sustainability

MDPI

Article

User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model

Meennapa Rukhiran [1], Sethapong Wong-In [2] and Paniti Netinant [2,*]

[1] Faculty of Social Technology, Rajamangala University of Technology Tawan-OK, Chanthaburi 22210, Thailand
[2] College of Digital Innovation Technology (DIT), Rangsit University, Pathum Thani 12000, Thailand
* Correspondence: paniti.n@rsu.ac.th

Abstract: Identity recognition is influenced at all educational levels by biometric technology. The invention of facial recognition technology has added new efficiencies to the traditional method of tracking student examination attendance. This study aims to determine whether biometric recognition technologies could be utilized to enhance undergraduate examination attendance systems. The study examined the perceptions of first-year college students regarding the system's use of face recognition technologies. Based on the proposed framework, experimental results were obtained by developing and deploying unimodal and multimodal face recognition methods. Using a quasi-practical design with sample groups, undergraduate students' perceptions of traditional and biometric examination attendance were compared. Adopting the Theory for Reasoned Action and the Technology Acceptance Model, a questionnaire was distributed and analyzed to determine perception factors. The findings reveal that perceived ease of use, and trust and security significantly impact perceived usefulness. It was discovered that perceived usefulness significantly affects behavioral intention to use a system. According to the research findings, multimodal biometric recognition receives significantly more positive ratings than unimodal biometric recognition. This study proposes that universities utilize biometric technology, particularly facial recognition, to assess users' acceptance of the system.

Keywords: biometric; examination attendance; face recognition; user perception; framework

Citation: Rukhiran, M.; Wong-In, S.; Netinant, P. User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model. *Sustainability* **2023**, *15*, 3092. https://doi.org/10.3390/su15043092

Academic Editor: Diego Monferrer

Received: 28 December 2022
Revised: 18 January 2023
Accepted: 6 February 2023
Published: 8 February 2023

1. Introduction

Universities have a significant requirement that students participate in class examinations. Student examinations are essential to students' academic success at all educational levels [1,2]. Traditionally, students are required to present identification to proctors before entering the examination room to verify their identities. The signature of each student is required on an examination attendance list. The traditional method of identity verification examines identification cards, driver's licenses, and passports. This method is insufficient in terms of accuracy and efficiency, which can lead to class discipline, monitoring, and fraud [3], especially in a large examination classroom [4]. Student identification is susceptible to forgery, loss, obsolescence, and damage. Students could sign the examination attendance list on behalf of classmates who could not attend. In large examination rooms, proctors may take longer to verify students' identities, which may negatively affect students' cognitive psychology [5]. Due to human error, proctors need technological tools to ensure the accuracy of student verification [6]. A modern university uses information technology extensively in a variety of areas, including admissions, registration, surrounding information, schedule management, learning, exams, and web-based exams [7–10]. The well-known online systems are made to handle important information and general tasks [11], and students use a username and password to log in and verify their identity [12].

Utilizing biometric technology to verify students is a reasonable solution. A student is not required to carry any identification with them. Numerous biometric techniques

are being used at present in various applications, involving fingerprint authentication for check-in and check-out [13] and face recognition for granting access to cloud services [14]. To ensure system accuracy and efficiency, some propose using unimodal and multimodal biometric techniques [15–18]. At present, no proposed verification system utilizes multimodal biometrics to verify student attendance on examinations. The hard work of figuring out how to use information technology to verify a student's identity is crucial to helping students with exam attendance verification.

Several identification and verification systems based on biometric recognition have been proposed, such as fingerprint [19,20] and facial recognition [21–26]. The other proposed verification system made use of barcodes [27], QR codes [28], Near-Field Communication (NFC) [29], and Radio Frequency Identification (RFID) [30–32]. Ahmed et al. [33] used fingerprint recognition to establish a security framework for online examination. Emmanuel and Okonkwo [34] also developed a biometric authentication system for Nigerian students. The other reason an educational institution might use a biometric system [35] is to create a biometric system that can use the iris to check if a student is in class.

Biometric technology's advantages, made possible by the Internet of Things (IoT), have resulted in its widespread use as a verification device in various applications. While Awojide et al. [36], Jain et al. [37], and Zainal et al. [20] have proposed an IoT user attendance system based on fingerprint recognition, the issue to date of a high number of users may result in a long queue and require a significant amount of time to verify each student. Facial recognition is an effective technique that requires a large amount of personal data. Numerous studies on unimodal face recognition have been investigated to allow students to verify a student's classroom attendance automatically [26,38].

Our previous work designed and explained a framework and architecture for student biometric recognition [39]. The authors developed an IoT-based student biometric recognition system for examination attendance in this work. As such, this system examines students' perceptions of the examination attendance system using facial biometric technologies compared to traditional and biometric approaches, particularly unimodal and multimodal biometric recognition. There are several critical concerns to be addressed in this study to improve student recognition and simplify the operational practice of facial recognition. The research questions were developed to support the study's objectives as follows:

Q1: What affects students' perceptions of using biometric technology for identity verification of examination attendance?

Q2: Which biometric technology, based on unimodal or multimodal face recognition, do students desire to use for the purpose of attendance verification during examinations?

2. Literature Review

2.1. Biometric Technology

Biometric technology is widely used for two primary purposes: identification and access control [40]. Numerous biometric technology studies are underway, at present, in various recent areas, including algorithms, architectures, modalities, and empirical studies. Three broad categories of biometric studies exist. Physical biometric verification entails the examination of physical characteristics of the human body, including the face, fingerprints, palm, hand geometry, retina, and iris. Behavioral biometrics studies human operations, such as speech, signature, posture, keystroke dynamics, and other behavioral biometric authentication activities on smartphones [41]. Chemical biometrics is the study of chemical cues associated with humans, such as personal odor. The human face is the most important biometric feature, as it is used in various applications, including felon recognition, security systems, forensics, observation systems, and credit card verification.

Generally, biometric systems are classified into two types [42]: unimodal and multimodal [43,44]. A unimodal system uses a single biometric source, such as the face, iris, fingerprint, palm, or other human body parts. By enhancing the performance of a biometric recognition system known as multimodal biometric recognition, multiple physical characteristics of humans can be identified. Four subcategories of multimodal biometric

recognition systems exist, including (1) multiple modalities: the recognition of a subject using more than two types of biometric technologies, such as a face and fingerprint. Ammour et al. [45] used facial and iris recognition to identify individuals in the system. Gunasekaran et al. [46] identified individuals through face, fingerprint, and iris blending. (2) Multiple sensors employ the same inspection pattern, for example, by combining images from two cameras. Zhao et al. [47] detected objects using two cameras on a mobile phone. (3) Multiple features: employ multiple algorithms to extract features from images or data, for instance, fingerprint extraction is to be used in conjunction with the first and second algorithms. (4) Multiple and repeated instances: using one or more biometric forms, such as left- and right-iris images for iris recognition, or using the same biometrics in recognition processes. Ye et al. [25] presented a concise overview of deep learning techniques for the re-identification of individuals. Additionally, numerous recent research papers discussed the multimodal biometric approach. Fenu et al. [21] described a multi-biometric recognition system for continuous learner validation in e-learning systems. The system authenticates and authorizes students' entries using their faces and fingerprint. Traore et al. [24] proposed a framework for an online examination that incorporates a multimodal biometric system that utilizes the continuous capture of images via a web camera.

Numerous published articles on contemporary biometric research discuss multimodal biometric technologies. Chen et al. [48] proposed a multimodal framework in their pioneering Variational Bayesian Extreme Learning Machine (VBELM). They created a block using facial images and fingerprint templates generated from a feature-image matrix. The proposed approach retrieved the core layer semantic aspects of local features, resulting in increased characterization capabilities, element reduction, and improved correctness for multimodal biometrics. In terms of generalization, testing accuracy, efficiency, and stability, the VBELM outperforms traditional methods. Gomez-Barrero et al. [49] described a technique for improving a multimodal biometric approach based on the homomorphic encoding technique, which encrypts all database data. Multimodal biometric fusion is a term that refers to the combination of features, scores, and decision levels. The experiments were performed using an online signature and fingerprint recognition database. The system complies with the ISO/IEC 24745. Biometric technology demonstrates that the biometric approach is applicable in a wide variety of fields. As a result, this study focused on the applications of unimodal and multimodal biometric recognitions that can be used to determine a student's examination attendance in place of the traditional method.

2.2. Related Face Recognition

Face recognition is the most widely used method for identifying and verifying individuals in person. A face recognition system's three critical processes are detection, feature extraction, and facial similarity. Face recognition applies to a broad range of research fields. For instance, Dass et al. [50] concentrated on face recognition techniques and real-time face recognition on the Raspberry Pi. Yadav and Vishwakarma [51] proposed a novel, advanced, efficient framework based on interval type-II fuzzy membership and a kernel-based sparse method. They quantified the pixels in a participation image using type-II fuzzy logic and a membership function for type-II extended intervals. When K-nearest neighbor and Euclidean distance metrics were used for sparse representation, the experimental analysis revealed a 10% increase in accuracy. According to Nguyen et al. [52], the human face is a passive biometric. Face images work well when combined with the individual's interaction, including blinking, nodding, and turning the face. The facial recognition system is an artificial intelligence system that identifies individuals through image patterns derived from the textures and shapes of their faces. Temperatures and wrinkles do not affect the visible imagery of facial biometrics. Yaddaden et al. [53] demonstrated the effectiveness of a facial recognition system built on a convolutional neural network architecture and equipped with an error detection module. The experiment used five benchmark facial expression datasets with promising results. For example, the accuracy was higher than 95%, and the number of false positives was cut by 20%.

2.3. User Perception Model

The Technology Acceptance Model (TAM) was adopted and developed to examine the use of system acceptance [54]. The principal keys of TAM influenced users' intention to use technology by assembling perceived usefulness and perceived ease of use. BioTAM was a new resolution for a biometric authentication system's technology acceptance model [55]. BioTAM proposed that factors, such as user interfaces, biometric enrollment or verification procedures, devices, and other auxiliary tools, were used to study the end-behavioral user's intention toward using a biometric system. The questionnaire was statistically evaluated based on confounding variables. Wang [56] extended a modified TAM to investigate financial biometric identification applications. The study suggested that perceived privacy and perceived trust were added as modified TAM variables for biometric identification, which includes the face, fingerprint, iris, and voice.

Additionally, TAM is not limited to the study of user perception. Ajzen and Fishbein [57] proposed the Theory for Reasoned Action (TRA) as a framework for forecasting and describing actions across a range of domains, including attitude, intention [58], and motivation. TRA is a very broad concept intended to describe essentially any aspect of human actions. To summarize, the proper determination of user perception is contingent upon the users' intention to use technology. Buabeng-Andoh [59] proposed a model for predicting students' intentions regarding mobile learning adaptation. A combination of TAM and TRA was used to ascertain students' intentions regarding m-learning usage in the classroom. Banga and Pillai [60] discussed the factors that should be considered. Biometric systems for mobile payments should include accuracy, capability, acceptability, cost-effectiveness, and hygiene factors. Behavioral biometrics measure how an activity was carried out rather than the outcome of the activity. For example, the login system is responsive to the speed with which a user enters a username and password. TAM and TRA were used in this study to establish a practical biometric relationship between six significant factors: perceived usefulness and ease of use, as well as users' trust and security, attitudes, intention to use, and actual system use.

3. Materials and Methods

This research employed the Internet of Things (IoT) and facial recognition to propose a student biometric recognition system for exam attendance. Comparing biometric technology to the conventional method enables the replacement of student identification cards with face recognition technology in examination rooms. Creating a fake student identification card is simple. Each semester, students are subject to traditional verification using student identification cards. During the midterm exam for the spring semester of 2020, a sampling group of 161 first-year students was subjected to the biometric examination attendance system. Students were separated into four classes for digital intelligence and software science. The unimodal biometric recognition system was used in a single examination session to examine student perception. The multimodal biometric recognition system was also tested on the same test subjects during a later examination session.

3.1. Proposed Face Recognition Framework

In order to develop a prototype software system for exam attendance, our framework outlined the specifics of biometric student recognition. The extension of the previous framework in this study made possible the deployment and investigation of a student examination attendance system based on the Internet of Things (IoT) in its present state for unimodal biometric recognition with a single camera and multimodal biometric recognition with two cameras, as illustrated in Figure 1. The student examination attendance system ran on a Raspberry Pi 4 with 8GB of RAM and was linked to cameras and a monitor displayed in front of the exam room. Our experiment utilized OpenCV and Python 3.9 to train and test data. There were two primary system users (proctors and students). Teachers and other staff members were assigned as proctors to monitor student examination attendance. A proctor must authenticate with the system and enter the examination session to gain access.

Figure 2a shows the home page of our examination attendance system. As depicted in Figure 2b, each examination session includes information about the examination, including the date, subject, time, student list, and proctors. Before entering the examination session, students must register their faces and personal information in the system. The real-time database system contained the facial templates of students from which the OpenCV face recognition technology-trained system. Prior to entering the examination room, when a student approaches, the proctor uses the verification mode to identify the student's face. The student examination attendance system can detect students' faces, validate their identity accuracy, and report on a student's rate of accurate face recognition.

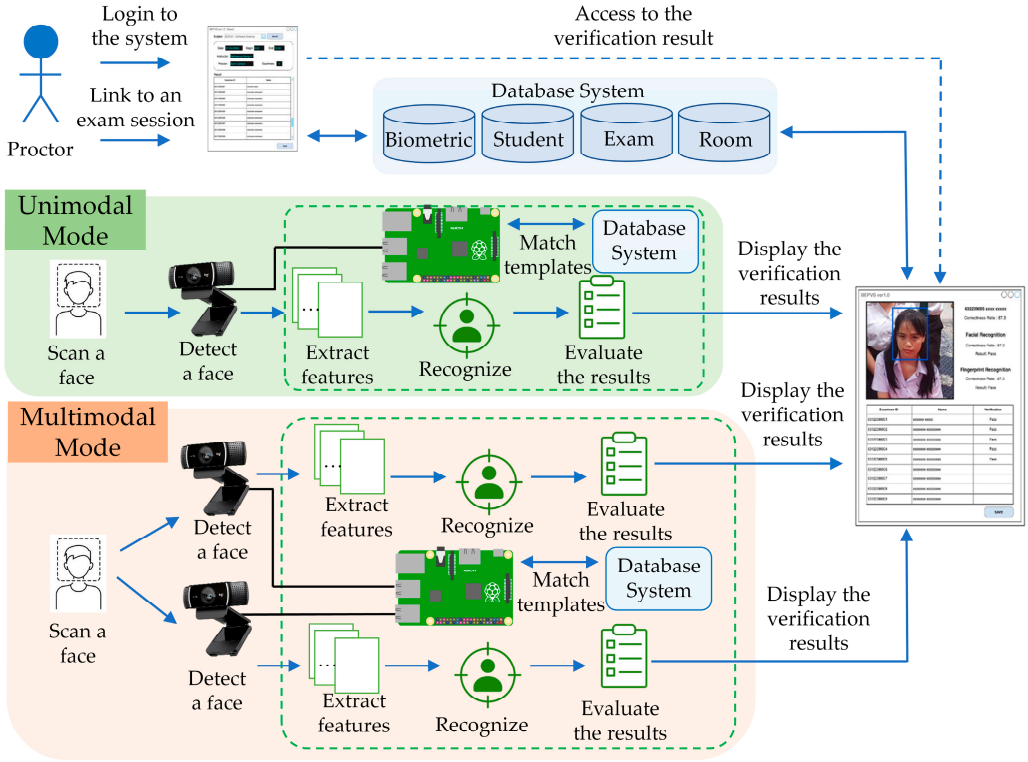

Figure 1. Proposed student biometric recognition framework for examination attendance system.

In addition, as shown in Figure 2c, a single camera was used to identify and verify the student's face, a technique known as unimodal biometric recognition. Multimodal biometric recognition requires two cameras to identify and verify the student's face; the system then calculates the average matching score, as shown in Figure 2d. Students gain practical experience with a cutting-edge face recognition system. The educational repercussion of biometric technology is the most challenging to implement. Therefore, in this study, the authors compared how people planned to make decisions based on how they used and satisfied biometric technologies in education.

3.2. Instrument

The questionnaire was separated into two major sections. The primary section examined the respondents' demographic characteristics (age and gender) in our experimental study. The secondary section of the study examined student perceptions using the Technology Acceptance Modal (TAM) and Theory for Reasoned Action (TRA). The following five components were assigned to students: perceived usefulness (4 items), perceived ease of use (6 items), trust and security (5 items), attitude (4 items), behavioral intention to use (3 items), and actual system use (2 items). The survey respondents evaluated every item on a 5-point Likert scale, varying from 1 (strongly disagree) to 5 (strongly agree). This study included a total of twenty-three items. After the multimodal biometric verification was completed and the students completed their examinations, the participants were surveyed.

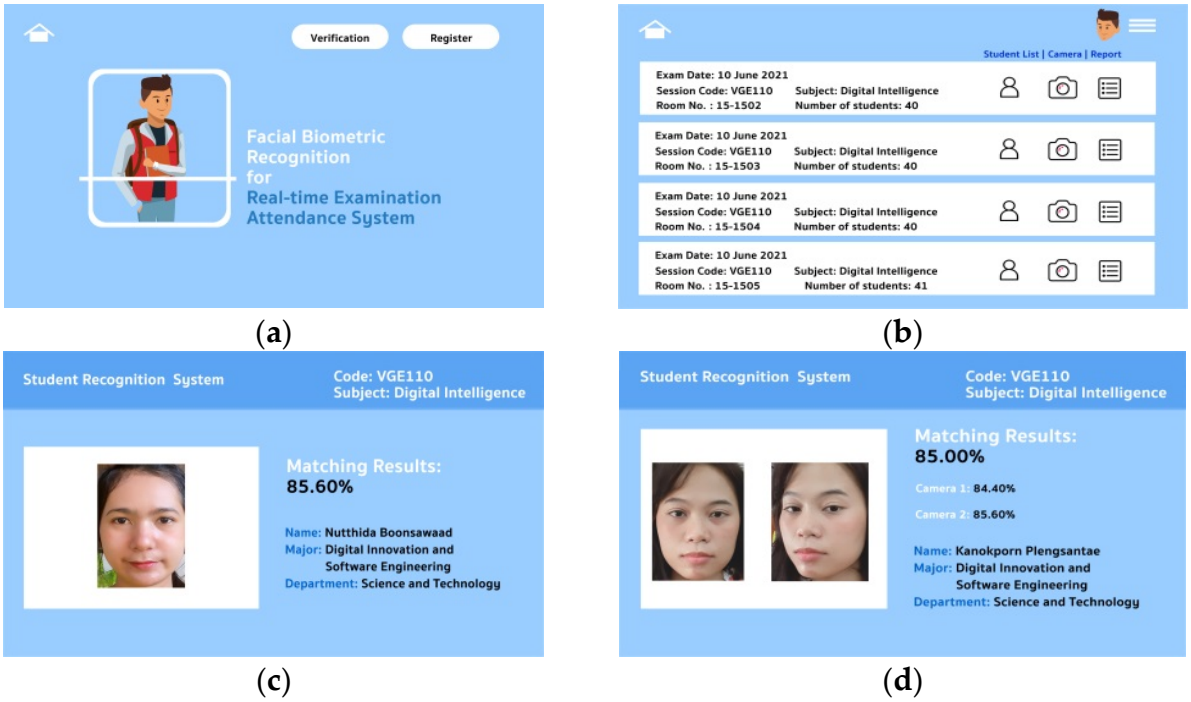

Figure 2. Samples of biometric recognition interfaces for examination attendance system: (**a**) the home page of the system; (**b**) examination information sessions; (**c**) the screen of a unimodal recognition result; (**d**) the screen of a multimodal recognition results.

3.3. Instrument Validation and Analysis

This study's methodology was quantitative. A questionnaire was initially developed to elicit student perceptions and test hypotheses. Perceptions and hypotheses were developed in accordance with DeVellis and Thorpe's guidelines [61]. The proposed method generated a list of components to evaluate, defined the items within each element, specified the measurement scale, and validated the model's reliability and validity. Cronbach's alpha [62], compound reliability (CR), convergent validity (AVE), and item analysis were used as indicators in the final step. SPSS was used to perform Exploratory Factor Analysis (EFA) and construct validity checks on the biometric recognition processes. Additionally, using the constructs' covariance matrix, the Confirmatory Factor Analysis (CFA) designed on Structural Equation Modeling (SEM) was assessed. Following that, one hundred and sixty-one students were asked to assess the end-user perception of facial biometric recognition with a 100% of response rate.

In addition, all study participants were given informed consent to ensure their contribution was anonymized and voluntary. The information presented was especially for the purpose of research. Justice, respect, autonomy, compassion, and confidentiality were all guaranteed as ethical values.

3.4. Hypotheses

Figure 3 depicts the proposed hypothesis model based on TAM and TRA. The authors labeled the following hypothesis about student perceptions of biometric recognition for examination attendance: Perceived ease of use has a positive effect on perceived usefulness (H1); trust and security have a positive effect on attitude (H2); perceived usefulness has a positive effect on behavioral intention to use (H3); perceived ease of use has a positive effect on behavioral intention to use (H4); attitude has a positive effect on behavioral intention to use (H5); trust and security have a positive effect on behavioral intention to use (H6); and behavioral intention to use has a positive effect on actual system use (H8).

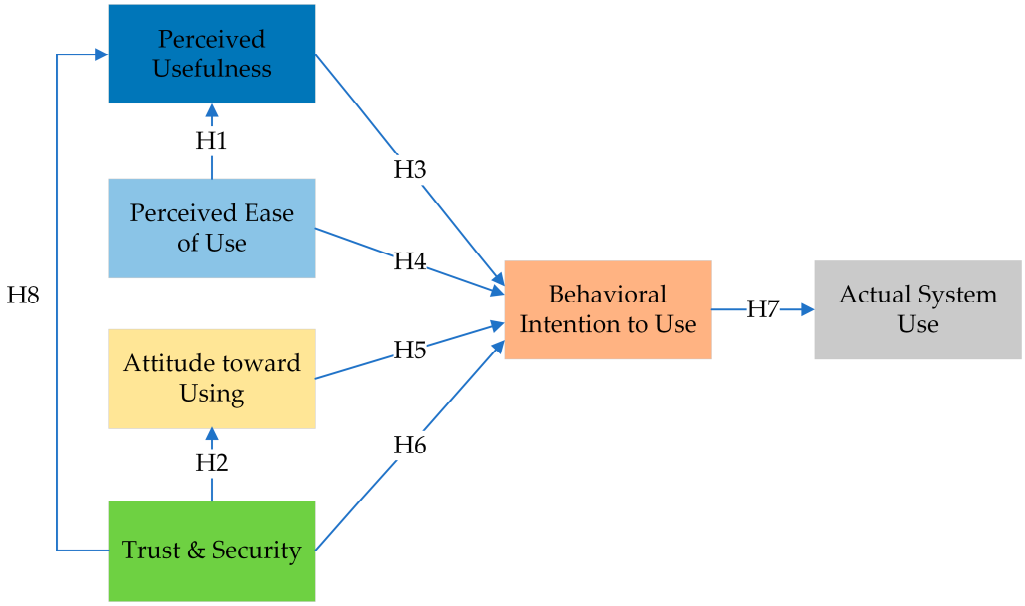

Figure 3. Proposed hypothesis model.

3.5. Evaluation Design and Data Collection

Using the extended TAM model, this study investigated the factors influencing the acceptance of face recognition technologies. The SEM model validated and verified the proposed hypothesis [63]. According to [64–66], at least 200 participants were required for an acceptable SEM analysis or at least 5 cases per parameter for a simple SEM model. Since this study contained 24 observable variables, the minimum sample size was 24 × 5 = 120. Students were used to selecting 161 user samples voluntarily. This research did not involve hazardous chemicals, equipment, procedures, animal or human testing, or the use of animals. However, this study obtained informed consent from individuals before collecting biometric data using and handling their facial biometric data. A consent form for facial biometric collection outlined the introduction, purpose, use, handling, rights, and contact information. As a part of the ethical research, the authors respected the participants' voluntariness, anonymity, freedom, and confidentiality. Students could make an informed decision about providing consent and then accept an individual's consent signature for collecting and using their facial biometric data.

3.6. Biometric Data Management

The management of collected biometric data is a crucial aspect of protecting the privacy and safety of individuals. Biometric data must be stored securely, using encryption and other security measures to prevent unauthorized access or data breaches. Administrators and authorized personnel must be the only ones with access to biometric data. Biometric information should be kept only as long as necessary for the purpose for which it was collected and should not be shared with third parties. When the data are no longer required, they should be deleted or anonymized to protect the privacy of individuals in accordance with all applicable laws and regulations, data protection and privacy laws, and to ensure that individuals have the right to access, correct, or delete their personal information. This study was conducted in accordance with all the applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and Thailand's Personal Data Protection Act BE 2562. (PDPA).

4. Result and Discussion

Experiments were used to determine student perceptions of facial recognition for the examination attendance system, followed by a survey of 161 students to collect the data.

Students were exposed to the conventional method of identifying students with a student card, unimodal face recognition with a single camera, and multimodal face recognition with two cameras. Each participant completed a survey questionnaire at the conclusion of the three examination sessions. This section provides a summary of the study of the perceptions performed.

4.1. Desctiptive Statistic

Males were the majority of participants (57.10%). The ages were 19 years old (33.50%). Table 1 shows the student demographic information in this research. The numerical assessment results for each aspect variable in the survey are shown in Table 2. In all the aspects, the three variables with the highest mean score (in order) were "The student identification using biometric recognition is reliable" (4.04). "The biometric recognition would be physically invasive" and "I would trust the face recognition system" had the same high mean score (4.01). On the other hand, the variables with the lowest mean score (in order) were "The biometric recognition does not require much effort to identify me." (2.74), "The biometric recognition is easy to use" (2.80), and "I think the face recognition for examination attendance is more useful than the traditional method (student card)" (2.84).

Table 1. Student demographic information.

Item	Description	Sample	%
Gender	Male	92	57.10
	Female	69	42.90
Age	18	107	66.50
	19	54	33.50
Education level	Freshman student	161	100.00

Table 2. Mean and SD of constructs and items.

Construct	Description	Mean	SD
Perceived Usefulness (PU) [54,67,68]	PU1: I think face recognition for examination attendance is more useful than the traditional method (student card).	2.84	0.766
	PU2: I think multimodal face recognition for examination attendance is more useful than unimodal face recognition.	3.19	0.818
	PU3. The biometric technology is useful for my daily studies.	2.85	0.823
	PU4. The biometric technology helps me increase my productivity during my class.	2.94	0.834
Perceived Ease of Use (PEU) [54,69]	PEU1: I think face recognition for examination attendance is easier than the traditional method (student card).	2.85	0.654
	PEU2: I think multimodal face recognition for examination attendance is easier than the unimodal face recognition.	3.12	0.714
	PEU3: The biometric recognition is easy to use.	2.80	0.614
	PEU4: One of the reasons this system is useful is because of its ease of use.	2.87	0.603
	PEU5: The student recognition is simpler to identify than the traditional method.	2.92	0.642
	PEU6: Biometric recognition does not require much effort to identify myself.	2.74	0.657
Trust and Security (TS) [56,70]	TS1: The biometric recognition would be physically invasive.	4.01	0.680
	TS2: I would trust the face recognition system.	4.01	0.652
	TS3: Student identification using biometric recognition is reliable.	4.04	0.660
	TS4: The system can identify me correctly.	3.99	0.707
	TS5: The system has high recognition accuracy.	3.96	0.660

Table 2. *Cont.*

Construct	Description	Mean	SD
Attitude (ATT) [57]	ATT1: I feel that using biometric technology better than I expect.	3.89	0.707
	ATT2: Most of my expectations of using face recognition system were confirmed.	3.89	0.689
	ATT3: I feel pretty much use biometric technology in my study.	3.74	0.712
	ATT4: I can trust the biometric recognition system because of high security.	3.77	0.700
Behavioral Intention to Use (BIU) [57,71]	BIU1: I prefer biometric recognition for examination attendance than the traditional method.	3.20	0.593
	BIU2: I will use facial biometric recognition when I have an examination attendance.	3.59	0.586
	BIU3: I hope that biometric technology can be applied in university as soon as possible.	3.52	0.571
Actual System Use (ASU) [72]	ASU1: I would use a face recognition system for examination attendance.	3.70	0.537
	ASU2: I would recommend my university use a face recognition system for student identification in all authentication areas.	3.78	0.559

4.2. Reliability Test

Confirmatory Factor Analysis (CFA) was utilized to validate the reliability test. Hair et al. [73] defined construct validity so that the degree to which a collection of observed variables correctly signified the theoretically quantifiable latent variables. Additionally, they assessed the convergent and discriminant validity of postulated criteria. The findings confirm a total of 23 items. As Bagozzi and Yi [74] suggested, no items were removed because the standardized item loading exceeded 0.5. The factor loadings were more significant than 0.50 and ranged from 0.606 to 0.992, indicating their high reliability. Additionally, the instrument's reliability, consistency, and validity were evaluated. As suggested, the composite reliability (CR) value was greater than 0.70 and fell between 0.773 and 1.000 [75]. The average extracted variance (AVE) was greater than 0.50 and ranged between 0.533 and 0.999, indicating that the data are highly reliable. Cronbach's alpha coefficient values were greater than 0.70 and ranged between 0.774 and 0.932, as Cronbach [62] suggested. As shown in Table 3, all achieved and recommended measures and values demonstrate convergent validity acceptance (CR > 0.70 and AVE > 0.50).

Table 3. Convergent validity and reliability of constructs.

Construct	Item	Factor Loadings >0.50	CR >0.70	AVE >0.50	Cronbach's Alpha >0.70
Perceived Usefulness (PU)	PU1	0.799	0.850	0.589	0.846
	PU2	0.915			
	PU3	0.818			
	PU4	0.759			
Perceived Ease of Use (PEU)	PEU1	0.622	0.864	0.520	0.859
	PEU2	0.750			
	PEU3	0.856			
	PEU4	0.781			
	PEU5	0.800			
	PEU6	0.789			
Trust and Security (TS)	TS1	0.790	0.932	0.735	0.932
	TS2	0.869			
	TS3	0.959			
	TS4	0.913			
	TS5	0.861			

Table 3. *Cont.*

Construct	Item	Factor Loadings >0.50	CR >0.70	AVE >0.50	Cronbach's Alpha >0.70
Attitude (ATT)	ATT1 ATT2 ATT3 ATT4	0.853 0.888 0.892 0.828	0.902	0.699	0.903
Behavioral Intention to Use (BIU)	BIU1 BIU2 BIU3	0.679 0.900 0.925	0.823	0.623	0.801
Actual System Use (ASU)	ASU1 ASU2	0.954 0.946	0.937	0.881	0.934

The discriminant's validity was established because the square root of each construct was more significant than their corresponding inter-construct correlation estimates, as illustrated in Table 4. Therefore, all of the constructs were tested for their reliability and validity, which also showed a significant level.

Table 4. Discriminant validity.

Construct	PU	PEU	TS	AT	BIU	ASU
PU	**0.767**					
PEU	−0.269 **	**0.721**				
TS	0.280 **	−0.059	**0.858**			
ATT	0.160 †	−0.108	0.480 ***	**0.836**		
BIU	0.224 *	−0.165 †	0.175 *	0.114	**0.789**	
ASU	0.042	−0.008	0.051	0.108	0.220 *	**0.939**

† $p < 0.100$, * $p < 0.050$, ** $p < 0.010$, *** $p < 0.001$.

4.3. Measurement Model Testing

According to Figure 4, the measurement model confirms that all six constructs (PU, PEU, TS, ATT, BIU, and ASU) are the primary factors in the study that were examined using the EFA model. The authors removed no items from the instrument to achieve the best fit for the measurement model because their regression weights were larger than the bare minimum acceptance measure of 0.60. To validate the measurement model, confirmatory factor analysis was used. The authors tested the model-fit determines against the model's advised fit indicators (x^2/df, GFI, RMSEA, RMR, NFI, CFI, IFI, and TLI) to validate the overall goodness of the fit index. The results show that all values are significantly greater than their relevant measures' (conventional least acceptance) quantities [73]. The model measurement of suitability indicators is shown in Table 5.

Table 5. Measurement of suitability indicators for the measurement model.

Model	x^2	*df*	x^2/df	GFI	RMSEA	RMR	NFI	CFI	IFI	TLI
Standards			$1 < x^2/df < 3$	≥0.90	≤0.08 < 0.1	≤0.08 < 0.1	≥0.90	≥0.90	≥0.90	≥0.90
Acquired	437.90	237	1.848	0.907	0.073	0.028	0.938	0.917	0.918	0.903

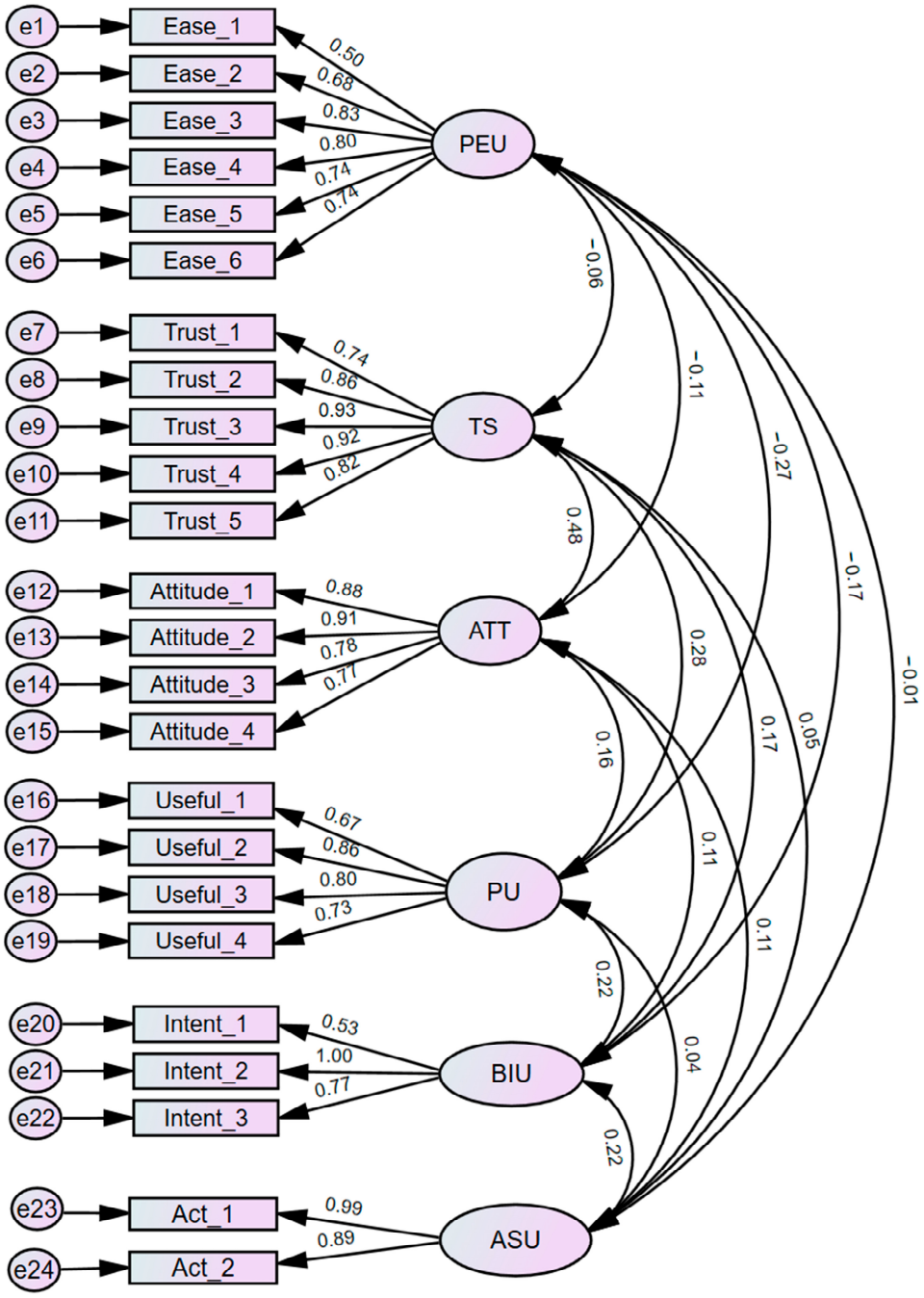

Figure 4. Measurement model of student perception toward biometric recognition.

4.4. Structural Model Estimation

As shown in Figure 5, our proposed exploration model was evaluated using SEM. Hair et al. [73] explained how exploratory and confirmatory factor analysis techniques could simultaneously examine multiple dependence relations. When the model's constructs have direct and indirect effects on one another, this analysis method is particularly useful. The initial step in interpreting SEM results is to examine the model-fit indicator, which demonstrates that the data perfectly fit the proposed model.

As shown in Table 6, the SEM model demonstrates that all fit indicators meet the bare minimum acceptable standards. Figure 5 depicts the path significances, coefficients, and variances justified for each affected variable.

Table 6. Measurement of suitability indicators for the revised measurement model.

Model	x^2	*df*	x^2/df	GFI	RMSEA	RMR	NFI	CFI	IFI	TLI
Criteria			$1 < x^2/df < 3$	≥0.90	≤0.08 < 0.1	≤0.08 < 0.1	≥0.90	≥0.90	≥0.90	≥0.90
Obtained	7.776	6	1.296	0.984	0.043	0.008	0.940	0.996	0.996	0.996

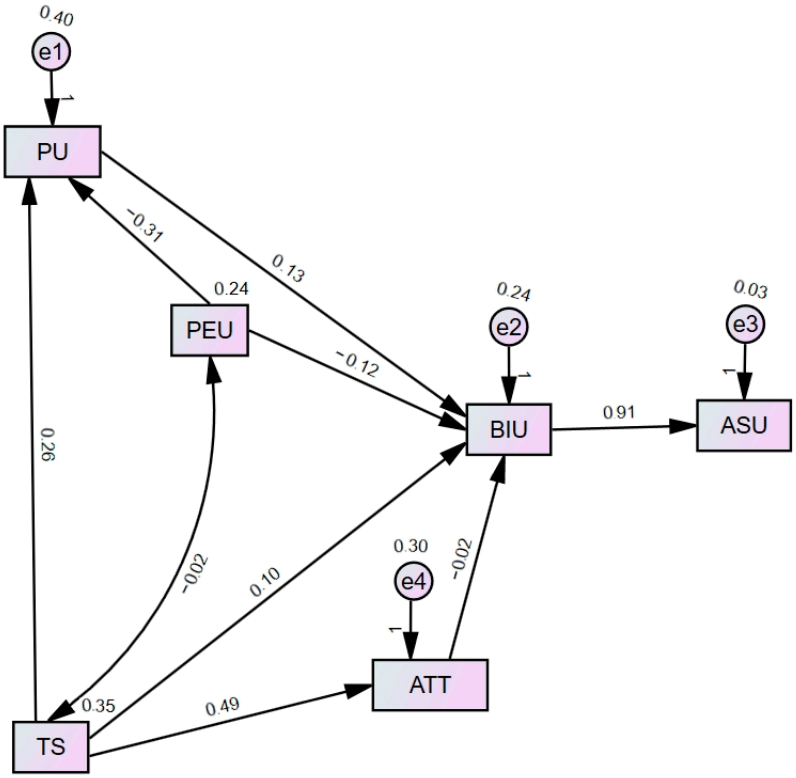

Figure 5. Revised measurement model of student perception toward biometric recognition.

4.5. Hypoteses Test Results

Overall, the results support five of the eight hypotheses tested. As shown in Table 7, the findings account for the following positive relationships: TS ($\beta = 0.469$, $p < 0.000$) has a highly significant positive impact on ATT, supporting hypothesis H2; PEU ($\beta = -0.288$, $p < 0.002$) and TS ($\beta = 0.230$, $p < 0.002$) have a highly significant positive impact on PU, supporting hypothesis H1 and H8; PU ($\beta = 0.169$, $p < 0.036$) has a significantly positive impact on BIU, supporting hypothesis H3, while PEU ($\beta = -0.117$, $p < 0.137$), ATT ($\beta = -0.024$, $p < 0.780$), and TS ($\beta = 0.115$, $p < 0.194$) do not have a positive result for BIU; and BIU ($\beta = 0.938$, $p < 0.000$) has a positive influence on ASU, supporting hypothesis H7. However, TS exerts the greatest influence on PU's decision to use facial recognition for the examination attendance system, confirming hypothesis H3.

4.6. Discussion

According to our findings from the first research question, perceived usefulness is significantly predicted by trust and security (H8) and perceived ease of use (H1). Our accuracy factor was indicated in our item questions under the trust and security construct. This study is consistent with Sidharta's, Priadana's, and Affandi's [76], and Norfolk's and O'Regan's [72] findings on trust and security based on biometric technology. They asserted that a strong correlation existed between accuracy and perceived usefulness. Kanak and Sogukpinar [55] discovered that perceived ease of use of biometric authentication systems had a significant relationship with perceived usefulness in a situational relationship. Our findings support the notion that students' experiences with biometric technology have a strong correlation with perceived ease of use and usefulness for identifying and verifying

examination attendance. Students expressed a concern that using a face recognition system would be more convenient than the traditional approach.

Table 7. Summary of results for hypotheses assessment.

Hypotheses	Relationship (Positive)	Value	*p*-Value	Results
H1	PEU → PU	−0.228	0.002 **	Accepted
H2	TS → ATT	0.469	0.000 ***	Accepted
H3	PU → BIU	0.169	0.036 **	Accepted
H4	PEU → BIU	−0.117	0.137	Rejected
H5	ATT → BIU	−0.024	0.780	Rejected
H6	TS → BIU	0.115	0.194	Rejected
H7	BIU → ASU	0.938	0.000 ***	Accepted
H8	TS → PU	0.230	0.002 **	Accepted

*** $p < 0.001$, ** $p < 0.05$.

In this study, a construct of trust and security (H2) had a positive effect on attitude. However, Norfolk and O'Regan [72] discovered an unexpected relationship between accuracy and attitude toward use. On the other hand, this study discovered that trust and security (H6) had no positive effect on behavioral intention to use. Our findings imply that students involved in biometric technology can be trusted to maintain a high level of security while minimizing identity fraud. For various reasons, students consider the employment of biometric technology as an intelligent tool for examination attendance.

The findings indicate that perceived usefulness (H3) positively affects behavioral intention to use. Additionally, behavioral intention (H7) was associated with a beneficial effect on actual system use, as previously mentioned [77,78]. This evidence demonstrates the numerous benefits of biometric technology for actual biometric recognition systems in universities. Surprisingly, the results show that students' perceptions of perceived ease of use (H4) and attitude (H5) have no positive effect on their behavioral intention to use, which is supported by Norfolk and O'Regan [72].

The results of the second research question indicate that multimodal biometric recognition receives significantly more favorable ratings than unimodal biometric recognition. Student perceptions of perceived usefulness and perceived ease of use received the highest scores compared to other factors in the same constructs. According to Labayen et al. [79], students are positively affected by multimodal biometric recognition.

5. Conclusions

5.1. Theoretical Contributions

Biometric technology has several potential applications, including K-12 education, higher education, teacher education, and training. The empirical findings of this study demonstrate that the application of biometric technology can transform traditional examination approaches, challenge established approaches to biometric examination attendance, and enable exam aspects to improve security, reliability, and efficiency. Additionally, this study discovered that when conservative and biometric identifications were compared, they resulted in significantly different experience outcomes. Students preferred the face recognition system over the conservative approach for examination attendance, which is attributed to concerns about trust and security. Biometric recognition enables students to easily and accurately identify and verify themselves. The results produced the following conclusions as the study's primary contribution:

- The framework for biometric examination attendance recognition was proposed and a prototype application was developed. The study demonstrates the educational biometric recognition framework's practical outcomes, emphasizing unimodal and

multimodal face recognition for first-year undergraduate students. Additionally, the proposed architecture and system provide real-time face recognition of students for examination attendance, information, and accuracy rates of face recognition.

- To investigate students' actual system use, this research adopted a Model of Technology Acceptance (TAM) and a Theory of Reasoned Action (TRA). The educational biometric recognition factors considered student perceptions of ease of use, usefulness, attitude, trust, and security.
- Trust and security are significantly related to IoT-based face recognition for class attendance because they are essential to protect individuals' rights and privacy, ensure compliance with laws and regulations, maintain the integrity and security of the system, and build trust with individuals.
- In comparison to traditional and biometric recognition for examination attendance, multimodal face recognition is significantly more useful than unimodal face recognition.

5.2. Practical Implications

The biometric recognition framework of the examination attendance system can be used to enhance the proctoring approach for student identification and verification in elementary, secondary, and higher education. This study can provide new perspectives and techniques for administrators, educators, and instructors with perception into an innovative biometric recognition system for educational examinations and enhance security, reliability, and efficiency.

At present, users increasingly accept biometric technologies in their daily lives, owing to the convenience and speed with which they can be identified and verified. The authors exclusively focused on face recognition for examination attendance in this study. Biometric recognition can track students' movement between areas and eliminate the need for identification in various other ways, such as no student cards. Since 2019, due to the spread of coronavirus disease, universities worldwide have adopted distance education, considered the best solution for social isolation, less contact, and disease prevention.

Several steps can be taken to prevent errors in recognizing a specific image of a student and any significant changes to their appearance in facial recognition systems used for class attendance. One potential solution is to periodically update the stored images of students in the system to reflect any changes in their appearance. This approach could involve regularly scheduled re-enrollments or updates to the system, where students would be required to provide updated images of their current appearance. Another solution is to use more robust multimodal facial recognition systems that use multiple modalities, such as thermal, depth, and 3D images, to improve the system's accuracy and make it more resistant to changes in appearance. Another approach could be to use a combination of facial recognition technology with other forms of identification, such as a student ID card, a password, or a PIN. To ensure that even if the facial recognition system cannot recognize a student due to changes in their appearance, they will still be able to prove their identity and access the class. It is also important to communicate with students about the potential impact of changes in their appearance on the system's accuracy and to provide guidance on how they can update their data in the system in case of significant changes.

5.3. Limitations and Future Work

The limited use of facial recognition technology raises ethical concerns from different perspectives, such as privacy, bias, transparency, surveillance, discrimination, misuse of data, and lack of proper regulations. These ethical concerns must be carefully considered and addressed to ensure that the technology is used responsibly and ethically that respects individuals' rights and dignity. It is important to have clear guidelines, regulations, and oversight mechanisms in place to govern the use of facial recognition technology to minimize any negative impacts.

Future research on IoT-based face recognition for class attendance systems should detail potential areas that can be undertaken to improve accuracy and performance. These

include using multimodal systems, deep learning algorithms, data privacy and security, addressing biases in the system, integration with other technologies, and real-time monitoring. Researchers and educators could elucidate additional factors influencing individuals' preferences for biometric recognition in their examination approaches. The university may announce biometric recognition for student examination attendance without obtaining permission. However, university administrators would be sensible to obtain consent from students and research their perceptions before biometric recognition is used to replace traditional processes. Thus, researchers and educators could further elucidate the factors influencing individuals' preference for biometric recognition in their examination approaches. Moreover, student biometric recognition can integrate online learning and assessment systems, ensuring that students remain focused during their study sessions. These trends are likely to persist in subsequent research.

Author Contributions: Conceptualization, P.N. and M.R.; methodology, S.W.-I. and P.N.; software evaluation and modeling, S.W.-I.; validation, P.N., M.R., and S.W.-I.; formal analysis, P.N. and M.R.; investigation, S.W.-I.; resources, S.W.-I.; data curation, P.N., M.R., and S.W.-I.; writing—original draft preparation, M.R. and S.W.-I.; writing—review and editing, P.N. and M.R.; visualization, P.N., M.R., and S.W.-I.; supervision, P.N. and M.R.; project administration, P.N., M.R., and S.W.-I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study because this research does not involve hazardous chemicals, equipment, procedures, animal or human testing, or the use of animals and human as a subject experiment. Rangsit University granted ethical approval, and the actual protocol number is RSU-GRAD 537/2561.

Informed Consent Statement: Informed consent was obtained from all study participants. Participants were at least 18 years old. As part of the ethical research, the authors respect the voluntariness, anonymity, freedom, and confidentiality of the participants. The provided data contained no information that could be used to determine the participants' identities.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Constantinou, C.; Wijnen-Meijer, M. Student evaluations of teaching and the development of a comprehensive measure of teaching effectiveness for medical schools. *BMC Med. Educ.* **2022**, *22*, 113. [CrossRef] [PubMed]
2. Banwarith, R.; Basuhail, A.; Fattouh, A.; Gamalel-Din, S. E-exam cheating detection system. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 176–181.
3. Vučković, D.; Peković, S.; Blečić, M.; Đoković, R. Attitudes towards cheating behavior during assessing students' performance: Student and teacher perspectives. *Int. J. Educ. Integr.* **2020**, *16*, 13. [CrossRef]
4. Roshan, A.S.; Gurbaz, M.Q.; Rahmani, S. The effects of large classes on English language teaching. *Integr. J. Res. Arts Humanit.* **2022**, *2*, 38–41. [CrossRef]
5. Lee, J.W. Impact of proctoring environments on student performance: Online vs offline proctored exams. *J. Asian Financ. Econ. Bus.* **2020**, *7*, 653–660. [CrossRef]
6. Anu, V.; Walia, G.; Bradshaw, G. Incorporating human error education into software engineering courses via error-based inspections. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, Seattle, WA, USA, 8–11 March 2017; pp. 39–44. [CrossRef]
7. Abass, O.A.; Olajide, S.A.; Samuel, B.O. Development of web-based examination system using open-source programming model. *Turk. Online J. Distance Educ.* **2017**, *18*, 30–42. [CrossRef]
8. Hameed, M.R.; Abdullatif, F.A. Online examination system. *Int. Adv. Res. J. Sci. Eng. Technol.* **2017**, *4*, 106–110. [CrossRef]
9. Hamid, R.A.; Mokhtar, U.A.; Yusof, M.; Warland, A. Electronic records management in schools: The case study of school examination analysis system. *J. Pengur.* **2020**, *57*, 1–13. [CrossRef]
10. Rukhiran, M.; Napasorn, P.; Netinant, P. Adoption of environmental information chatbot services based on the internet of educational things in smart schools: Structural equation modeling approach. *Sustainability* **2022**, *14*, 15621. [CrossRef]
11. Divya, H.; Nandhini, S.; Shobana, S.; Sujithra, M. Examination management system. *Int. J. Adv. Res. Publ.* **2021**, *9*, 920–923. [CrossRef]

12. Rukhiran, M.; Pukdesree, S.; Netinant, P. Biometric cloud services for web-based examinations: An empirical approach. *Int. J. Inf. Technol.* **2022**, *17*, 22. [CrossRef]
13. Shamsi, S.V.; Andrews, J.V. A survey paper on fingerprint recognition and cross matching. *Int. J. Res. Appl. Sci. Eng. Technol.* **2019**, *7*, 573–575. [CrossRef]
14. Kortli, Y.; Jridi, M.; Falou, A.A.; Atri, M. Face recognition systems: A survey. *Sensors* **2020**, *20*, 342. [CrossRef]
15. Raju, A.S.; Udayashankara, V. A survey on unimodal, multimodal biometrics and its fusion techniques. *Int. J. Eng. Technol.* **2018**, *7*, 689–695. [CrossRef]
16. Rukhiran, M.; Netinant, P. A practical model from multidimensional layering: Personal finance information framework using mobile software interface operations. *J. Inf. Commun. Technol.* **2020**, *19*, 321–349. [CrossRef]
17. Poria, S.; Cambria, E.; Bajpai, R.; Hussain, A. A review of affective computing: From unimodal analysis to multimodal fusion. *Inf. Fusion* **2017**, *37*, 98–125. [CrossRef]
18. Singh, M.; Singh, R.; Ross, A. A comprehensive overview of biometric fusion. *Inf. Fusion* **2019**, *52*, 187–205. [CrossRef]
19. Zainal, I.; Sidek, K.A.; Gunawan, T.S.; Mansor, H.; Kartiwi, M. Design and development of portable classroom attendance system based on Arduino and fingerprint Biometric. In Proceedings of the 5th International Conference on Information and Communication Technology for The Muslim World, Sarawak, Malaysia, 17–19 November 2014. [CrossRef]
20. Zainal, N.I.; Sidek, K.A.; Gunawan, T.S. Portable anti forgery recognition for attendance system using fingerprint based biometric. *ARPN J. Eng. Appl. Sci.* **2016**, *11*, 396–403.
21. Fenu, G.; Marras, M.; Boratto, L. A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognit. Lett.* **2018**, *113*, 83–92. [CrossRef]
22. Mehta, P.; Tomar, P. An efficient attendance management system based on face recognition using Matlab and Raspberry Pi 2. *Int. J. Eng. Res. Technol.* **2016**, *3*, 71–78.
23. Sayeed, S.; Hossen, J.; Kalaiarasi, S.; Vaithiyashankar, J.; Yusof, I.; Samraj, A. Real-time face recognition for attendance monitoring system. *J. Theor. Appl. Inf. Technol.* **2017**, *95*, 24–30.
24. Traore, I.; Nakkabi, Y.; Saad, S.; Sayed, B.; Ardigo, J.D.; Quinan, P.M. *Ensuring Online Exam Integrity through Continuous Biometric Authentication*; Springer: New York, NY, USA, 2017; pp. 73–81. [CrossRef]
25. Ye, M.; Shen, J.; Lin, G.; Xiang, T.; Shao, L.; Hoi, S.C. Deep learning for person re-identification: A survey and outlook. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *44*, 2872–2893. [CrossRef] [PubMed]
26. Yusof, Y.M.; Nasir, M.M.; Othman, K.A.; Suliman, S.I.; Shahbudin, S.; Mohamad, R. Real-time internet-based attendance using face recognition system. *Int. J. Eng. Technol.* **2018**, *7*, 174–178. [CrossRef]
27. Khan, R.U.; Wee, V.C.; Lui, V.W.; UlHaq, M.I.; Khan, Y.; Barawi, M.H. Mobile barcode based examination attendance system. *Int. J. Eng. Technol.* **2018**, *7*, 49–54. [CrossRef]
28. Rahni, A.A.; Zainal, N.; Adna, M.Z.; Othman, N.E.; Bukhori, M.F. Development of the online student attendance monitoring system (SAMS™) based on QR-codes and mobile devices. *J. Eng. Sci. Technol.* **2015**, *10*, 28–40.
29. Mohandes, M.A. Class attendance management system using NFC mobile devices. *Intell. Autom. Soft Comput.* **2016**, *23*, 251–259. [CrossRef]
30. Bhalla, V.; Singla, T.; Gahlot, A.; Gupta, V. Bluetooth based attendance management system. *Int. J. Innov. Eng. Technol.* **2013**, *3*, 227–233.
31. Rjeib, H.D.; Ali, N.S.; Farawn, A.A.; Al-Sadawi, B.; Alsharqi, H. Attendance and information system using RFID and web-based application for academic sector. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 266–274. [CrossRef]
32. Taileb, M. Design and implementation of RFID and fingerprint-based student verification system design and implementation of RFID and fingerprint-based student verification system. *Int. J. Recent. Technol. Eng.* **2020**, *8*, 2084–2092. [CrossRef]
33. Ahmed, I.B.; Mohamed, M.A.; Noma, A.M. A framework for secure online exam using biometric fingerprint and steganography techniques. *Int. J. Eng. Technol.* **2018**, *7*, 32–35. [CrossRef]
34. Emmanuel, E.; Okonkwo, T. A biometric authentication approach to examination conduct in Nigerian universities. *Int. J. Innov. Res. Technol. Sci. Eng.* **2019**, *8*, 2176–2182. [CrossRef]
35. Mir, G.M.; Balkhi, A.; Lala, N.A.; Sofi, N.A.; Kirmani, M.; Mir, I.A.; Hamid, H.A. The benefits of implementation of biometric attendance system. *Oriental J. Comput. Sci. Technol.* **2018**, *11*, 50–54. [CrossRef]
36. Awojide, S.; Awe, O.S.; Babatope, T.S. Biometric fingerprint system using an online based pattern recognition for candidate's authentication in Nigeria institution examinations. The Design Perspective. *Int. J. Sci. Eng.* **2018**, *9*, 1680–1694. [CrossRef]
37. Jain, T.; Tomar, U.; Arora, U.; Jain, S. IoT based biometric attendance system. *J. Electr. Eng. Technol.* **2020**, *11*, 156–161.
38. Sunaryono, D.; Siswantoro, J.; Anggoro, R. An android-based course attendance system using face recognition. *J. King Saud Univ.—Comput. Inf. Sci.* **2021**, *33*, 304–312. [CrossRef]
39. Wong-In, S.; Netinant, P. Designing an examinee personal verification system using biometric technology. *J. Curr. Sci. Tecnnol.* **2018**, *8*, 75–86. [CrossRef]
40. Ahmed, A.A. Future effects and impacts of biometrics integrations on everyday living. *Al-Mustansiriyah J. Sci.* **2019**, *29*, 139–144. [CrossRef]
41. Mahfouz, A.; Mahmoud, T.M.; Eldin, S.A. A survey on behavioral biometric authentication on smartphones. *J. Inf. Secur. Appl.* **2017**, *37*, 28–37. [CrossRef]

42. Gawande, U.; Golhar, Y. Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques. *Int. J. Biom.* **2018**, *10*, 142–175. [CrossRef]
43. Walia, G.S.; Singh, T.; Singh, K.; Verma, N. Robust multimodal biometric system based on optimal score level fusion model. *Expert Syst. Appl.* **2019**, *116*, 364–376. [CrossRef]
44. Yang, W.; Wang, S.; Hu, J.; Guanglou, Z.; Valli, C. A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognit.* **2018**, *78*, 242–251. [CrossRef]
45. Ammour, B.; Boubchir, L.; Bouden, T.; Ramdani, M. Face–Iris multimodal biometric identification system. *Electronics* **2020**, *9*, 85. [CrossRef]
46. Gunasekaran, K.; Jayamani, R.; Ramasamy, P. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. *Automatika* **2019**, *60*, 253–265. [CrossRef]
47. Zhao, Y.; Xu, J.; Wu, J.; Hao, J.; Qian, H. Enhancing camera-based multimodal indoor localization with device-free movement measurement using WiFi. *IEEE Internet Things J.* **2020**, *7*, 1024–1038. [CrossRef]
48. Chen, Y.; Yang, J.; Wang, C.; Park, D. Variational Bayesian extreme learning machine. *Neural Comput. Appl.* **2014**, *27*, 185–196. [CrossRef]
49. Gomez-Barrero, M.; Maiorana, E.; Galbally, J.; Campisi, P.; Fierrez, J. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognit.* **2017**, *67*, 149–163. [CrossRef]
50. Dass, S.; Sadrulhuda, M.Q.; Pasha, N.N.; Nayan, N.; Nayak, J.S. Real time face recognition using Raspberry Pi. *Int. J. Comput. Appl.* **2020**, *176*, 1–4. [CrossRef]
51. Yadav, S.; Vishwakarma, V.P. Extended interval type-II and kernel based sparse representation method for face recognition. *Expert Syst. Appl.* **2019**, *116*, 265–274. [CrossRef]
52. Nguyen, K.; Fookes, C.; Sridharan, S.; Tistarelli, M.; Nixon, M. Super-resolution for biometrics: A comprehensive survey. *Pattern Recogniti.* **2018**, *78*, 23–42. [CrossRef]
53. Yaddaden, Y.; Adda, M.; Bouzouane, A.; Gaboury, S.; Bouchard, B. User action and facial expression recognition for error detection system in an ambient assisted environment. *Expert Syst. Appl.* **2018**, *112*, 173–189. [CrossRef]
54. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–339. [CrossRef]
55. Kanak, A.; Sogukpinar, I. BioTAM: A technology acceptance model for biometric authentication systems. *IET Biom.* **2017**, *6*, 457–467. [CrossRef]
56. Wang, J.S. Exploring biometric identification in FinTech applications based on the modified TAM. *Financ. Innov.* **2021**, *7*, 42. [CrossRef]
57. Ajzen, I.; Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*; Prentice–Hall: Hoboken, NJ, USA, 1980.
58. Sheppard, B.H.; Hartwick, J.; Warshaw, P.R. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *J. Consum. Res.* **1988**, *15*, 325–343. [CrossRef]
59. Buabeng-Andoh, C. Predicting students' intention to adopt mobile learning: A combination of theory of reasoned action and technology acceptance model. *J. Res. Innov. Technol. Learn.* **2018**, *11*, 178–191. [CrossRef]
60. Banga, L.; Pillai, S. Impact of behavioural biometrics on mobile banking system. *J. Phys. Conf. Ser.* **2021**, *1964*, 062109. [CrossRef]
61. DeVellis, R.F.; Thorpe, C.T. *Scale Development: Theory and Applications*, 5th ed.; Sage Publications: Washington, DC, USA, 2021.
62. Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* **1951**, *16*, 297–334. [CrossRef]
63. Molnar, G.; Szuts, Z. The role of chatbot in formal education. In Proceedings of the 16th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia, 13–15 September 2018; pp. 197–200. [CrossRef]
64. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411–423. [CrossRef]
65. Bentler, P.M.; Chou, C.P. Practical issues in structural modeling. *Sociol. Methods Res.* **1987**, *16*, 78–117. [CrossRef]
66. Huang, Y.C. Integrated concepts of the UTAUT and TPB in virtual reality behavioral intention. *J. Retail. Consum. Serv.* **2023**, *70*, 103127. [CrossRef]
67. Rukhiran, M.; Netinant, P.; Elrad, T. Effecting of environmental conditions to accuracy rates of face recognition based on IoT solution. *J. Curr. Sci. Technol.* **2020**, *10*, 21–33. [CrossRef]
68. Song, B.K. E-portfolio implementation: Examining learners' perception of usefulness, self-directed learning process and value of learning. *Australas. J. Educ. Technol.* **2021**, *37*, 68–81. [CrossRef]
69. Acosta-Medina, K.K.; Torres-Barreto, M.L.; Cárdenas-Parga, A.F. Students' preference for the use of gamification in virtual learning environments. *Australas. J. Educ. Technol.* **2021**, *37*, 145–148. [CrossRef]
70. Hassanein, K.; Head, M. Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *Int. J. Hum. Comput.* **2007**, *65*, 689–708. [CrossRef]
71. Ngugi, B.; Kamis, A.; Tremaine, M. Intention to use biometric systems. *e-Serv. J.* **2011**, *7*, 20–46. [CrossRef]
72. Norfolk, L.; O'Regan, M. Biometric technologies at music festivals: An extended technology acceptance model. *J. Conv. Event Tour.* **2021**, *22*, 36–60. [CrossRef]
73. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*, 7th ed.; Prentice–Hall: Hoboken, NJ, USA, 2010.
74. Bagozzi, P.R.; Yi, Y. On the evaluation of structural equation models. *J. Acad. Mark. Sci.* **1964**, *16*, 74–94. [CrossRef]

75. Hair, J.F.; Hult, T.G.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publications: Washington, DC, USA, 2014.
76. Sidharta, I.; Priadana, S.; Affandi, A. Extending end-user computing satisfaction on academic information systems. *Indian J. Sci. Technol.* **2016**, *9*, 1–5. [CrossRef]
77. Ko, C.H. Exploring employees perceptions of biometric technology adoption in hotels. *Biotechnol. Indian J.* **2014**, *10*, 13242–13246.
78. Morosan, C. Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *J. Hosp. Tour. Res.* **2012**, *36*, 52–84. [CrossRef]
79. Labayen, M.; Vea, R.; Flórez, J.; Aginako, N.; Sierra, B. Online student authentication and proctoring system based on multimodal biometrics technology. *IEEE Access* **2021**, *9*, 72398–72411. [CrossRef]