked whether they preferred the robot-assisted system over manual methods, 44% (n = 41) of students favored the new approach (Q8), 36% (n = 34) were neutral, and 20% (n = 19) still preferred the manual method. These results indicate generally positive user perception, although preferences for replacing manual attendance were more divided, with concerns mainly related to privacy and perceived speed (Figure 10).

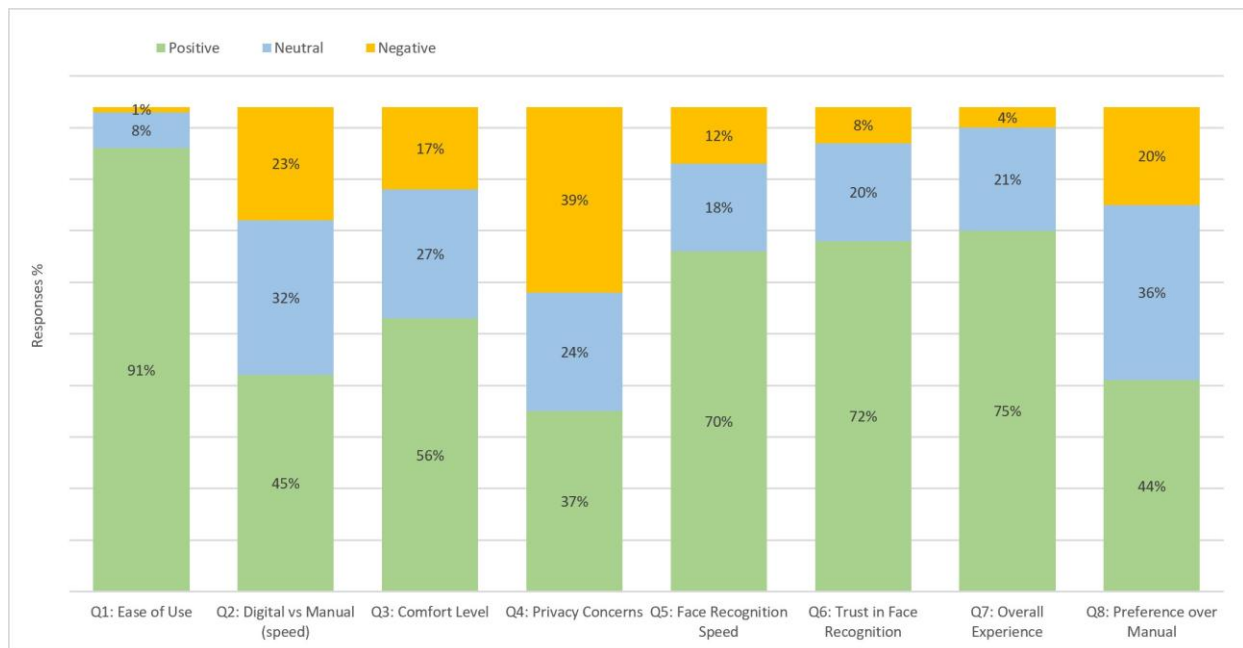


Figure 10. Student survey results

The optional free-form section (Q9) was completed by 13 (14%) students, whose comments primarily addressed privacy concerns, perceived speed, queuing to use the robot assistant, and occasional technical issues. Of the 13 responses, 12 contained substantive comments, while one

(1%) respondent indicated that they had no additional comments. Several students (4%, $n = 4$) expressed dissatisfaction with the facial recognition feature, citing issues with privacy, speed, and discomfort with the synthetic voice used to pronounce names. Some students preferred (2%, $n = 2$) alternative methods such as QR codes, while others (2%, $n = 2$) noted that the system felt slower than manual attendance, especially due to queuing. Technical issues like card reader malfunctions and bugs in the system were also mentioned (2%, $n = 2$). Despite the criticisms, a few comments recognized the potential of the project, with one student (1%) describing it as a “cool project” and another (1%) acknowledging the need for facial recognition while still preferring improved safety measures. These insights highlight the importance of addressing UX, system responsiveness, and transparency in data handling to improve acceptance.

Overall, the findings related to RQ2 indicate that students perceive the robot-assisted attendance system as largely usable and technically reliable, with strong agreement regarding ease of use and system accuracy. However, perceptions of efficiency and privacy were more divided, with a considerable proportion of students expressing concerns about data handling and comparative speed. These results suggest general acceptance of the system among students, while highlighting privacy transparency and process optimization as important areas for refinement.

5.3 Socio-Technical Evaluation from Lecturers’ Perspective

To address RQ3, which investigates lecturers’ perceptions of usability, efficiency, workload impact, and privacy implications of the robot-assisted attendance system, a structured UX survey and semi-structured interviews were conducted among participating lecturers following their experience with both attendance methods.

Before the experiment began, participating lecturers were trained to use the ACD to ensure familiarity with its functionalities and effective management of attendance data. Each lecturer was provided with login credentials, including a username and an initial password that could later be changed for secure access, and their interactions with the system were evaluated to understand its impact on administrative workload and ease of use.

A total of six lecturers (86%) participated in the UX survey of the ID ACA and its associated ACD. Participation in the survey was voluntary, and one lecturer involved in the experimental sessions did not complete the survey. All six respondents completed the eight Likert-scale items assessing perceived workload reduction, efficiency, ease of use, usefulness of reporting features, trust in system accuracy, privacy concerns, acceptability of facial recognition, and preference compared to manual attendance methods. The demographic data shows that the majority of respondents were male, with 4 lecturers identifying as male and 2 choosing not to disclose their gender. No lecturers were identified as female (Table 4). Most respondents were aged 35–44 (50%, $n = 3$), followed by 45–54 (33%, $n = 2$) and 55+ (17%, $n = 1$), with no lecturers under 35, indicating that the survey reflects mid-career to senior academic staff.

Table 4. Lecturer demographic distribution ($n = 6$)

Category	Subcategory	N (%)
Gender	Male	4 (67%)
	Female	0 (0%)
	Prefer not to say	2 (33%)
Age Group	Under 24	0 (0%)
	25-34	0 (0%)
	35-44	3 (50%)
	45-54	2 (33%)
	55+	1 (17%)

The survey (Appendix B) results (Figure 11) reveal that lecturers generally responded positively to the robot-assisted attendance system and its supporting database. Four lecturers (66%) agreed that the system reduced their workload (Q1), while one (17%) remained neutral and one (17%)

disagreed. Perceptions of attendance efficiency followed a similar trend, with four lecturers (66%) agreeing (Q2), one (17%) remaining neutral, and one (17%) disagreeing, showing broad support but also one instance of strong criticism.

Regarding ease of use, all lecturers (100%) rated the ACD system as easy to use (Q3), indicating unanimous positive evaluations of the interface. Similarly, all respondents (100%) agreed that downloading attendance and consent reports was useful (Q4).

Trust in the system's accuracy and reliability was fully positive, with all six lecturers (100%) expressing agreement that the robot-assisted system correctly registered student attendance (Q5). In contrast, data privacy concerns revealed a more divided perspective: three lecturers (50%) expressed concerns (Q6), one (17%) remained neutral, and two (33%) indicated no concerns, reflecting mixed attitudes toward data handling and GDPR compliance.

Regarding the acceptability of facial recognition for attendance in HE, five lecturers (83%) responded positively (Q7), while one (17%) remained neutral. When asked about preference compared to manual attendance methods, four lecturers (67%) expressed a positive preference for the robot-assisted system (Q8), while two (33%) were neutral. Overall, the results indicate strong trust in system reliability and general acceptance of the automated approach, with privacy remaining the most sensitive issue.

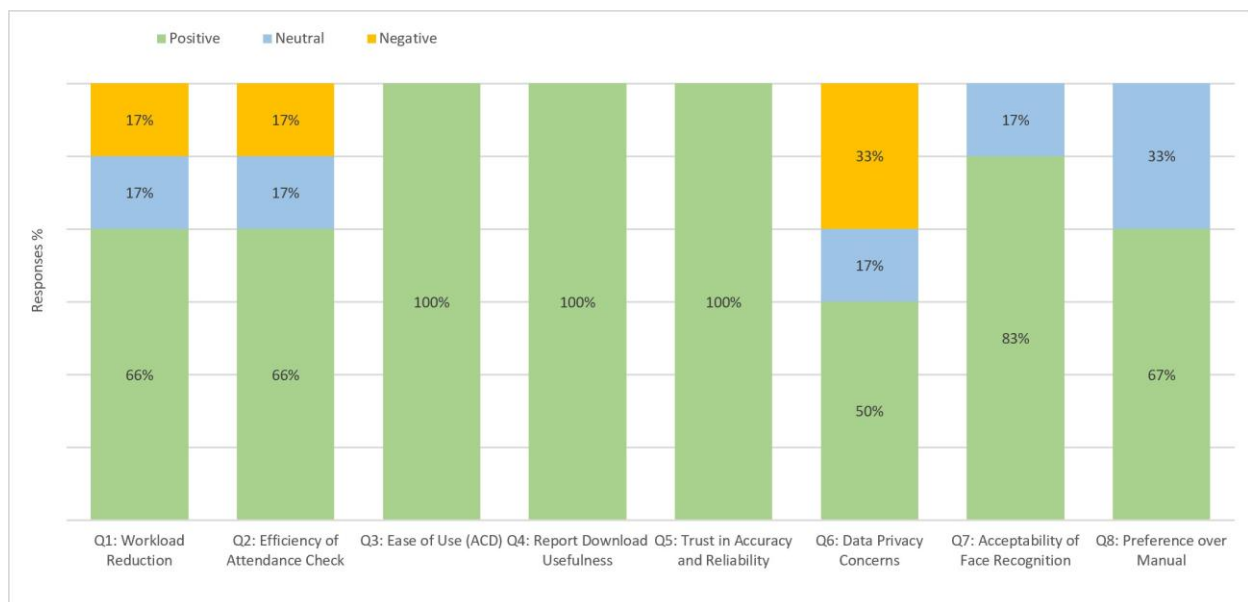


Figure 11. Lecturer Survey Results

The optional free-form section (Q9) was completed by three (50%) lecturers. The free-form comments from lecturers provided a mix of praise and key suggestions regarding the robot-assisted attendance system. One noted the system's efficiency but raised concerns about data privacy and suggested integration with other platforms. Another recommended simplifying the interface to reduce delays. One lecturer criticized the system's scalability and recommended limiting its use to high-trust scenarios like exams. Overall, the comments highlight the need for improved data handling, system integration, and usability.

In addition to the UX survey, semi-structured interviews were conducted with six lecturers after the experimental sessions to explore their experiences with the robot-assisted attendance system and the Lecturer ACD. The interviews addressed overall experience, workload impact, system accuracy, student reactions, and long-term adoption. Each interview lasted approximately 5-10 minutes, was audio-recorded with participant consent, transcribed, and analyzed using an inductive thematic analysis approach [45], [46]. The transcripts were reviewed to identify recurring statements concerning system usability, workload, reliability, privacy, and institutional adoption. To make the thematic findings traceable, the interview transcripts were further reviewed, and

relevant statements were assigned descriptive codes, including “examination suitability,” “reduced manual data entry,” “LMS integration barriers,” “older ID-card incompatibility,” “perceived spoofing risks,” “student curiosity,” “privacy-related hesitation,” and “institutional policy requirements.” Related codes were grouped into five reported themes, retaining both shared experiences and contrasting lecturer perspectives.

The semi-structured interviews covered five open-ended questions:

1. Can you describe your overall experience using the robot-assisted attendance system in your classes? (What worked well? What felt challenging or unusual compared to traditional methods?)
2. How did the use of the robot-assisted attendance system and the Lecturer Attendance Check Database (ACD) affect your administrative workload during and after class sessions? (Did the system and database make attendance management easier or more time-consuming? Was the ACD intuitive to use for viewing or downloading attendance data?)
3. What are your thoughts on the accuracy and reliability of the robot-assisted attendance system compared to manual attendance? (Did you encounter any missed students, mismatches, or unexpected issues?)
4. How did your students respond to the robot-assisted process? Did you observe any hesitation, confusion, or positive reactions? (Were there any noticeable differences between students' behavior with manual and automated attendance?)
5. Do you believe this type of system could be adopted long-term in higher education? Why or why not? What improvements would you recommend before wider implementation? (Consider practicality, privacy concerns, ease of use, and institutional support.)

The thematic analysis resulted in five dominant themes: (1) contextual usefulness, (2) workload and workflow compatibility, (3) reliability and security, (4) student reactions and privacy, and (5) institutional readiness.

Theme 1: Contextual Usefulness. Most lecturers described their overall experience as positive, convenient, and technically functional. However, several emphasized that usefulness depends on the teaching context. In courses where attendance was already managed through controlled digital environments or existing login systems, the robot-assisted method was perceived as supplementary rather than necessary. In contrast, in examination settings or large-cohort scenarios requiring strict identity verification, the system was viewed as highly beneficial. Lecturers repeatedly highlighted exam situations as the strongest use case, particularly when managing large groups efficiently and ensuring that “the right people are in the right place.” Thus, adoption was seen as scenario-specific rather than universally required.

Theme 2: Workload and Workflow Compatibility. Most lecturers reported that the ACD was intuitive, user-friendly, and easy to learn with minimal guidance. Real-time attendance display, automatic saving, and downloadable Excel reports were highlighted as key advantages. Several participants noted reduced administrative workload by eliminating paper-based processes and avoiding manual digitization of attendance sheets.

However, perceptions differed depending on existing workflows. Some lecturers with established automated systems (e.g., Moodle-based or integrated lab platforms) felt the robot-assisted approach could slow their routines due to limited system integration. File reformatting requirements were identified as practical bottlenecks. Integration with existing institutional learning management systems (LMS), such as Moodle, was repeatedly recommended to improve workflow compatibility. Technical enhancements such as RFID-based reading and API interoperability were suggested to increase efficiency and reduce queuing.

Theme 3: Reliability and Security. The system was widely perceived as more reliable than traditional paper-based attendance, which was described as prone to error and falsification. Several lecturers compared the ID-based verification to formal identity checks, emphasizing enhanced security. Accuracy was considered very high, with only isolated mismatches reported.

Some technical concerns emerged, including incompatibility with older-generation ID cards and occasional mismatches due to outdated photos. One lecturer mentioned potential spoofing risks

and the need for stronger anti-spoofing measures, while another emphasized continued lecturer oversight. Despite these issues, overall trust in system accuracy remained strong.

Theme 4: Student Reactions and Privacy. Lecturers generally observed positive or curious student reactions, with many finding the system engaging. Technology-oriented students in particular perceived it as a natural extension of digital tools.

However, some hesitation was noted among a minority of students, mainly due to privacy concerns or reluctance to use ID cards. Lecturers emphasized that transparent communication about data handling is essential to improve participation. Facial recognition was occasionally perceived as a “black box,” potentially affecting trust.

Theme 5: Institutional Readiness. All lecturers acknowledged strong potential for long-term adoption, especially in examinations and identity-sensitive contexts. However, broader implementation requires institutional policy support, legal recognition, and clear privacy governance. Cost, robot availability for class use, and scalability were identified as practical constraints, particularly during peak exam periods.

The qualitative findings were further examined alongside the lecturer survey results (Figure 11). Regarding workload and workflow compatibility (Theme 2), four of six lecturers reported perceived workload reductions, while all six rated the downloadable attendance and consent reports as useful. However, one lecturer disagreed that workload had been reduced, while interview findings also identified integration difficulties. For reliability and security (Theme 3), all six lecturers expressed trust in attendance accuracy, although interview responses identified concerns about document compatibility and potential spoofing. Regarding privacy (Theme 4), three lecturers expressed concerns, one remained neutral, and two reported no concerns, reflecting differing attitudes toward biometric verification. Finally, four lecturers preferred future use of robot-assisted attendance, while two remained neutral, supporting the context-dependent adoption considerations identified under institutional readiness (Theme 5).

In response to RQ3, lecturers expressed strong acceptance of the system’s usability and reliability, with unanimous agreement on system accuracy and ease of use. While most lecturers acknowledged workload reduction and efficiency gains, qualitative interviews revealed context-dependent adoption preferences and concerns related to privacy, scalability, and system integration. Together, the survey and interview findings suggest that the robot-assisted attendance system is perceived as a viable tool for HE, particularly in high-stakes or identity-sensitive scenarios.

5.4 System Usability Scale (SUS) Evaluation

To investigate the usability of the proposed robot-assisted attendance check system, we conducted a survey according to the method by Brooke [15]. The SUS survey included 30 respondents (30%) from both participant groups: 24 students (26%) and six lecturers (86%). The SUS questionnaire is a quick, reliable tool for assessing system usability across diverse contexts. The calculation of the SUS score followed the standard scoring method: for each odd-numbered question, 1 was subtracted from the participant’s score, and for each even-numbered question, the score was subtracted from 5. The resulting adjusted values were then summed and multiplied by 2.5 to obtain the overall SUS score. The final computed SUS score for the system was 80.8.

Since the same anonymous SUS questionnaire was administered to both students and lecturers without participant-group identifiers, individual responses could not be attributed to either group. Consequently, separate SUS scores for students and lecturers could not be calculated retrospectively. The combined score of 80.8, therefore, represents an aggregated usability assessment and does not independently establish the usability of the student-facing ACA and lecturer-facing ACD interfaces.

According to the curved grading scale [16], a SUS score between 80.8 and 84.0 falls within the ‘A’ grade, placing the system in the 90–95th percentile for perceived usability. Scores above this range (84.1–100) correspond to the A+ category, indicating exceptional usability, whereas scores

below 80.8 fall into lower grades (A–, B, C, or below), representing progressively average to poor usability levels. The combined SUS score indicates a positive overall perception of system usability among respondents. However, the absence of group-specific results limits conclusions about the usability of the individual interfaces.

Considering the findings across RQ1–RQ3, the overall socio-technical evaluation indicates that system performance and adoption were shaped by interactions among technical factors, including verification reliability and ID card compatibility; human factors, reflected in student and lecturer perceptions of usability, acceptance, and privacy; and organizational factors, such as lecturer workload, workflow integration, and institutional readiness.

6 Discussion

From a socio-technical perspective, this study evaluated robot-mediated multi-factor attendance verification as an interaction between a technical subsystem (comprising the robot, ID card reader, biometric models, and ACD) and a social-organizational subsystem (comprising students, lecturers, consent and privacy practices, and institutional workflows). Consistent with the principle that technical and human-organizational factors should be considered together [11]–[13], the findings show that processing time and verification reliability alone do not determine the system’s practical value. Its use and adoption are also shaped by identity document compatibility, user acceptance, privacy concerns, lecturer workload, fallback procedures, and integration with existing institutional systems. Beyond attendance tracking, the underlying architecture may support identity verification in other institutional and non-academic contexts.

In response to RQ1, the estimated robot-assisted attendance duration was 17.1 seconds per verification attempt, compared with an observed manual attendance average of 24.1 seconds per student, corresponding to an approximately 29% shorter average duration under the experimental conditions. At the same time, the multi-factor identity verification achieved a genuine verification success rate of 99% and a false-rejection rate of 1%. As impostor attempts were not evaluated, false-acceptance performance remains unverified. These findings demonstrate the potential of integrating national ID-card authentication with live facial recognition to support efficient attendance processing and stronger identity assurance through multi-factor verification.

Unlike QR-code or password-based systems, which remain vulnerable to proxy attendance and credential sharing [4], [5], [8], the multi-factor approach requires physical possession of a trusted credential and biometric confirmation. In comparison to the approach proposed by Budagov [34], our system strengthens identity anchoring by using an official ID document rather than a locally enrolled facial dataset. Similarly, RFID- or fingerprint-based systems [27], [28] provide strong verification but lack mobility and interactive adaptability. The hybrid design in this study combines document authentication, biometric validation, and robotic mobility, enabling flexible deployment at classroom entry points.

The UX findings reinforce the socio-technical interpretation that system adoption depends on the interaction between technical performance, user perceptions, and institutional context. Students rated usability highly (91% agreement on ease of use), and lecturers expressed unanimous trust in the system’s accuracy. However, privacy perceptions among students were divided (39% reporting concerns), highlighting that acceptance of biometric technologies depends not only on technical safeguards but also on transparency and institutional communication. Lecturers emphasized that the system is particularly appropriate for high-stakes contexts such as examinations, suggesting that scenario alignment is critical for sustained use.

The findings also reveal several socio-technical interdependencies. In particular, missing or incompatible ID cards prevented 70 students (41%) from completing robot-assisted verification, demonstrating the practical importance of document availability and compatibility. Consequently, parallel manual attendance registration remained necessary to accommodate students unable to use the automated method. The processing time and lecturer workload associated with manual fallback were not measured, limiting conclusions about the overall efficiency of the combined attendance

workflow. However, the incompatibility of Estonian ID cards issued before August 2021 represents a transitional limitation, as these cards had reached their five-year expiry by August 2026. Their replacement may reduce the need for manual registration, provided the system supports newer ID-card versions, although missing and non-Estonian ID cards remain potential barriers. The ACD reduced manual handling in paper-based workflows, yet limited integration reduced its value in courses with established digital systems. Similarly, technical privacy safeguards did not fully remove participant concerns. Although biometric images were not retained, facial recognition still involved processing sensitive biometric information for individual identification. Furthermore, the ACD maintained identifiable attendance records linking students to specific courses and attendance events. Therefore, privacy risks extend beyond biometric image storage to potential unauthorized access, identification of attendance patterns, and misuse of personal identifiers. Both temporary biometric processing and longer-term management of identifiable attendance records require consideration in the privacy assessment. These interdependencies align with Rajanen [47], who emphasizes balanced relationships among technology, organizations, tasks, and users, and with Saddiqa et al. [48], who show that educational technologies require alignment between technical performance, usability, software compatibility, and stakeholder needs.

The present study used traditional paper-based attendance as the baseline for evaluating the robot-assisted method. However, lecturer interviews revealed that some courses already employed digital attendance systems, including Moodle-based registration, which could reduce the practical benefits of introducing an additional attendance solution. As no digital attendance system was included in the experimental comparison, the findings do not establish whether the proposed approach offers greater processing efficiency or workload reduction than existing digital alternatives. Nevertheless, the integration of national ID-card authentication and live facial verification may provide additional value in scenarios requiring stronger identity assurance, particularly examinations.

The most immediate application of the multi-factor verification system lies in exam attendance verification. Examination settings require strict identity confirmation to prevent impersonation and ensure academic integrity [27], [28], [32]. Manual ID checks are time-consuming [1], [5] and inconsistently applied, while QR-based solutions do not guarantee identity [4], [49]. The high reliability and structured logging capabilities demonstrated in this study position the system as a practical solution for secure exam entry and auditable attendance records. In large lecture courses, the practical impact of per-student processing time depends on student arrival patterns and available attendance registration procedures. To avoid entry delays, queues can be managed through early placement or the parallel use of multiple robots. With an estimated interaction duration of 17.1 seconds per attempt, the system shows potential for routine attendance verification, although efficiency in large classes requires further evaluation.

The system also shows promise for conferences, seminars, and workshops, where identity-confirmed participation may be required for certification, funding documentation, or accreditation reporting. Current event check-in methods often rely on QR codes or printed badges without biometric confirmation [50]. A mobile robotic multi-factor verification point could provide stronger assurance while automating attendance certificate generation through backend logs. However, applicability to international events remains unverified because the current implementation supports only compatible Estonian national ID cards. Broader deployment would require support for additional identity documents or alternative registration procedures.

The architectural pattern implemented in this study, trusted credential reading, live biometric comparison, and structured event logging, extends beyond HE.

In clinical environments, patient misidentification remains a recognized safety concern [51]. A robot-assisted document and facial verification workflow at reception points could streamline check-in while reducing administrative errors and improving traceability. In secure package delivery [52] and logistics [53], identity verification is increasingly required for high-value handovers. Current solutions often rely on one-time codes or app confirmations, which may be

shared. Integrating credential-based verification with facial confirmation would increase delivery assurance and enable non-repudiable logging of transactions. Visitor management in corporate or research facilities could benefit from mobile multi-factor identity verification systems that replace manual sign-in sheets with auditable digital logs [54]. Although a fixed kiosk equipped with an ID card reader and camera could perform the same identity verification procedure, a mobile robot offers potential advantages when equipment needs to be shared across different classrooms, examination rooms, or other institutional settings. The robot can be relocated according to operational needs and potentially support additional educational assistance functions, reducing the need for dedicated attendance stations in individual rooms. Furthermore, the robot's mobility and interactive capabilities could contribute to a more engaging and enjoyable classroom environment. Through autonomous navigation, verbal communication, and personalized interaction, the robot could approach students, provide instructions, and create a more interactive experience that stimulates curiosity and interest in educational technologies. Positive student experiences were reported in both studies: 90% of participants in the earlier pilot [34] described their interactions with the robot as pleasant, while 75% of students in the present study rated their overall experience positively. Lecturer interviews also indicated generally positive and curious student reactions. However, during the experiment, the robot remained positioned at the classroom entrance, and its navigation capabilities and effects on student engagement were not evaluated. Since no direct comparison with a fixed kiosk was conducted, the findings do not establish superiority in processing efficiency, verification accuracy, or cost. A fixed kiosk may be more appropriate for permanent attendance checkpoints, whereas a mobile robot may offer greater flexibility and opportunities for interactive educational applications.

A key strength of the system lies in combining multi-factor verification with identity authentication, robotic interaction, digital reporting, and institutional attendance practices. Its effectiveness depends on the alignment of these technical, human, and organizational components.

Importantly, biometric images are processed only in main memory and not stored in secondary memory, reflecting a privacy-by-design principle aligned with GDPR compliance. Nevertheless, student privacy concerns underscore the need for transparent communication and clearly defined data governance policies to ensure long-term trust.

The lecturer–student relationship also requires particular attention when considering the voluntariness of biometric consent. Before the experiment, students were explicitly informed that participation in either manual or robot-assisted attendance registration was entirely voluntary. Lecturers did not require or pressure students to participate in either procedure, and declining participation did not result in penalties. Students could independently choose their preferred attendance method or decline participation altogether. Ensuring freedom of choice is particularly important when implementing biometric verification in educational environments.

Scalability considerations include broader ID-card compatibility, integration with institutional platforms (e.g., learning management systems), and optimization of throughput in dense entry scenarios. Multi-robot deployments and workflow adjustments may further enhance operational efficiency.

Overall, the socio-technical evaluation indicates that robot-mediated multi-factor identity verification may provide a transferable model for secure and auditable human–robot interaction in higher education and related identity-sensitive institutional settings. Its practical value depends on the combined performance of the verification technology, user interaction, privacy governance, and organizational integration. By evaluating these dimensions together under real classroom conditions, this work contributes evidence on both the technical capability and institutional applicability of robot-mediated attendance verification.

7 Conclusion

Efficient and reliable attendance verification remains a challenge in higher education, particularly in scenarios requiring strong identity assurance, such as examinations or large-group teaching.

Conventional manual methods increase administrative workload, and existing automated approaches often rely on limited authentication mechanisms or fixed infrastructures. This study applied a socio-technical evaluation perspective to a robot-mediated multi-factor attendance verification system, treating its technical components as interdependent with users, consent, privacy practices, and institutional workflows. The primary aim was to assess the system's technical performance together with usability, privacy implications, lecturer workload, and workflow compatibility under real classroom conditions to evaluate its practical applicability for attendance verification in higher education.

The estimated robot-assisted attendance duration was 17.1 seconds per verification attempt, compared with an observed average of 24.1 seconds per student during manual attendance, representing an approximate difference of 29%. At the same time, 99% of genuine verification attempts were successful, with a false-rejection rate of 1%. These findings suggest that combining ICAO-compliant national ID validation with live facial recognition on a mobile robot platform has the potential to improve attendance-processing efficiency and strengthen identity assurance, although further comparative evaluation is necessary. We deem that the results answer RQ1.

Student and lecturer UX surveys indicated generally positive usability perceptions, while the combined SUS score of 80.8 (grade A) reflected an overall usability assessment that could not be differentiated by participant group (Section 5.4). Lecturers trusted the system's accuracy and reported reduced workload, especially in identity-sensitive scenarios, while students found it easy to use but expressed mixed views on privacy, indicating the need for clear communication when deploying biometric technologies. We deem that the results answer RQ2 and RQ3.

Overall, the socio-technical evaluation suggests that the proposed robot-mediated multi-factor identity verification may provide a feasible approach to attendance checking in higher education, particularly in identity-sensitive scenarios such as examinations, with promising estimated attendance processing times under the observed classroom conditions. However, successful adoption depends not only on processing efficiency and verification reliability but also on user trust, document accessibility, privacy governance, manual fallback arrangements, and integration with institutional workflows.

Despite promising results, several limitations must be acknowledged. First, the system was configured to operate exclusively with Estonian national ID cards supporting the ICAO standard and EstID interface, limiting generalizability to other national identity documents. Students using older-generation Estonian ID cards or non-Estonian IDs were unable to complete automated verification and were redirected to manual attendance. This restriction may particularly affect international students, including newly enrolled first-year students who may not possess supported identity documents, limiting the system's applicability in institutions with diverse international student populations. Second, only 97 of the 171 students (57%) used the robot-assisted method, while 70 students (41%) were unable to complete verification due to missing or incompatible ID cards. As participation was voluntary, students who used the system may have been more comfortable with the technology or better prepared with compatible documents, introducing potential selection bias. Consequently, the verification performance and usability findings may not fully represent the broader student population, limiting the generalizability of the results. Third, the manual and robot-assisted attendance methods were evaluated using different time measurement procedures. The robot-assisted processing time was supplemented with an estimated 7 seconds for approaching the robot and initiating verification, resulting in an approximately 29% shorter average attendance processing duration compared with the manual method. Furthermore, the robot-assisted sessions represented an initial technology adoption period, during which students could approach the robot voluntarily throughout the 90-minute class session. Additionally, lecturer active time was not directly measured. Therefore, the reported workload benefits reflect lecturer perceptions rather than objectively measured reductions in administrative work. Fourth, the biometric evaluation was limited to genuine verification attempts, as no controlled impostor attempts were conducted to assess false-acceptance performance. Finally,

although biometric images were processed only in memory and not stored, privacy perceptions among participants indicate that technical safeguards alone do not eliminate user concerns.

Taken together, the findings should be interpreted as promising, yet preliminary, evidence of the feasibility and applicability of robot-mediated attendance verification under the specific experimental conditions. Although the results indicate potential benefits regarding processing efficiency, identity verification, and user acceptance, the evaluation was conducted within a limited institutional context and does not establish the system's effectiveness across different educational environments or attendance workflows. Therefore, the findings should not be generalized beyond the evaluated conditions without further empirical validation. Nevertheless, the study provides a foundation for subsequent investigations into the technical, human, and organizational factors influencing the wider adoption of robot-assisted attendance verification in higher education.

Future research will focus on expanding ID compatibility to support multiple national identity documents and potentially switching to NFC-based readers to eliminate the need for physical card insertion. Evaluating the system in formal examination settings would provide stronger validation of its applicability in high-integrity environments. Future experiments could also include controlled impostor verification attempts to assess false-acceptance rates and evaluate the effectiveness of the system's anti-spoofing mechanisms. Scalability improvements, such as deploying multiple robots simultaneously to reduce queuing time in large cohorts, could also be explored. Future studies could also examine attendance processing efficiency following a longer technology familiarization period and evaluate the complete attendance workflow, including student waiting times and alternative manual registrations. Additionally, long-term investigations could examine institutional integration with learning management systems, optimization of biometric processing speed, and cross-domain applications such as secure event management or identity-sensitive service workflows. Future experiments are also planned at universities outside Estonia to evaluate the system's applicability across different educational environments, national identity document standards, and institutional attendance workflows. Such evaluations would provide further evidence of the system's generalizability, user acceptance, and potential for adoption beyond the Estonian higher education context.

References

- [1] F. Alali, W. AlGhamdi, N. Albasara, and A. Bashar, "Cognito: A Multipurpose Robotic Assistant for Higher Education Environment," in *2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, IEEE, 2023, pp. 145–151. Available: <https://doi.org/10.1109/EECSI59885.2023.10295871>
- [2] M. M. Al-Dabbagh, "A Review of Students Attendance Management Systems," *Eurasian Journal of Science and Engineering*, vol. 10, no. 3, pp. 136–145, 2024. Available: <https://doi.org/10.23918/eajse.v10i3p13>
- [3] K. Hubbard and L. Tallents, "Challenging, Exciting, Impersonal, Nervous: Academic Experiences of Large Class Teaching within STEM," *Journal of Perspectives in Applied Academic Practice*, vol. 8, no. 1, pp. 59–73, 2020. Available: <https://doi.org/10.14297/jpaap.v8i1.405>
- [4] M. S. Mohammed and K. A. Zidan, "Enhancing attendance tracking using animated QR codes: a case study," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1716–1723, 2023. Available: <https://doi.org/10.11591/ijeecs.v31.i3.pp1716-1723>
- [5] S. Z. Sweidan, S. M. Alsharif, and K. A. Darabkh, "SCATAA-CT: smart course attendance tracking android application in classroom teaching," *International Journal of Computer Applications in Technology*, vol. 67, no. 1, pp. 79–97, 2022. Available: <https://doi.org/10.1504/IJCAT.2021.120740>
- [6] V. Darshan, D. S. Kenny, H. R. Shreyas, N. Vinay, and S. Revathi, "IoT Based Attendance Monitoring System Using Facial Recognition," in *2024 Second International Conference on Advances in Information Technology (ICAIT)*, IEEE, 2024. Available: <https://doi.org/10.1109/ICAIT61638.2024.10690462>
- [7] P. P. Jadhav, Y. D. Patil, S. P. Shah, A. A. Mane, and S. S. Barphe, "ScanIn: QR Code based Attendance System using Python," in *2023 International Conference on Sustainable Communication Networks and*

Application (ICSCNA), IEEE, 2023, pp. 1491–1496. Available: <https://doi.org/10.1109/ICSCNA58489.2023.10370666>

- [8] Prapti V. Kallawar and Suresh S. Asole, “Divergent Techniques of Attendance Management,” *International Journal of Scientific Research in Science and Technology*, vol. 11, no. 2, pp. 458–462, Apr. 2024. Available: <https://doi.org/10.32628/IJSRST52411285>
- [9] N. Salih Ali, M. Nasser Al-Mhiqani, Z. Hussein Arif, and N. Azma Zakaria, “Attendance Management System for Educational Sector: Critical Review,” *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 7, no. 8, pp. 60–66, 2018. Available: <https://ijcsmc.com/index.php/volume-7-issue-8/>
- [10] M. Rajput and T. Singh, “Face-Recognition Attendance Management System,” *International Journal for Research Trends and Innovation*, vol. 8, no. 4, pp. 492–498, 2023.
- [11] E. Mumford, “The story of socio-technical design: reflections on its successes, failures and potential,” *Information Systems Journal*, vol. 16, no. 4, pp. 317–342, 2006. Available: <https://doi.org/10.1111/j.1365-2575.2006.00221.x>
- [12] G. Baxter and I. Sommerville, “Socio-technical systems: From design methods to systems engineering,” *Interacting with Computers*, vol. 23, no. 1, pp. 4–17, 2011. Available: <https://doi.org/10.1016/j.intcom.2010.07.003>
- [13] C. W. Clegg, “Sociotechnical principles for system design,” *Applied Ergonomics*, vol. 31, no. 5, pp. 463–477, 2000. Available: [https://doi.org/10.1016/S0003-6870\(00\)00009-0](https://doi.org/10.1016/S0003-6870(00)00009-0)
- [14] R. P. Bostrom and J. S. Heinen, “MIS Problems and Failures: A Socio-Technical Perspective: Part II: The Application of Socio-Technical Theory,” *MIS Quarterly*, vol. 1, no. 4, pp. 11–28, 1977. Available: <https://doi.org/10.2307/249019>
- [15] J. Brooke, “SUS: A ‘Quick and Dirty’ Usability Scale,” in *Usability Evaluation in Industry*, 1996.
- [16] J. R. Lewis and J. Sauro, “Item Benchmarks for the System Usability Scale,” *Journal of Usability Studies*, vol. 13, no. 3, pp.158–167, 2018.
- [17] B. Thakur and R. Chakre, “A Systematic Review on Smart Attendance System Leveraging Deep Learning-Based Face Recognition Techniques,” *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 27, no. 4, pp. 80–86, 2025.
- [18] A. Abu Snehneh and W. A. Salah, “Smart Attendance System for University Students Based on QR Code,” *Journal of Electrical and Electronics Engineering*, vol. 18, no. 1, pp. 5–10, 2025. Available: <https://electroinf.uoradea.ro/index.php/jeee/13-cercetare/reviste/jeee/236-vol-18-nr-1-may-2025.html>
- [19] Z. Zhang, Z. He, K. Mostafa, and B. Quadir, “Facial Recognition Educational Attendance System,” in *Selected Proceedings from the 2nd International Conference on Intelligent Manufacturing and Robotics, ICIMR 2024, Lecture Notes in Networks and Systems*, vol. 1316, 2025, pp. 253–269. Available: https://doi.org/10.1007/978-981-96-3949-6_19
- [20] V. Krishna, D. P. Mankame, B. Patil, and V. Dhavalgi, “Smart ID Cards for Colleges to Track Attendance and Student Information on Campus,” *International Journal of Research Publication and Reviews*, vol. 5, no. 7, pp. 4633–4639, 2024. Available: <https://ijrpr.com/uploads/V5ISSUE7/IJRPR31842.pdf>
- [21] M. Mohyiddeen, A. E. Amal, M. Varghese, M. K. Rasnal A, and R. N. Sekhar, “SARA: A College Receptionist System,” *International Journal on Emerging Research Areas (IJERA)*, vol. 3, no. 1, pp. 84–88, 2023. Available: <https://doi.org/10.5281/zenodo.8015917>
- [22] V. D. Nguyen, H. Van Khoa, T. N. Kieu, and E. N. Huh, “Internet of Things-Based Intelligent Attendance System: Framework, Practice Implementation, and Application,” *Electronics*, vol. 11, no. 19, article 3151, 2022. Available: <https://doi.org/10.3390/electronics11193151>
- [23] D. Srivastava, S. Anwarul, A. Rai, A. Pal, and A. Srivastava, “Attendify: A Facial Recognition-Based Automated Institutional Attendance System Application,” in *2024 13th International Conference on System Modeling & Advancement in Research Trends (SMART)*, IEEE, 2024, pp. 662–667. Available: <https://doi.org/10.1109/SMART63812.2024.10882197>
- [24] Mardiana, M. A. Muhammad, and Y. Mulyani, “Library Attendance System using YOLOv5 Faces Recognition,” in *2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE)*, 2021, pp. 68–72. Available: <https://doi.org/10.1109/ICCTEIE54047.2021.9650628>

- [25] J. B. Olojido and B. J. Oladimeji, "A Face Recognition-Based System for Monitoring Examination Attendance: A Case Study in a Tertiary Institution," *Faculty of Natural and Applied Sciences Journal of Computing and Applications*, vol. 2, no. 3, pp. 73–80, 2025. Available: <https://doi.org/10.63561/jca.v2i3.838>
- [26] M. Rukhiran, S. Wong-In, and P. Netinant, "User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model," *Sustainability*, vol. 15, no. 4, article 3092, 2023. Available: <https://doi.org/10.3390/su15043092>
- [27] R. Nagendra et al., "Biometric and RFID Passive Tag based Student Identification System for Secure Attendance Management," in *2023 4th International Conference on Intelligent Engineering and Management (ICIEM)*, IEEE, 2023. Available: <https://doi.org/10.1109/ICIEM59379.2023.10166924>
- [28] H. Üçgün, E. İleri, U. Yüzgeç, and R. Yayla, "Development of Microcontroller Based Two Stage Student Attendance Management System," *Academic Perspective Procedia*, vol. 1, no. 1, pp. 429–437, 2018. Available: <https://doi.org/10.33793/acperpro.01.01.86>
- [29] A. Y. Mustafa and L. M. Jawad, "Electronic Student Attendance Management System Based on ID-Card," *Sumer Journal for Pure Science (SJPS)*, vol. 1, no. 1, pp. 56–66, 2022. Available: <https://journals.sujps.com/index.php/sj/article/view/11>
- [30] L. Hakim, S. P. Kristanto, D. Yusuf, and N. Z. Fanani, "Empowering Library Attendance System with IoT-Enabled Student ID Cards," in *2023 International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation (ICAMIMIA)*, IEEE, 2023, pp. 673–678. Available: <https://doi.org/10.1109/ICAMIMIA60881.2023.10427690>
- [31] J. Sathishkumar, S. Asritha, K. Kiruthika, and S. Sandhiya, "Realtime Automated Classroom Attendance Monitoring System Using RFID," *IJSRED-International Journal of Scientific Research and Engineering Development*, vol. 8, no. 1, pp. 1347–1354, 2025. Available: <https://doi.org/10.5281/zenodo.15152194>
- [32] B. Benyó, B. Sódor, T. Doktor, and G. Fördös, "Student attendance monitoring at the university using NFC," in *Wireless Telecommunications Symposium 2012*, 2012, pp. 1–5. Available: <https://doi.org/10.1109/WTS.2012.6266137>
- [33] T.-W. Chiang et al., "Development and Evaluation of an Attendance Tracking System Using Smartphones with GPS and NFC," *Applied Artificial Intelligence*, vol. 36, no. 1, article 2083796, 2022. Available: <https://doi.org/10.1080/08839514.2022.2083796>
- [34] F. Budagov, J. Leoste, M. T. Meeran, T. Robal, and L. B. Leoste, "Attendance Check of Students via Robot Assistant in Higher Education Classes," in *Futureproofing Engineering Education for Global Responsibility, Lecture Notes in Networks and Systems*, vol. 1260, 2025, pp. 305–316. Available: https://doi.org/10.1007/978-3-031-85652-5_31
- [35] International Civil Aviation Organization, "Machine Readable Travel Documents, Part 1: Introduction," 2021. Available: https://www.icao.int/sites/default/files/publications/DocSeries/9303_p1_cons_en.pdf. Accessed on Jun. 14, 2026.
- [36] EUR-Lex, "Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement," 2019. Available: <https://eur-lex.europa.eu/eli/reg/2019/1157/oj/eng>. Accessed on Jun. 14, 2026.
- [37] International Civil Aviation Organization, "Machine Readable Travel Documents, Part 11: Security Mechanisms for MRTDs," 2021. Available: https://www.icao.int/sites/default/files/publications/DocSeries/9303_p11_cons_en.pdf. Accessed on Jun. 14, 2026.
- [38] Republic of Estonia Information System Authority, "EstEID v. 3.5. Estonian Electronic ID card application specification," 2013. Available: <https://www.ria.ee/sites/default/files/documents/2022-11/RIA-EstEID-3.5.pdf>. Accessed on Jun. 14, 2026.
- [39] J. Xiang and G. Zhu, "Joint face detection and facial expression recognition with MTCNN," in *2017 4th International Conference on Information Science and Control Engineering (ICISCE)*, IEEE, 2017, pp. 424–427. Available: <https://doi.org/10.1109/ICISCE.2017.95>
- [40] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823. Available: <https://doi.org/10.1109/CVPR.2015.7298682>
- [41] O. Lucena, A. Junior, V. Moia, R. Souza, E. Valle, and R. Lotufo, "Transfer Learning Using Convolutional Neural Networks for Face Anti-spoofing," in *Image Analysis and Recognition*, 2017, pp. 27–34. Available: https://doi.org/10.1007/978-3-319-59876-5_4

- [42] EUR-Lex, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance),” 2016. Available: <http://data.europa.eu/eli/reg/2016/679/oj>. Accessed on Jun. 14, 2026.
- [43] R. B. Johnson and A. J. Onwuegbuzie, “Mixed Methods Research: A Research Paradigm Whose Time Has Come,” *Educational Researcher*, vol. 33, no. 7, pp. 14–26, 2004. Available: <https://doi.org/10.3102/0013189X033007014>
- [44] International Organization for Standardization, “ISO/IEC 19795-1:2021. Information technology — Biometric performance testing and reporting — Part 1: Principles and framework,” 2021. Available: <https://www.iso.org/standard/73515.html>
- [45] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006. Available: <https://doi.org/10.1191/1478088706qp063oa>
- [46] M. E. Kiger and L. Varpio, “Thematic analysis of qualitative data: AMEE Guide No. 131,” *Medical Teacher*, vol. 42, no. 8, pp. 846–854, 2020. Available: <https://doi.org/10.1080/0142159X.2020.1755030>
- [47] M. Rajanen, “One Design Rule to Rule Them All: Towards a Universal Golden Rule for Designers of Human-Technology Interaction,” *Complex Systems Informatics and Modeling Quarterly*, no. 33, pp. 1–13, 2022. Available: <https://doi.org/10.7250/csimq.2022-33.01>
- [48] M. Saddiq, M. Kirikova, R. Magnussen, B. Larsen, and J. Pedersen, “Towards Using Sensors as Data Sources in Teaching: Requirements for School Curricula-Compatible Sensors,” *Complex Systems Informatics and Modeling Quarterly*, no. 26, pp. 78–93, 2021. Available: <https://doi.org/10.7250/csimq.2021-26.05>
- [49] J. Hendrawan, I. D. Perwitasari, and F. Maulana, “QR Code-Based Attendance Systems in Education: A Systematic Literature Review on Data Accuracy and Sustainable School Management,” in *Proceedings of The International Conference on Computer Science, Engineering, Social Science, and Multi-Disciplinary Studies*, vol. 1, pp. 80–87, 2025. Available: <https://doi.org/10.64803/cessmuds.v1.14>
- [50] R. Collins, “Event Management System with QR Code-Based Check-in,” *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, vol. 2, no. 3, 2025. Available: <https://doi.org/10.63345/sjaibt.v2.i3.203>
- [51] L. Schulmeister, “Patient misidentification in oncology care,” *Clinical Journal of Oncology Nursing (CJON)*, vol. 12, no. 3, pp. 495–498, 2008. Available: <https://doi.org/10.1188/08.CJON.495-498>
- [52] Y. Yang, P. Gope, A. Pasikhani, and B. Sikdar, “Privacy-Preserving Robotic-Based Multi-Factor Authentication Scheme for Secure Automated Delivery System,” *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 11860–11875, 2025. Available: <https://doi.org/10.1109/TIFS.2025.3623374>
- [53] C.-L. Chen, D.-P. Lin, H.-C. Chen, Y.-Y. Deng, and C.-F. Lee, “Design of a Logistics System with Privacy and Lightweight Verification,” *Energies*, vol. 12, no. 16, article 3061, 2019. Available: <https://doi.org/10.3390/en12163061>
- [54] V. P. Prabhulkar, N. D. Adulkar, S. C. Gurav, and B. Tekwani, “Visitor Management System using Convolutional Neural Network,” *IJEDR – International Journal of Engineering Development and Research*, vol. 8, no. 4, pp. 211–221, 2020. Available: <https://rjwave.org/ijedr/viewpaperforall.php?paper=IJEDR2004035>

Appendix A. Student User Experience Survey Questions

Table A1. Student User Experience Survey Questions

#	Questions	Scale
Q1	How easy was it to use the robot-assisted attendance system?	5. Very Easy / 4. Somewhat Easy / 3. Neutral / 2. Somewhat Difficult / 1. Very Difficult
Q2	The robot-assisted system made the attendance process faster than manual methods.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q3	I felt comfortable using my national ID card and facial recognition for attendance registration.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q4	I had concerns about my personal data privacy while using the system.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q5	The facial recognition process was quick and efficient.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q6	I trust that my attendance records are accurate and error-free in the robot-assisted system.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q7	I found the overall experience of using the robot for attendance registration to be pleasant.	5. Very Pleasant / 4. Somewhat Pleasant / 3. Neutral / 2. Somewhat Unpleasant / 1. Very Unpleasant
Q8	I would prefer using the robot-assisted system over traditional manual attendance methods.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree

Appendix B. Lecturer User Experience Survey Questions

Table B1. Lecturer User Experience Survey Questions

#	Questions	Scale
Q1	The robot-assisted attendance system reduced my workload compared to manual attendance methods.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q2	The system improved the efficiency of attendance tracking in my class.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q3	I found the Lecturer Attendance Check Database (ACD) easy to use and manage.	5. Very Easy / 4. Somewhat Easy / 3. Neutral / 2. Somewhat Difficult / 1. Very Difficult
Q4	The ability to download attendance reports from the database was beneficial.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q5	I trust the accuracy and reliability of the robot-assisted attendance system.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q6	I had concerns about student data privacy and security in the attendance system.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q7	The use of facial recognition technology in attendance tracking is an acceptable method in higher education.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree
Q8	I would prefer using the robot-assisted attendance system over manual attendance tracking in future courses.	5. Strongly Agree / 4. Agree / 3. Neutral / 2. Disagree / 1. Strongly Disagree