

Received 26 January 2023, accepted 1 March 2023, date of publication 6 March 2023, date of current version 9 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3253024

RESEARCH ARTICLE

IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach

MEENAPA RUKHIRAN¹, SETHAPONG WONG-IN², AND PANITI NETINANT¹ 

¹Faculty of Social Technology, Rajamangala University of Technology Tawan-ok, Chanthaburi 22210, Thailand

²College of Digital Information Technology, Rangsit University, Lak Hok, Pathum Thani 12000, Thailand

Corresponding author: Paniti Netinant (paniti.n@rsu.ac.th)


ABSTRACT Traditional identity verification of students based on the human proctoring approach can cause a scam identity verification and ineffective processing time, particularly among vast groups of students. Most student identification cards outdated personal information. Several biometric recognition approaches have been proposed to strengthen students' identity verification. Most educational adoption technologies struggle with evaluation and validation techniques to ensure that biometric recognition systems are unsuitable for utilization and implementation for student identity verification. This study presents the internet of things to develop flexible biometric recognition systems and an approach to assess the quality of biometric systems for educational use by investigating the effectiveness of identity verification of various biometric recognition technologies compared to the traditional verification method. The unimodal, multimodal, and semi-multimodal biometric technologies were tested using the developed internet of things-base biometric recognition systems examined by applying the proposed quality metrics of scoring factors based on accuracy, error rate, processing time, and cost. Hundreds of undergraduate exam takers were a sample group. Key findings indicate that the designed and presented systems suitably attain identity verification of exam students using a unimodal biometric. The unimodal facial biometric system promises excellent support. A unimodal fingerprint biometric system ensures second excellent aid for student identity verification. However, multimodal and semi-multimodal biometric systems provide better accuracy with fewer handling times and higher costs. This study contributes significantly to the knowledge of utilizing biometric recognition for identity verification in smart educational applications.

INDEX TERMS Biometrics, recognition, identity, verification, Internet of Things, quality assessment.

I. INTRODUCTION

The internet of things (IoT) has ushered in a new era of connectedness, allowing numerous objects and systems to communicate and share data effortlessly [1]. This has resulted in various applications, including biometrics [2]. In recent years, considerable advances have been in the IoT research. Incorporating IoT technology into biometric recognition systems enables real-time monitoring and remote system access [3], thereby increasing system accessibility and flexibility. Moreover, IoT technology can improve the

accuracy and efficiency [4] of biometric recognition systems by enabling the integration of several biometric modalities, such as facial recognition and fingerprint identification [5]. These systems can leverage physiological or behavioral characteristics to identify individuals uniquely, lower the chance of cheating, and enhance educational security [6]. IoT-based biometric recognition systems can provide a more secure and convenient method of identifying and confirming students during classes and exams in the educational setting. However, these studies also identify key implementation issues, such as assuring the accuracy and dependability of the identification process, protecting students' privacy, and controlling implementation costs.

The associate editor coordinating the review of this manuscript and approving it for publication was Rebecca Strachan .

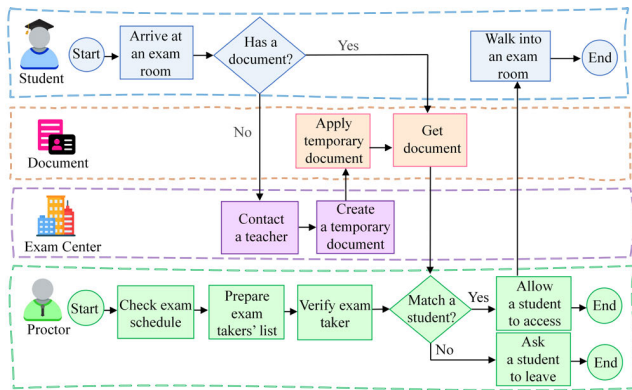


FIGURE 1. Traditional approach of examination takers' identification verification.

Moreover, information technology is a widely used in a variety of educational tasks. To become a smart school digital framework [7], numerous schools implement systems such as registration systems, and schedule management systems in their institutions [8]. However, the examination system is one of the most important factors in determining each student's academic achievement. Although many educational institutions have incorporated an electronic system into examination tasks, such as web-based examinations [9], online testing [10], and online examination systems [11], previous research has focused primarily on how to manage basic information and general tasks [12]. Student verification is the examination's most important and primary procedure for identifying the correct candidate for school, class, and examination authentications. Numerous educational institutions continue to use the conventional method, which includes personal documentation (e.g., student card and ID card), to verify exam takers. One of the most prominent issues with the conventional examination approach is that the proctor must be confident, and the student is the actual exam taker. No technological tools are available to the proctor to verify student identity. Even if a student's photograph appears on a personal document, it may not be possible to identify the actual exam taker using the photo. The student's personal document is also susceptible to lose or damage.

Checking a student's identification documents, such as a personal identification card, a student identification card, and a driver's license card is the standard procedure for confirming a student's eligibility to take an exam. Numerous complexities associated with this approach. At Valaya Rajabhat University in Thailand, for instance, the conventional approach to verifying student identity documents prior to entering an examination room is depicted in Fig. 1.

As shown in Fig. 1, verifying the identity of each exam candidate involves multiple steps and considerations. A student must present his/her document to a proctor prior to taking an exam. The proctor must then verify and match the information as well as the photo on the identification document to the specific student. There are multiple potential

causes for student verification, the first of which is how the proctor determines that the student is the actual exam taker. The student is granted access to the examination room if the student and the identification document match. The second scenario addresses the proctor's actions in the absence of an identification document. The proctor must contact the administrator of the registrar office at the university. The administrator must then provide the students with a one-day temporary identification card. In the third scenario, if the proctor suspects an exam taker, the student may request additional documentation or leave the examination room. Typically, proctors walk around the examination room to collect each student's signature. Consequently, this action may disturb the concentration of other test-takers during the exam.

An automated verification system is a contemporary method of identifying the correct individual. Several automated verification systems that employ biometric technologies have been proposed. The use of biometric technology in identity verification systems has several advantages over traditional identity verification. Access control using fingerprint recognition [13], face recognition to grant access [14], healthcare [15], citizen identification [16], [17], security systems [18], finance [19], airport [20], canteen management systems [21], visitor management systems [22] and parking management systems [23], [24], [25] have addressed the advantages of implementing biometric technologies. Biometric technology is a practical and useful alternative for verifying exam takers. Students were not required to provide or present identification during the examination. However, automated student verification requires extensive research into personal information technology verification design and development. Certain researchers have implemented a unimodal biometric technique as a face or voice-only biometric technology. Multiple biometric modalities are utilized in multimodal biometrics to ensure system quality and prevent biometric systems from having a single point of failure [26]. The biometric protocol gaps between unimodal and multimodal biometrics for identity verification in education are primarily concerned with the cost and accuracy of identity verification [27], [28]. The system evaluation is a crucial stage when standard objectives are evaluated to compare the new system's performance to those of the existing system [29]. There has never been a system that uses multimodal biometrics to verify the identity of students taking exams. Therefore, this research proposes an education-based biometric recognition system for identity verification services that focuses on a quality assessment metric.

This study makes three contributions to the scientific community as follows:

- The authors propose a system design and software development for examination management and biometric recognition systems using the IoT technology named biometric examinee personal verification system (BEPVS). The proposed system can support face and fingerprint recognition using many verification protocols.

- The authors compare the system quality of unimodal, semi-multimodal, and multimodal biometric examination verification systems. The quality measurement metrics for the proposed system are a pioneer investigation. The practical application's quality measurement metrics of biometric verification systems consisted of accuracy rate, error rate, response time, and cost.

- A relevant evaluation result for measuring the quality of each biometric verification protocol is analyzed to summarize the optimal biometric technology of IoT-based development.

The rest of the paper is organized as follows: Section II presents the literature review and theoretical background. The methodology used in this paper is deliberated in Section III. The experimental evaluation is described in Section IV. Section V reports the results and presents the discussion. Finally, Section VI summarizes the conclusions of this research.

II. LITERATURE REVIEW

This section summarizes the biometric technology principles, unimodal and multimodal biometric technologies, biometric verification systems in education, Internet of Things platforms for biometrics, and open-source computer vision (OpenCV) image processing for application development. The following section describes the works mentioned in this article.

A. BIOMETRIC TECHNOLOGY

Surveillance, identification, and access control are the three most prevalent biometric technology uses [30]. Numerous types of biometric technology-related research include algorithms, architecture, modalities, and applications. Physical biometrics focuses on human physical measurements such as the face, fingerprints, palm, retina, iris scans, and hand geometry. Behavior biometrics focuses on human operations, including voice, signature, gait, keystroke dynamics, and other activities (for instance, behavioral biometric authentication on smartphones [31]). Chemical biometrics are concerned with chemical identifiers, such as a person's scent. The biometric system can be classified as either unimodal or multimodal [32].

B. UNIMODAL BIOMETRIC TECHNOLOGY

The unimodal system uses a single biometric verification source, such as the face, iris, fingerprint, palm, or other distinctive human body parts.

Face recognition - The unimodal system employs a single biometric verification source, such as the face, iris, fingerprint, palm, or other distinctive human body parts. The human face is a well-known biometric characteristic utilized in various applications, including criminal identification, security systems, forensics, surveillance systems, credit card verification, etc. According to [33], the face is a passive biometric, and face images are used for effective development regardless of the individual's participation. The facial recognition system is a biometric artificial intelligence

system that identifies individuals by analyzing patterns of facial texture and shape patterns. Face biometrics primarily rely on visible imagery because temperature and eyewear have no effect on face verification.

Face recognition is a commonly used method for identifying or validating a person, and it is utilized in a variety of scientific disciplines. The three primary aspects of face biometrics are face recognition, feature extraction, and face matching. Recent studies [34], [35] focused on face recognition techniques and implemented real-time face recognition systems using Raspberry Pi, internet of things device. Yadav and Vishwakarma [36] proposed a novel, sophisticated, and efficient framework based on the interval type-II fuzzy membership with the kernel-based sparse method. The percentage of pixels contributing to the image was determined using interval type-II fuzzy logic, specifically an extended interval type-II membership function. Using the K nearest neighbor and Euclidean distance metric for sparse representation, the experimental analysis revealed a two to ten percent increase in accuracy over the current standard.

Kas et al. [37] presented a novel method for developing a feature descriptor called mixed neighborhood topology cross decoded patterns (MNTCDP) that can be combined across platforms to produce robust, computationally affordable, and simple solutions. MNTCDP depends on the pattern encoding scheme and neighborhood topology to produce a stable and discriminative face representation. Face alignment and detection supervised image classification, and the K-Nearest Neighbor classifier can improve precision rates. Experiments were conducted on the YALE, ORL, FERET, and AR datasets under various illumination conditions, and it was determined that the proposed MNTCDP descriptor exhibits outstanding performance. Yaddaden et al. [38] presented an efficient facial recognition system based on a Convolutional Neural Network architecture and radio-frequency identification (RFID) tags equipped with an error detection module. The experiment was conducted on five benchmark facial expression datasets and yielded promising results above 95 percent, with a false positive detection rate that was decreased by 20 percent and consistently improved results.

Fingerprint recognition - Fingerprint recognition is a well-established biometric technique. Hardware is used to collect and scan fingerprint data by the development system. Each fingerprint recognition technique utilizes a unique fingerprint data format. Awojide et al. [39] developed a biometric fingerprint system for candidate authentication in Nigeria Institution Examinations using online-based pattern recognition. Taileb [40] provided fingerprint recognition and RFID technology to verify students. Tatar [41] presented a novel algorithm for fingerprint recognition to illustrate research employing a novel algorithm. A finger vein recognition system has two primary phases: enrollment and verification, according to Wencheng et al. [42]. First, finger vein images are captured and enhanced for quality.

The extracted features are then saved as templates. In the second authentication phase, a vein sample is extracted from the user's finger for testing, followed by preprocessing and feature extraction techniques. The testing features were compared to the stored templates to display the verification result. In their study, Xi et al. [43] proposed a framework for a biometric system based on the finger vein modality, employing the discriminative binary code method and the PolyU and MLA databases. Moreover, they use supervised information and support vector machines (SVM) to make discriminative binary codes (DBC) more discriminatory and shorter. Various biometric systems, including Noma-Osaghae et al. [44], have granted door access using an iris and fingerprint verification.

C. MULTIMODAL BIOMETRIC TECHNOLOGY

Numerous researchers have examined multimodal biometric verification to improve the performance of the biometric recognition systems used to verify exam takers. Emmanuel and Ogadimma [45] created a multimodal cloud-based biometric service for online examinations. The proposed system uses face and voice recognition to access cloud services so students can access web-based examinations. Mir et al. [46] designed a novel framework for multimodal systems. The system utilized face and fingerprint images with block-based and feature-image matrices. The proposed method retrieved the semantic features of the middle layer of local biometric features, resulting in improved characterization capabilities, reduced dimension, and high accuracy rates for multimodal biometrics. They achieved highly stable and generalizable outcomes using the variational bayesian extreme learning machine (VBELM). The experimental results demonstrated greater precision, efficiency, and consistency in testing than conventional techniques.

Gomez-Barrero et al. [47] presented a method for developing a multibiometric system based on the homomorphic encryption method, with all encrypted database information. Multibiometric fusion utilized the characteristics, scores, and decision levels. On Biosecurity identification's online signature and fingerprint database, experiments were conducted. The system complied with the ISO/IEC 24744 requirements. Walia et al. [48] proposed a robust biometric system based on the optimal score-level fusion model and multiple identifiers. The system considered iris, finger vein, and fingerprint biometric modalities. The backtracking search optimization technique and proportional conflict redistribution rules were utilized in this study. Using multiple traits and a fusion approach to biometric scores produced better results than a single biometric. The multimodal system can be divided into the following four subcategories:

- **Multiple modalities:** the examination uses more than two types of biometric technology, such as face image and fingerprint verification. For instance, Ammour et al. [49] utilized the face and iris to identify a system user. Gunasekaran et al. [50] fused the face, fingerprint, and iris for the purpose of identifying individuals.

- **Multiple sensors:** the same inspection pattern is utilized with multiple sensors, such as images from two cameras. For instance, Zhao et al. [35] utilized two mobile phone cameras to detect the objects.

- **Multiple features:** multiple algorithms are used to extract images or data from the source [51], such as extracting fingerprint images using the first and second methods.

- **Multiple and repeated occurrences:** multiple biometric forms are used, such as left and right iris images for iris recognition, or the same biometrics are used multiple times. A brief overview of deep learning techniques for the re-identification of individuals. Fenu et al. [52] and various publications on multimodal biometrics presented a multibiometric system for continuous student authentication in e-learning platforms that uses face, voice, touch, mouse, and keystroke verification to authenticate students for e-learning. Traore et al. [53] designed a framework for a multimodal biometric system for online examinations via continuous image capture with a webcam.

D. BIOMETRIC EXAM TAKER VERIFICATION SYSTEM

Many obstacles are involved in the biometric verification of test-takers in higher learning. To support the biometric verification technology, a number of factors, including the integration of an existing system, the developers' skills, and the technology's maturity, must be considered. Using fingerprint recognition [54] provided a safety infrastructure for the online examination. The biometric system developed to authenticate examinees in Nigeria was created by [45]. Another reason for utilizing biometric technology in educational institutions, such as those researched by [46]. The objective of Okokpujie et al. [55] was to develop an iris-based biometric system for verifying the student's attendant. A smart door using biometric development enhanced a security system [22]. The BEPVS [56] was presented with the conceptual design model for verifying exam takers, which included components for developing a biometric system. The six components of an examinee biometric information system are illustrated in Fig. 2 of the BEPVS conceptual model. The purpose of this framework is to demonstrate the creation and implementation of the biometric exam-taker verification system. Examiner information, the examination information system, the result and output, biometric technology, the biometric examinee personal verification system, and the intelligence system are the six principal components of the system development framework.

The BEPVS conceptual framework also presented the specifics of a revised software design model created software for use in an educational institution. Fig. 3 depicts the BEPVS architecture, consisting of thirteen system components demonstrating the design and development of a biometric exam-taker verification system.

Exam taker information is provided by examiner information (EI) component. The examination information system (EMS) component provides an examination information

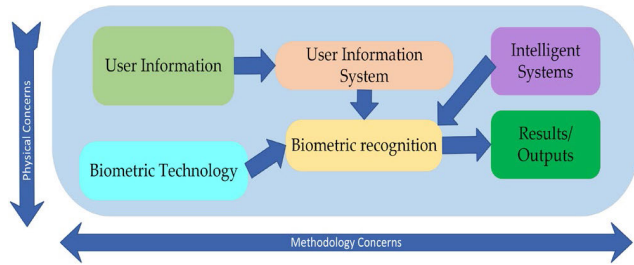


FIGURE 2. Revised BEPVS conceptual framework.

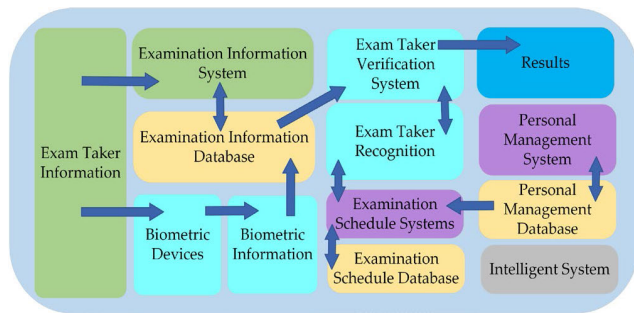


FIGURE 3. Biometric recognition framework in education.

management system. A component of the examination information database (EIDB) manages the student database by communicating with a component of biometric information (BI) stored on a component of the biometric device (BD). Exam taker verification system (ETVS) component responds to detect and identify students using exam taker verification (ETV), examination schedule database (ESSDB), and examination schedule system (ESS). A Personal Management System (PMS) and personal management database (PMDB) components oversee student data creation, retrieval, modification, and deletion. A personal management system (PMS) is an administration system of faculty in the educational institute. A result component provides feedback on a student’s system identification. An intelligent component of the system prepares for a future support system for artificial intelligence.

E. BIOMETRIC TECHNOLOGY ON INTERNET OF THINGS PLATFORM

The IoT is currently the most popular platform for human life support, particularly in education [1], [7], [8]. Utilizing biometric technology on IoT platforms has the advantages of being economical, compact, and mobile. Recent studies have demonstrated various biometric applications utilizing the Internet of Things to create systems and applications. Emerging internet of things services in smart cities, industry, smart homes, and personal assistants, among others, require security at multiple stages. Intruders may inject fabricated data into the communications of the internet of things. Applying security to IoT devices makes it possible to realize mobility, portability, and multiple services. These issues are

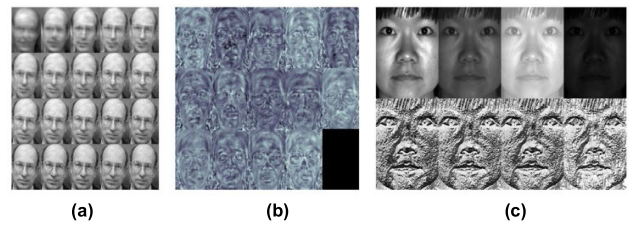


FIGURE 4. (a) Eigenfaces, (b) Fisherfaces, and (c) LBPH in OpenCV.

circumvented by utilizing biometric security, which does not require action or memory. Biometric authentications are popular, more reliable, and user-friendly than conventional methods. The previous research has discussed IoT issues and challenges regarding biometric security and application, including where biometrics can be integrated into IoT infrastructure [26], [51], [57].

F. OPENCV FACE RECOGNITION DEVELOPMENT

OpenCV is a well-known artificial intelligence library for image processing founded in 1999 by Intel. The cross-stage library emphasizes continuous image processing and includes non-patent-protected implementations of the latest computer vision calculations. OpenCV now includes a programming interface for the C, C++, Python, and Android programming languages. OpenCV is distributed under the BSD license, which is used for academic projects and commercial products. Fig. 4 illustrates OpenCV’s three primary algorithms.

Eigenfaces - The image depiction is rendered with a high degree of dimension. Two-dimensional PQ grayscale images span PQ-dimensional vector space, so a 100 × 100 pixel image resides in a 10,000-dimensional image space. A developer can settle on any variation in relevant data and search for information. Pearson [58] and Hotelling [59] independently proposed the Principal Component Analysis (PCA) to transform a large number of possibly related factors into a more compact arrangement of uncorrelated factors. Frequently, associated factors represent a high-dimensional dataset. The majority of the data is comprised of a handful of significant aspects. The PCA technique tracks down the bearings with the best difference in information called the head parts. Fig. 4 (a) illustrates the Eigenfaces of OpenCV image processing.

Fisherfaces - Principal component analysis (PCA), the core of the Eigenfaces method, identifies a direct mixture of components. The method accentuates the extreme fluctuation in data. Although this is an unquestionably excellent method for addressing data, it does not consider classes. As a result, many discriminative data could be lost when discarding parts. Imagine a scenario in which an external source modifies the information of a user. Let there be no darkness. The components distinguished by a PCA lack discriminative data, so the projected examples are dispersed, making it impossible to characterize the population. The fisherfaces of OpenCV image processing are depicted in Fig. 4 (b).

Local binary pattern histogram (LBPH) - Eigenfaces and fisherfaces are adaptable to support a comprehensive acknowledgment strategy. Information is represented as a vector in high-dimensional image space. High-dimensionality is awful, so a lower-dimensional subspace is distinguished and (presumably) utilized to store useful information. The Eigenfaces strategy expands the total dissipation, which can cause issues if an external source fluctuates since parts with the greatest difference in overall classes are not useful for arrangement. The authors have utilized a linear discriminant analysis to safeguard some discriminative data, which was enhanced according to the fisherfaces method.

Numerous types and techniques have been investigated by analyzing the development performance of biometric systems. Under various weather conditions, Ahsan et al. [60] compared the performance of three facial recognition algorithms in OpenCV, including eigenface, fisherface, and local binary pattern histogram-based methods. In their research, the evaluation criteria were the accuracy, precision, recall, F1 score, and execution time. According to the findings of their study, LBPH had better outcomes than other treatments. Fig. 4(c) depicts the LBPH of the OpenCV image processing. The factors used to assess biometric efficiency in the various domains are presented in Table 1.

III. RESEARCH MODEL AND HYPOTHESES

This primary objective of this study was to experimentally investigate a biometric recognition system for education. This investigation commences with a framework design for IoT-based biometric technologies, which consists of designing and developing a biometric exam-taker management system and biometric verification architecture. The authors developed an IoT-based biometric verification system that supports various biometric technologies, including face and fingerprint-based unimodal, multimodal, and semi-multimodal biometrics. The developed system's effectiveness and efficiency have been evaluated. The accuracy rate, error rate, response time, and cost are used to compare the effectiveness and efficiency of using a biometric verification system for exam takers. Four biometric approaches involve the experimental study of the system's evaluation: zero-biometric (Z), unimodal biometric system (U), multimodal biometric system (M), and semi-multimodal biometric system (S). Using face and fingerprint experiments, the authors implement a biometric verification system for each testing group. Identifying the sampling group, testing the system, and collecting data for each testing group are the three aspects of each experiment. This study has compared each experimental outcome by determining which biometric protocol best suits the biometric verification system for educational applications.

A. RESEARCH OBJECTIVES AND HYPOTHESES

The authors have adopted the BEPVS conceptual framework [56] depicted in Fig. 3. To investigate the research

TABLE 1. Survey of performance evaluation criteria in biometric system usages.

References	Evaluation Criteria	Factors
Dube <i>et al.</i> [61]	A framework for evaluation of biometric based authentication system	- Performance - Privacy - Security
Kanak and Sogukpinar [62]	BioTAM: A technology acceptance model for biometric authentication systems	TAM + Trust - Public willingness - Confident - Estimate Privacy - Estimated Security
Zhou [63]	Evaluation of biometric recognition in the Covid-10 period	Universality, Permanency, Uniqueness, Accuracy, Acquisition, Usability, Safety
Oh <i>et al.</i> [64]	Usability evaluation model for biometric system considering privacy concern based on MCDM model	- Technical aspect (Effectiveness, Efficiency) - Ergonomic aspect (Anthropometry-fit, Accessibility, Affordance Psychological aspect) - Psychological aspect (privacy concern, Satisfaction)
Malatji <i>et al.</i> [65]	Acceptance of biometric authentication security technology on mobile devices	Performance, User Acceptance, Acquisition Device
Ammour <i>et al.</i> [48]	Multimodal biometric identification system based on the face and iris	Accuracy (FAR, FRR)
Siddique <i>et al.</i> [66]	Reliability and acceptance of biometric system in Bangladesh: Users perspective	Reliability, Ease of use, Security, Cost
El-Abed <i>et al.</i> [67]	Evaluation of biometric systems	Universality, Uniqueness, Permanency, Collectability, Acceptability
Ahsan <i>et al.</i> [60]	Evaluating the performance of eigenface, fisherface, and local binary pattern histogram-based facial recognition methods under various weather conditions	Accuracy, Precision, Recall, F1 Score, Execution Time

objectives, the practical implementation of an IoT-based biometric system for exam taker verification is also created. This section describes the design and development of the experimental system in accordance with the IEEE systems design—software design descriptions (SDD) standard [68] and systems and software engineering - Systems and software quality requirements and evaluation (SQuaRE) [69]. Use-case diagrams represent the context viewpoint, class diagrams represent the information viewpoint, deployment diagrams show the composition viewpoint, and graphical user interface (GUI) diagrams represent the interface viewpoint, and sequence diagrams represent the interaction

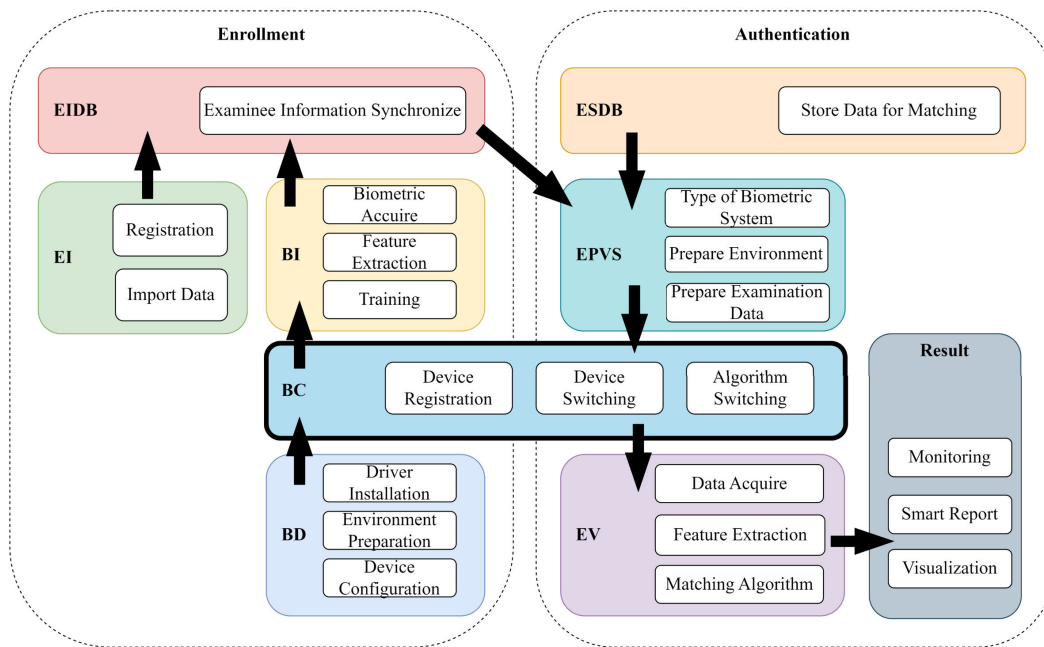


FIGURE 5. Biometric verification processing framework.

viewpoint. Using this study's quality assessment metric approach, the following are the primary concerns for confirming and evaluating the practical use of the IoT-based biometric recognition system for identity verification services.

Using IoT technology, the first objective is to propose software design and development for examination management and biometric recognition systems with face and fingerprint. IoT-based biometric examination verification systems can utilize unimodal, semi-multimodal, or multimodal biometrics. Consequently, the feasibility and promise of biometric technologies used for student identity verification can be evaluated by effectiveness and efficiency to determine if the IoT-based biometric system for verifying exam takers could adequately replace traditional proctoring for student identity verification.

The secondary objective is to examine quality measurement metrics for the biometric verification system by analyzing biometric effectiveness in an actual exam environment. The proposed quality metric for biometric verification of students in actual examination classrooms could evaluate and ensure biometric quality assurance of accuracy rate [49], error rate [23], [70], response time [46], and cost [66].

The hypotheses of this study are identified as contributing to biometric assessment quality assurances for educational applications. The following are the answers to the questions posed by the hypothesis:

Hypothesis 1 (H1): The quality of the unimodal biometric system for verifying exam candidates is superior to that of a conventional system.

Hypothesis 2 (H2): The quality of the multimodal biometric system for verifying exam takers is superior to that of a conventional system.

Hypothesis 3 (H3): The multimodal biometric system for verifying exam takers is of a higher quality than the unimodal biometric system.

B. BIOMETRIC DATA ENROLLMENT

Fig. 5 depicts the system architecture derived from the revised design model of a biometric examinee personal verification system as illustrated in Fig. 3. Examinee registration, biometric collection, biometric verification, biometric databases, and verification results are components of the biometric verification processing framework. The framework comprises two major components: exam taker enrollment and authentication.

The data enrollment or training phase involves collecting test-takers biometric information into a database. The information about the exam taker is typically personal information, including biometric data. The system can collect personal information from existing data by accessing student identification numbers. However, biometrics collection is contingent on the biometric trait and devices used. This study employs the face and fingerprint as biometric system characteristics. Face and fingerprint biometrics share similar data collection procedures. By implementing an IoT-based biometric verification system in front of the examination room, the biometric registration device must install drivers, set the verification environments, and configure parameters to function correctly. After acquiring a student's face and fingerprint, the feature extraction processes commence, and

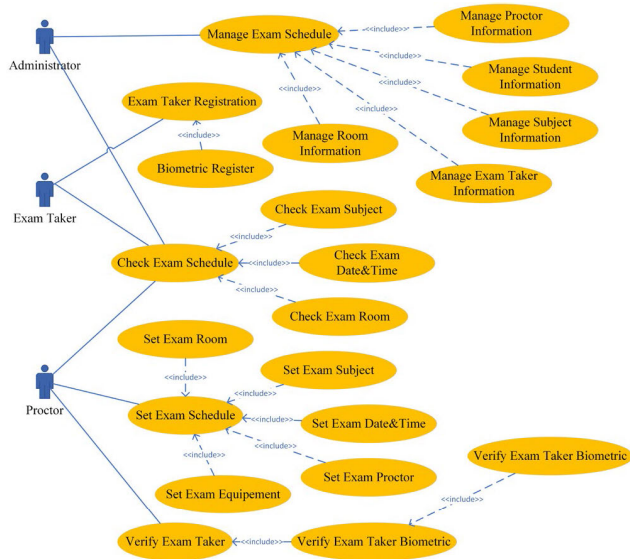


FIGURE 6. General use-case diagram of examination management system.

the system registers students’ biometrics and information as a training set in a database. Face and fingerprint-based multimodal biometric systems have been investigated in this study. Therefore, two biometric scanners are configured to support dynamic manners. Each scanner device can seamlessly switch between unimodal and multimodal modes. The IoT-based biometric verification system box is developed as a biometric system controller. The smart box can scan facial and fingerprint biometrics and manage biometric recognition algorithms for experimental data enrollment.

The testing phase of biometric recognition is a verification procedure utilizing an IoT-based biometric verification system for exam takers. The verification of an exam taker’s identity relies on biometric datasets. A smart box permits flexible examination verification protocols. If a test taker uses face-only biometric verification, the system verifies only the test taker’s face. The verification result can be determined by accuracy and error rates by comparing recent biometric datasets from training sources in the database system. The results of the detection is then reported as the verification value. Educational administrators can utilize face and fingerprint biometric systems to match a test-biometric taker’s data with the biometric data stored in a database.

C. EXAMINATION MANAGEMENT SYSTEM DESIGN

Fig. 6 depicts a use-case diagram that describes the system’s actors and their respective responsibilities. Beginning with a user needs survey, the authors analyzed and designed the exam taker biometric verification system using a use-case diagram containing three actors: the exam taker, the administrator, and proctor. The test-taker biometric verification system consists of twenty-two key processes. Administrators

are responsible for managing all data, including exam subjects, exam information, biometric information, proctors, exam lists, exam locations, and student information. The examinees use the system to register their biometric data and review the exam details. Proctors utilize the biometric verification system to verify the identity of examination candidates and monitor the functionality of the system. Fig. 7 depicts a database system with a class diagram format, a data format, and a relationship for the biometric exam-taker verification system. The developer team can create the database system. Seven classes make up the database collection (verified-result, examschedule, examinerbiometricinfo, examiner, subject, place, and proctor).

D. INFRASTRUCTURE DEVICES

The IoT-based biometric verification system consists of the hardware of the system, face images and fingerprint template-based biometric technologies. This research uses two biometric devices: an 8-megapixel Raspberry Pi camera for face recognition and a fingerprint scanner (Arduino compatible). Raspberry Pi cameras can capture 1080p images with a high resolution and can be completely programmed. A Raspberry Pi 4 8GB is connected to a camera, fingerprint scanner, and monitor in front of an exam room. This research uses two Raspberry Pi Camera (8-megapixel) biometric devices for face recognition. The Raspberry Pi camera can capture high-resolution images, 1080p video in full HD, and programmable code. Fingerprint scanners compatible with Arduino are used for fingerprint recognition. In Table 2, the specifics of each device are listed.

E. IOT-BASED BIOMETRIC VERIFICATION SYSTEM DESIGN AND DEVELOPMENT

Fig. 8 represents an overview of the experiment’s IoT-based biometric verification system architecture. EDIB, ESSDB, and PMDB were developed using MySQL server as a centralized biometric database to support web-based application programs for exam taker verification systems. Students face images, and fingerprint templates were collected and stored in a centralized database. Each training dataset for an IoT-based biometric verification system must be used to train the two biometrics listed below:

- Face recognition training: The system is developed using the OpenCV library with Python and the LBPH model as a face recognition algorithm to recognize a student’s face.
- Fingerprint recognition training: The OpenCV library and Python programming language, in conjunction with the scale-invariant feature transform (SIFT) algorithm, are used to extract key points and detect descriptors for the best-retained features.

After receiving the examination room’s student roster, the proctor logs into the system during the verification phase. The students formed a single line in front of the examination room, awaiting verification. Each student requires to use face

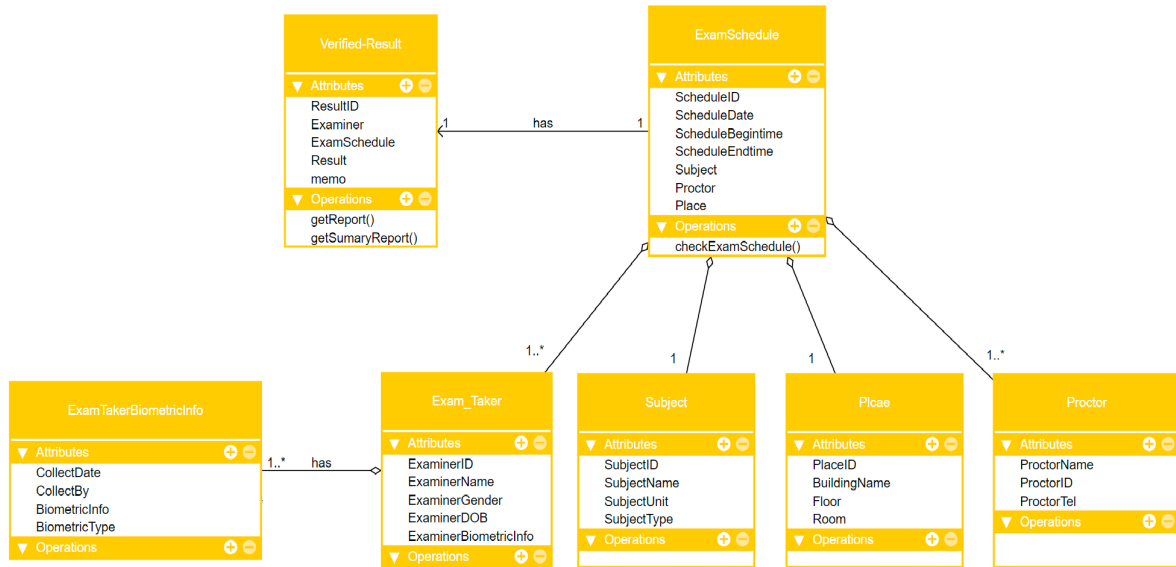


FIGURE 7. Class diagram of exam taker biometric verification system.

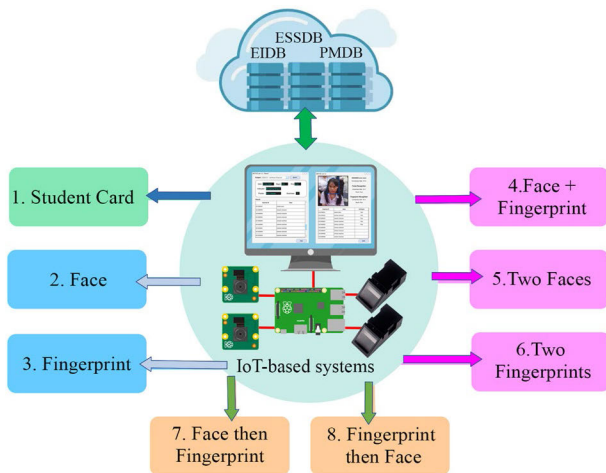


FIGURE 8. Overview of experimental scenarios of IoT-based biometric identity recognitions system.

and fingerprint biometric verification to identify the identity phase as follows:

- Face recognition matching algorithm: The system matches biometric data utilizing the LBPH model within the OpenCV framework.

- Fingerprint recognition matching algorithm: The authors used feature matching with the fast library for approximate nearest neighbors (FLANN) algorithm to match the fingerprint image of the exam taker with the pattern from the database.

The quality scores and scanning times for student recognition were recorded in a database log and displayed on an LCD screen after biometric verification.

This study categorizes the potential biometric verification case studies into eight identity verification approaches. The first method employs identification cards. Other approaches rely on biometrics for identification. The second method employs facial biometrics, while the third method employs fingerprint biometrics. The fourth method employs face and fingerprints. The fifth method uses a face captured by two cameras, while the sixth method uses fingerprints captured by two scanners. The seventh method uses the face, then the fingerprint, while the eighth method uses the fingerprint, then the face. Each biometric protocol’s configuration is handled by a single-board computer (Raspberry Pi 4). Over a wireless network, the Raspberry Pi 4 connected to biometric devices captures a student’s identity and retrieves the student’s biometric from the database system to determine whether the student is authentic or fraudulent.





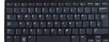


IV. METHODOLOGY

The experimental methodology includes collecting and analyzing datasets, training and testing datasets, comparing various biometric verification approaches, and evaluating biometric quality criteria for effectiveness and efficiency.

A. DATA COLLECTION AND ANALYSIS

The preparation and conduct of this study occurred between January and October of 2022. This research meeting was open to sixty undergraduates from three examination classrooms at the Valaya Alongkorn Rajabhat University, Thailand. The authors explained the research’s objectives, contents, and methodology to the students. When students had questions, the authors provided online contact information to the researcher and research assistant. The authors informed the students through consent that they would provide facial and

TABLE 2. Biometric device specification in development.

Biometric Device	Specification	Cost
	Raspberry Pi Camera (8mp) - Sensor: Sony IMX219 - Sensor Resolution: 32480 x 2464 (8 megapixels) - Sensor Image Area: 3.69 x 2.81 mm - Pixel Size: 1.12um x 1.12um - Optical Size: 1/4" - Video: Dimension: 25mm x 23mm x 9mm / 0.98" x 0.90" x 0.35" 1920 x 1080 (1080p), 30 fps 1280 x 720 (720p), 60 fps 640 x 480 (480p), 90 fps - Weight: (Camera board + attached cable): 3.4g	\$40
	Fingerprint reader Adafruit R305 - Fingerprint Imaging Time: less than 1 second - Match Mode: Compare Mode 1:1 - Search Mode: 1: N - Window Area: 14 mm. x 18 mm. - Signature File Size: 256 bytes - Template File Size: 512 bytes - Storage Capacity: 162 templates - Safety Ratings: 1 (low) to 5 (high) - False Acceptance Rate: less than 0.001% - False Reject Rate: less than 1% - Interface: Serial UART TTL - Baud Rate: 57600 by default (9600, 19200, 28800, 38400, 57600 configurable) - Working Temperature Rating: -20 to +50 Degree Celsius - Working Humidity: 40 to 85 %RH - Full Dimension: 56 mm. x 20mm x 21.5mm (H x W x L)	\$55
	Raspberry Pi 4 Model B - BCM2711 SoC - 8GB DDR4 RAM - USB 3.0 - PoE Enabled	\$335
	LG 50 inches UQ8000PSC UHD 4K Smart TV	\$315
	Raspberry Pi Black - Grey QWERTY (UK) Raspberry Pi Keyboard	\$20
	256 GB MICRO SD Card	\$40
	Pair wires - GPIO Extender cable male female 40 Pin - Jumper wire male to female	\$10

fingerprint biometric data voluntarily. Students' information confidentiality and biometric information were safeguarded and only used to verify their identity in front of examination rooms on scheduled examination dates. All the students consented to participate in the research project. To ensure the accuracy of the biometric data, each student's face and fingerprint recognition during the training and testing phases must reach an accuracy score of 85 percent. The study

recruited thirty students by dividing each sample group into two types of exam takers: five fake exam takers and twenty-five real exam takers. The first sample group confirmed each student's identity using an IoT-based biometric verification system. A second sample group was subjected to traditional examination proctoring in which an identification document verified each student's identity.

By comparing zero-biometric, unimodal, multimodal, and semi-multimodal biometrics, the data analysis measured the quality of an IoT-based biometric verification system. As depicted in Fig. 9, the metric performance of the quality measurement could be assessed using a combination of conventional and biometric verification techniques. The protocols for detecting student identification consisted of 1) student identification for a traditional method of verification as a zero-biometric. 2) The facial unimodal biometric system recognizes only the face. 3) Only fingerprint recognition is supported for the unimodal biometric system. 4) Face and fingerprint verifications for a multimodal biometric system. 5) Face recognition through two cameras for a multimodal facial biometric system. 6) Fingerprint examinations utilizing two scanners for the multimodal fingerprint biometric system. 7) Face and then fingerprint verification for the semi-multimodal biometric system. 8) For the semi-multimodal biometric system, fingerprint verification is followed by face verification. Comparing traditional and biometric verification methods, the system then calculates the exam-identity taker's recognition results for quality scoring.

B. TRAINING AND TESTING DATASET

This experiment's dataset preparation consisted of two distinct phases: preparation for facial recognition and preparation for fingerprint recognition. The development of the biometric recognition system utilized OpenCV and Python to train and test a portion of the training and testing datasets. According to the findings of Ahsan et al. [60], the LBPH algorithm is the simplest and most effective face recognition method. In this experiment, system development utilized the LBPH algorithm. To optimize the environment for face recognition with the camera, experimentation was conducted by [51] to determine the optimal distance between the camera and the subject for a 640 x 480 resolution. This experiment replicates their findings by limiting the camera-to-subject distance to 1.12 meters and employing the Python face recognition package to calculate the bounding box around each face, facial embedding, and face comparisons in the encoding dataset.

The authors took ten photos of each exam taker's face without eyeglasses from various angles for the training dataset and then used the LBPH method to train and store the biometric pattern of each exam taker in the database. Each participant collected their faces in a single round. Ten images were captured by the IoT camera for each student using the same camera angle and distance.

The training and testing datasets of students' faces were collected under the same environmental conditions of

ambient daylight with two fluorescence in open areas from 8:00 a.m. to 9:00 a.m. A digital multimeter measured the lux level of illumination for a light meter as 197.

The authors captured two images of each finger as part of the biometric fingerprint training and testing dataset. Using cloud computing, one exam candidate enrolled and remained in the database using two fingers. Proctors applied alcohol every time fingerprints were collected. A fingerprint reader's glass must be wiped clean for each student scanned. This study configured the fingerprint reader Adafruit R305 and Arduino libraries using the solution from [71] to match the fingerprint image to the examinee.

C. COMPAIRISON OF DIFFERENT VERIFICATION SCENARIOS

This experiment compared four testing technologies of biometric approaches to evaluate the quality of an IoT-based biometric verification system for the identity verification of exam takers in a higher education institution: Zero-Biometric System (Z), Unimodal Biometric System (U), Multimodal Biometric System (M), and Semi-Multimodal Biometric System (S). Therefore, the experimental results can be divided into eight protocols.

1) ZERO BIOMETRIC (Z)

The zero-biometric system is a conventional method of identity verification that employs human proctors. A proctor verifies the students' identities by examining the photographs on their identification documents, such as student ID cards, personal ID cards, driver's licenses, and passports. Consider a student who appears to lack identification. In such a case, a proctor will request that a student obtains a day temporary identification card from the registrar's office or contacts the instructor of a specific examination subject to confirm a student's status. The instructor can verify the student's identity. As depicted in Fig. 1, a proctor will then permit the student to sign a temporary identification form for entry into the examination room.

2) UNIMODAL BIOMETRIC (U)

A unimodal biometric system includes only a single biometric. This experimental protocol utilizes facial or fingerprint biometrics. This study chose facial and fingerprint biometrics because examination verification systems require speed and convenience, and numerous exam candidates are available in the exam room. The study utilizes biometrics with universally high acceptance, reasonable costs, and experimentation suitability.

Algorithm 1 depicts the verification procedure for exam takers utilizing facial or fingerprint biometrics in conjunction with an IoT-based verification system. The examination results indicate that the examinee's biometric information does not match the biometric data in the database. In such a circumstance, the examinee will be denied entry into the

Algorithm 1 Pseudocode of Unimodal Biometric Verification

Input A student's face or fingerprint

Output The verification result of each student

Start Algorithm

A biometric verification system sets active

A biometric device is activated with configuration

A student walks into an examination room

Foreach data acquire on training dataset

For each biometric data captures, n data

 Biometric area detection

 Biometric preprocessing

 Biometric feature extraction

 Store a biometric feature as a biometric template on the database

 Display storing information

 Display results

End

For each data acquire on testing dataset

 Biometric area detection

 Biometric preprocessing

 Biometric feature extraction

 Match a biometric feature to biometric templates on the database

 Return the verification result

If the accuracy matching result is more than 0.85

 Accepted result of identity verification

Else

 Unaccepted result of identity verification

 Display results

End

End Algorithm

examination room. The rejected candidate must contact the subject instructor or other instructors who can verify the candidate's eligibility to take the examination. A proctor will then permit the student to sign a temporary identification form for entry into the examination room.

3) MULTIMODAL BIOMETRICS (M)

A multimodal biometric system incorporates at least two biometrics. This experiment requires two facial and fingerprint biometrics to detect and verify the identity of students.

Algorithm 2 represents the identity verification workflow of the multimodal biometric method. There are three possible verification outcomes. The system accepts two biometric protocols for the student to enter the exam room. The system accepts either protocol but denies access to the examination room if neither is presented. A proctor requests that the student undergo verification multiple times until the system can confirm his/her face and fingerprints. The system rejects all biometric protocols, denies the student access to the examination room, and flags him or her as a fraud student.

Algorithm 2 Pseudocode of Multimodal Biometric Verification**Input**A student's faces and fingerprints**Output**The verification result of each student**Start Algorithm**

A biometric verification system sets active

First biometric devices are activated with configuration

Second biometric devices are activated with configuration

A student walks into an examination room

For each data acquire on training dataset **For** each of the first biometric data captures, n data

First biometric area is detection

Second biometric area detection

Both biometric data preprocessing

Both biometric features extraction

Store biometric features as biometric templates on the database

Display storing information

Display results

End**For** each data acquire on testing dataset

First biometric area detection

Second biometric area preprocessing

Both biometric data extraction

Both biometric feature extraction

Match first biometric feature to biometric templates on the database

Match second biometric feature to biometric templates on the database

Return both verification results

Accuracy fusion calculation of first and second biometric recognition

If the fusion biometric recognition of accuracy matching result is more than 0.70

Accepted result of identity verification

Elseif the accuracy matching of first result is more than 0.85

Accepted result of identity verification

Elseif the accuracy matching of second result is more than 0.85

Accepted result of identity verification

Else

Unaccepted result of identity verification

Display results

End**End Algorithm**

Face and fingerprint - Upon student entry into the examination room, the multimodal biometric method can simultaneously apply face and fingerprint recognition. A web camera focuses on a test-taker as they enter a fingerprint-scanning device and sends the data to a database. Only examination candidates accepted by both biometric devices may enter the examination room. If a candidate were accepted by only one

biometric device, he or she would be denied access to the examination room.

Face with two cameras - Using multiple sensors and two cameras, this experimental group has verified exam takers. The brand and quality of the first and second cameras are identical, but their positions differ. Consequently, the images captured by the two cameras have distinct perspectives. The proctor admits only examination candidates who are approved by both cameras. If only one camera accepts an exam candidate, that individual will not be allowed into the examination room.

Fingerprint with two scanners - This experimental group has implemented a technique involving multiple sensors and two fingerprint scanners to verify exam takers. The quality and brand of the first and second fingerprint scanners are identical. Examinees must scan their fingerprints simultaneously on two fingerprint scanners. The proctor admits only exam candidates who both scanners have approved. If either scanner permitted the examinee to enter the exam room, the examinee would be denied entry.

4) SEMI-MULTIMODAL BIOMETRICS (S)

A single biometric system incorporates two biometrics. Face biometrics and fingerprints are sequentially required by semi-multimodal biometrics to detect and confirm student identity.

This experimental method sequentially verifies the face and fingerprint biometric identifiers. In our research, face recognition precedes or follows fingerprint recognition or vice versa. For instance, a genuine student may walk past a camera sensor or scan a fingerprint. Consider that the first biometric recognition using the camera sensor, or the fingerprint scanner captures the student's biometrics, and then the biometric database management system identifies biometric extraction. In this instance, the student's identification is accepted for entry into the examination room if the biometric templates captured match the biometric templates contained in the biometric database. If the initial biometric recognition during biometric scanning fails, a proctor asks the student to rescan the biometric until a result is obtained.

Alternatively, if the student's first biometric is rejected, he or she must scan a second biometric device to confirm his or her identity. If the student is scanned by a second biometric, the scanned biometric template is located on the biometric database management system. Then, the student is permitted to enter the examination room after his or her identity has been confirmed.

The biometric database management system cannot confirm the student's identity if the second biometric scan fails. A proctor will then be alerted by the system notification. Suppose that the student continues to be rejected by both types of biometrics. In such a scenario, a proctor requests that the student contact an instructor of the exam subject, who can verify the student's identity to verify student identity. If an instructor of the exam subject can verify the student, a proctor will provide a temporary identification

Algorithm 3 Pseudocode of Semi-Multimodal Biometric Verification**Input** A student's faces then fingerprints, or vice versa**Output** The verification result of each student**Start Algorithm**

A biometric verification system sets active

First biometric devices are activated with configuration

Second biometric devices are activated with configuration

A student walks into an examination room

For each data acquire on training dataset **For** each of the first biometric data captures, n data

First biometric area is detection

Second biometric area detection

Both biometric data preprocessing

Both biometric features extraction

Store biometric features as biometric templates on the database

Display storing information

Display results

End**For** each data acquire on testing dataset

First biometric area detection

First biometric data extraction

First biometric feature extraction

Match first biometric feature to biometric templates on the database

Return verification results

If the accuracy matching result is more than 0.85

Accepted result of identity verification

Else

Second biometric area preprocessing

Second biometric data extraction

Second biometric feature extraction

Match second biometric feature to biometric templates on the database

Return verification results

If the accuracy matching of second result is more than 0.85

Accepted result of identity verification

Else

Unaccepted result of identity verification

Display results

End**End Algorithm**

form with the student's signature. This method's workflow is represented by Algorithm 3.

D. BIOMETRIC QUALITY METRIC OF EFFECTIVENESS EVALUATION CRITERIA

Numerous researchers evaluate the biometric system and determine its quality based on various factors [24], [71], [72]. The essential aspects of a biometric system's quality investigation involve measuring its performance, accuracy, precision, recall, and execution time. Cost is also taken into

account when assessing biometric quality. Using a set of evaluation criteria, the authors compare biometric approaches. The biometric quality metric evaluates quantitative factors, including accuracy, error rate, processing time, and cost, as indicated by (1), the biometric quality metric.

Biometric quality metric

$$= \{Accuracy, ErrorRate, ProcessingTime, Cost\} \quad (1)$$

The average classification accuracy (ACE) formula has been utilized by Accuracy to evaluate and compare verification performance. ACE can be calculated using (2).

$$ACE = 100 \frac{(FMR + FNMR)}{2} \quad (2)$$

The error rate is a numerical score that indicates the proportion of potential genuine cases. False exam-takers have been permitted to enter a room titled false accept rate (FAR). Genuine exam candidates were denied entry to the examination room named false reject rate (FRR). The error rate indicator score should ideally be nearly zero, meaning that FAR and FAR are equal to zero. FAR can be expressed as (3).

$$FAR = FMR * (1 - FTA) \quad (3)$$

In addition, False match rate (FMR) is the percentage at which biometric processing incorrectly identifies biometric signals from two distinct individuals originating from the same individual. FMR is designated as (4).

$$FMR = \frac{\text{Number of false acceptance}}{\text{Number of impostor attempts}} * 100 \quad (4)$$

False reject rate (FRR) is the inverse of the false acceptance rate (FAR), which is the error rate score when the system denies the real examinee access to the examination room. FRR can be computed using (5). In addition, False to acquire (FTA) is the percentage of attempts in which the system fails to acquire a sample of adequate quality. FNMR can be computed using (6).

Time (T) is the duration of an exam-taker verification's execution. When the system cannot acquire an examinee detection result, the exam taker must re-verify his or her face or fingerprint until the system can acquire the biometric information. As (7) summarizes that each examinee is subject to multiple checks.

$$FRR = FTA + (FNMR) * (1 - FTA) \quad (5)$$

$$FNMR = \frac{\text{Number of false rejection}}{\text{Number of genuine exam taker attempts}} * 100 \quad (6)$$

$$T = \sum_{i=1}^n T_n \quad (7)$$

where n is a number of verifications for a student

Cost (C) is the cost of equipment for the IoT-based biometric system used to verify exam candidates. While the multimodal biometric system is more efficient than the

unimodal biometric system, the Internet of Things-based multimodal biometric system has a higher budget.

V. RESULTS AND DISCUSSION

The experimental verification results of eight testing protocols were as follows: first protocol (student identification card detection), second protocol (face detection only), third protocol (fingerprint detection only), fourth protocol (face and fingerprint detection), fifth protocol (face with two- cameras detection), sixth protocol (fingerprints with two- scanners detection), seventh protocol (face then fingerprint detection), and eighth protocol (fingerprint then face detection). For each testing protocol, the outcome is subdivided into five criteria of verification result: the average accuracy rate, the average error rate, the effective response times, the cost of biometric devices, and the estimated cost of 500 hours of usage. The verification results of eight testing protocols are summarized in Table 3 in terms of average precision, average error rate, average processing time, and the average cost of biometric devices.

According to Table 3, the sixth testing protocol (two fingerprints) has the highest average rate of identity recognition accuracy at 96.67 percent. In contrast, the initial testing protocol received the lowest score of 66.67 percent. The sixth testing protocol has the lowest average error rate for identity recognition at 1.82 percent, while the first testing protocol has the highest average error rate at 21.29 percent. The second testing protocol has the best average response time for identity verification at 2.49 seconds, while the first testing protocol has the worst average response time at 14.01 seconds. The cost of the biometric device is the subject of this study. Due to the absence of biometric devices in the first testing protocol, the device cost is unavailable. Therefore, the sixth testing protocol has the highest cost of biometric devices, at \$110, while the second testing protocol has the lowest cost, at \$40.

Valaya Alongkorn Rajabhat University proctor was estimated to cost US\$11.43 per hour. The estimated cost of IoT usage is based on the mean time before the failure of Raspberry Pi (MTBF). It has been estimated that Raspberry Pi could operate reliably for five to seven years [73]. The authors assume that the minimally functional hardware will continue to operate reliably for 1.5 years (approximately 500 hours). The IoT-based biometric verification system costs \$720 (according to Table 2), and biometric sensors are excluded. Using these formulas, the price of the IoT-based biometric verification system with biometric sensors was determined (8).

$$\text{Total system cost} = \text{System cost} + \sum_{1}^n \text{Sensor}_n \quad (8)$$

where n is the number of biometric sensors

For instance, a facial biometric verification system based on IoT was estimated to cost a total of US\$760 (US\$720 + US\$40). Therefore, the cost per hour was calculated to be \$1.52 (US\$760 / 500 hours).

Therefore, the first testing protocol has the highest estimated cost per examination class (three hours), at US\$34.29. In contrast, the second testing protocol costs the least at \$4.56.

To rank-compare the scores of each testing protocol in Table 3, the authors reformat the result using the triangular law. Consider the maximum value of the average processing time to be 14.01 seconds. In this instance, the value is converted to 100 percent, and the new score is computed using the triangular law, as shown in Table 4. The total score for each of the eight testing protocols was determined by using the category rankings. The values for each category range from five to zero. The same proportion of ranks and scores in each category are identical. The highest possible score in each category is 5 for the category winner. In contrast, the lowest position receives no points. Each group was responsible for determining the sum of their scores. The highest total scores are converted to 100 percent using the triangular law, and a new score is calculated. Table 4 displays the revised score.

Table 4 and Fig. 9 detail the biometric quality metric scores for each testing protocol, excluding the traditional proctoring system, also known as a zero biometric system, which received no score. Fig. 9 demonstrates that the best scoring system was the unimodal face biometric system. The multimodal face and fingerprint biometric system, the multimodal fingerprint biometric system with two scanners, and the semi-multimodal face then fingerprint biometric system received the second-highest scores. The two-camera, multimodal face biometric system received the third-highest score.

To prove the research hypotheses H1 and H2, it was determined that the unimodal and multimodal biometric approaches' accuracy, error rate, and processing time are superior to the conventional verification method.

H1: The quality of the unimodal biometric system is superior to the quality of the conventional system for exam-taker verification.

Fig. 10 (A) displays the outcomes of the zero and unimodal biometric approaches utilized in the experiment. The results of the biometric quality metric were calculated and reported to compare the biometric techniques. The biometric quality metric employs identity verification factors to assess the quality scores of biometric devices (1). The traditional method yielded the highest scores for error rate, processing time, and cost but the worst performance in terms of accuracy rate for exam-taker identity verification.

However, the conventional approach's biometric quality metric is not calculated. On the other hand, the results indicate that the unimodal face or fingerprint has greater accuracy, processing speed, and effectiveness while maintaining a lower error rate and cost. The biometric quality metric of the unimodal face biometric system is the highest-ranked metric. The unimodal fingerprint biometric verification system ranks second. Therefore, the overall quality of unimodal biometric verification systems is superior to that of a biometric verification system with no biometric features.

TABLE 3. Results of biometric quality metric for traditional and biometric verification approaches.

Criteria	1. Zero Biometric	2. Face	3. Finger	4. Face + Finger	5. Two Faces	6. Two Fingers	7. Face then Finger	8. Finger then Face
Accuracy	66.67%	86.78%	86.67%	93.33%	90.00%	96.67%	93.33%	93.33%
Error Rate	21.29%	11.28%	3.49%	2.76%	4.83%	1.82%	2.35%	1.94%
Time (sec.)	14.01	2.49	4.69	6.54	2.76	9.81	6.69	6.77
Sensor cost	-	\$40	\$55	\$95	\$80	\$110	\$95	\$95
Estimate cost (3 hrs.)	\$34.29	\$4.56	\$4.65	\$4.89	\$4.80	\$4.98	\$4.89	\$4.89

TABLE 4. Transformation scores for each testing group.

Criteria	1. Zero Biometric	2. Face	3. Finger	4. Face + Finger	5. Two Faces	6. Two Fingers	7. Face then Finger	8. Finger then Face
Accuracy (%)	68.97	89.76 (2)	89.65 (1)	96.54 (4)	93.10 (3)	100.00 (5)	96.55 (4)	96.55 (4)
Error Rate (%)	100.00	52.97	16.39 (1)	12.97 (3)	32.09	8.55 (5)	11.04 (4)	9.11 (2)
Time (%)	100.00	17.75 (5)	33.46 (3)	46.67 (2)	19.70 (4)	70.04	47.76 (1)	48.31
System cost (%)	-	91.57 (5)	93.37 (4)	98.19 (2)	96.39 (3)	100 (1)	98.19 (2)	98.19 (2)
Total Score	-	12.00	9.00	11.00	10.00	11.00	11.00	8.00
Biometric Quality Metric	-	100.00	75.00	91.67	83.33	91.67	91.67	66.67

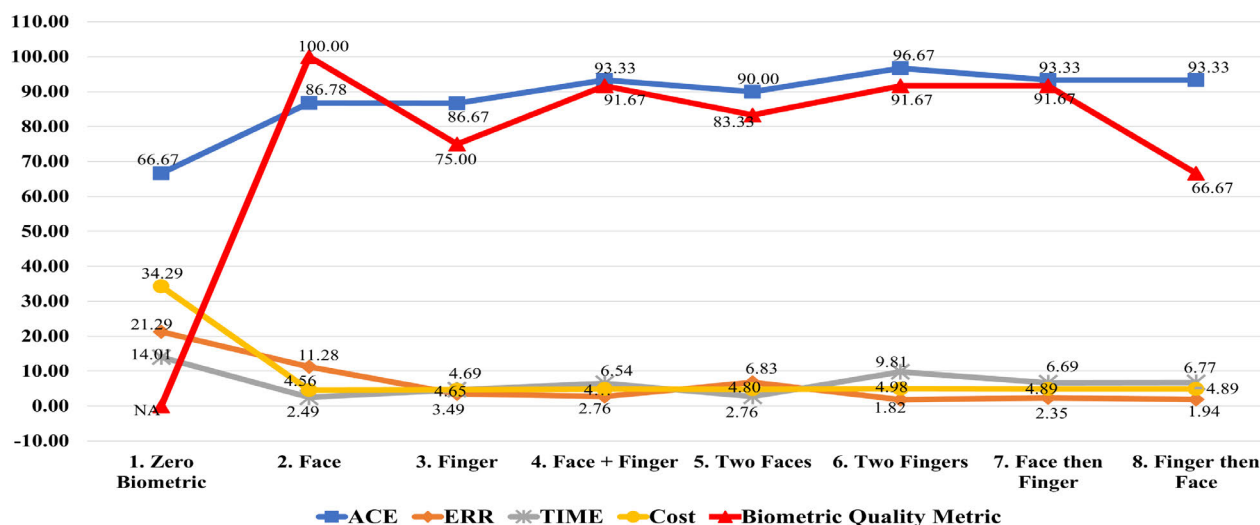


FIGURE 9. Comparison testing scores of biometric quality metric for different verification approaches.

H2: The multimodal biometric approach is superior to the conventional approach in terms of quality. Fig. 10 (B) and (C) depict the experimental outcomes of the conventional verification approach and multimodal biometric approaches. The results of the biometric quality metric calculation revealed that the traditional approach yields the

highest scores for error rate, processing time, and cost but the worst performance in terms of accuracy rate for exam taker identity verification. However, the conventional approach’s biometric quality metric is not calculated. The results of multimodal verification systems indicate, however, that face and fingerprint biometrics, face biometrics with two cameras,

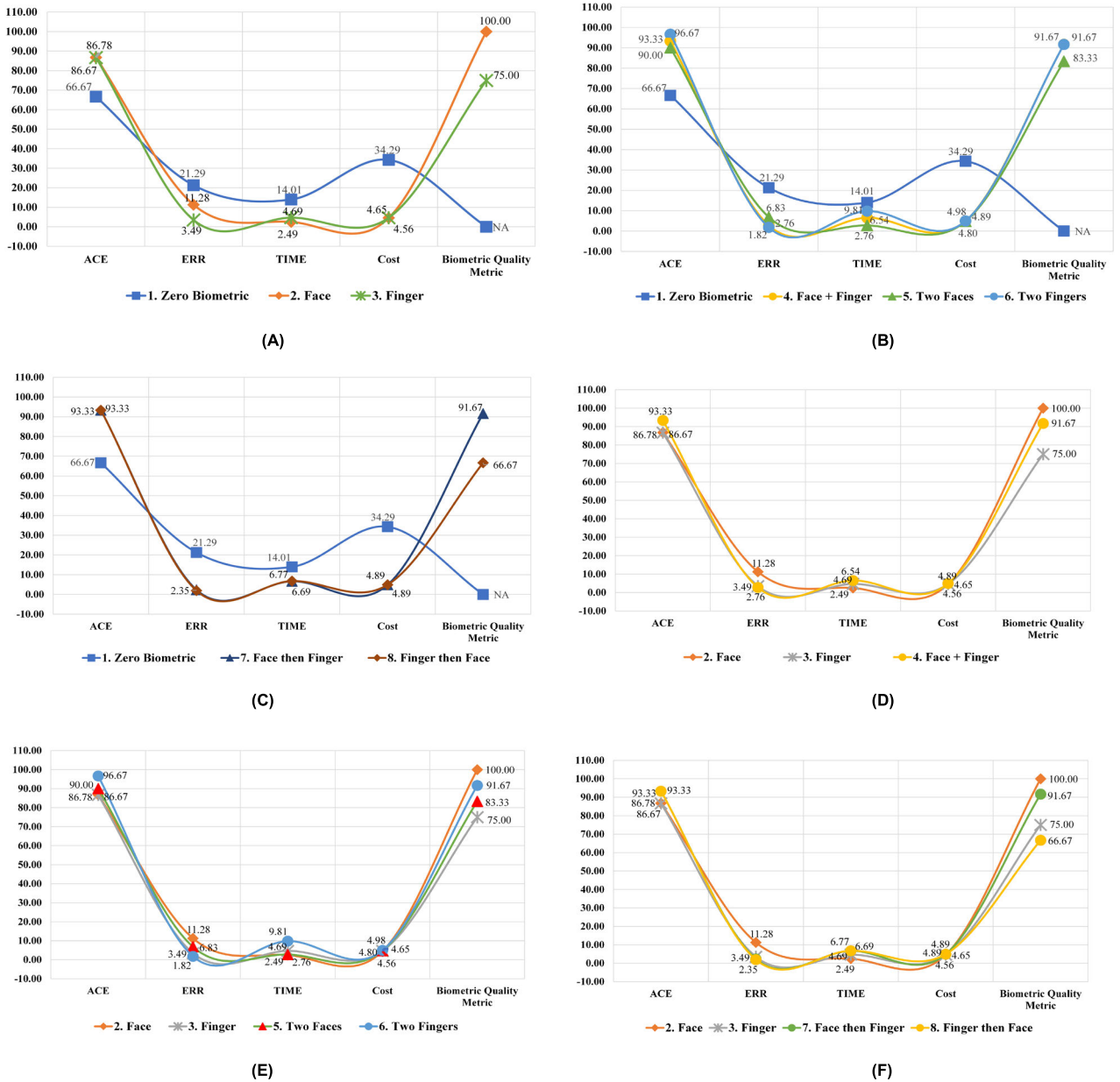


FIGURE 10. Each biometric verification approaches ranking by biometric quality metric.

and fingerprint biometrics with two scanners are more effective and efficient in terms of accuracy, processing time, and cost while maintaining a lower error rate and expense. In addition, the results of semi-multimodal verification systems indicate that face verification followed by fingerprint verification and fingerprint verification followed by face verification is more effective and efficient in terms of accuracy, processing time, and cost while maintaining a lower error rate. Face and fingerprints are utilized in the biometric quality metric of multimodal verification systems. The two fingerprints and the semi-multimodal face are ranked highest, followed by the fingerprint biometric verification system. Consequently, the overall quality of

multimodal and semi-multimodal biometric verification systems surpasses that of the zero biometric verification system.

H3: The multimodal biometric approach is superior to the unimodal biometric system for exam-taker verification in terms of quality. Fig. 10 (D), (E), and (F) illustrate that the biometric quality scores of unimodal face biometrics are the most effective and efficient overall. Multimodal biometric recognition systems employing face and fingerprint biometrics, face biometrics with two cameras or two fingerprints, have improved accuracy and a lower error rate at the expense of a significantly slower processing speed and a rising price. Multimodal biometric verification systems produce identical

TABLE 5. Comparative analysis of approaches.

Criteria	Contributions	Limitations
Zero Biometric	<ul style="list-style-type: none"> - Simple to use, as it only requires a physical card to be presented and verified. - Cost depends on the number of proctors and exam takers, as no additional hardware or software is required. 	<ul style="list-style-type: none"> - Vulnerable to fraud and errors, as cards can be lost, stolen, or duplicated, and there is no updated information on an exam taker. - Limited to one form of identification and a proctor-to-examinee ratio.
Face	<ul style="list-style-type: none"> - Non-intrusive and user-friendly, requiring only a camera to capture the image. - Can be used for real-time identification and verification with the quickest response time and lowest cost for unimodal recognition. 	<ul style="list-style-type: none"> - Is sensitive to focusing ranges, lighting conditions, facial expressions, and aging. - Requires capturing a clear image of the face, which is not always possible. - Face recognition with eyeglasses and face variations requires complex algorithms.
Finger	<ul style="list-style-type: none"> - Simply perform implementation and maintenance. - Non-intrusive and user-friendly, requiring only a fingerprint sensor to capture the image. - Capable of real-time identification and verification with the highest accuracy and lowest error rate for unimodal recognition. - Require fairly implementation and maintenance. 	<ul style="list-style-type: none"> - Finger and scanner can be affected by factors such as dryness, moisture, and dirt. - Requires capturing a clear fingerprint image, which is not always possible. - Fingerprint scanners for capturing and verifying must be identical.
Face + Finger	<ul style="list-style-type: none"> - Provides a higher level of security due to the use of multiple forms of identification. - Improve the accuracy of the identification and verification process at the lowest cost for multimodal recognition. - Adapt to unimodal recognition. 	<ul style="list-style-type: none"> - More complex and costly than using a single form of identification. - Subject to the same limitations as the individual face and fingerprint recognition methods. - Require an additional complicated implementation, recognition techniques, and maintenance.
Two Faces	<ul style="list-style-type: none"> - Provides a higher level of security due to the use of multiple forms of identification. - Multimodal recognition can achieve the highest level of identification and verification accuracy at the same cost as face and fingerprint recognition. - Support fault-tolerant cameras. 	<ul style="list-style-type: none"> - More complex and costly than using a single form of identification. - Subject to the same limitations as the individual face recognition methods. - Additional expenses for an additional camera, implementation, recognition techniques, and maintenance are necessary.
Two Fingers	<ul style="list-style-type: none"> - Provides a higher level of security, as it employs multiple forms of identification. - Increase the accuracy of the identification and verification process, as multimodal recognition has the lowest error rate. - Support fault-tolerant scanners. 	<ul style="list-style-type: none"> - More complicated and costly than using a single form of identification. - Subject to the same limitations as individual methods of finger recognition. - Require an additional scanner cost, implementation, recognition techniques, and maintenance.
Face then Finger	<ul style="list-style-type: none"> - Provides a higher level of security due to the use of multiple forms of identification. - Improve the accuracy of the identification and verification process with the quickest response time for semi-multimodal recognition. - Offer a quicker response time than multimodal recognition. 	<ul style="list-style-type: none"> - More complex and costly than using a single form of identification. - Subject to the same limitations as face and fingerprint recognition alone. - Require complex implementation, recognition techniques, and maintenance.
Finger then Face	<ul style="list-style-type: none"> - Provides a higher level of security due to the use of multiple forms of identification. - Improve the accuracy of the identification and verification process with the lowest error rate for semi-multimodal recognition. - Multimodal recognition is somewhat more expensive. 	<ul style="list-style-type: none"> - More complicated and costly than using a single form of identification. - Subject to the same limitations as fingerprint and face recognition methods. - Require complex implementation, recognition techniques, and maintenance.

results to semi-multimodal biometric verification systems. Thus, out of eight testing protocols, unimodal face recognition is an excellent factor for verifying the identity of exam candidates. These experimental results demonstrate that unimodal biometric technologies are superior to multimodal ones. However, the performance of the multimodal biometric approach in the IoT-based biometric system used to verify exam candidates is superior to that of the unimodal biometric approach. Regarding cost and processing time, it was determined that the performance of the unimodal biometric system was superior to that of the multimodal biometric method. In contrast, the multimodal biometric system has superior reliability.

Therefore, hypotheses H1 and H2 are accepted. The biometric quality scores of unimodal and multimodal face recognition systems indicate that unimodal face recognition is marginally superior to multimodal face recognition and finger recognition systems. Numerous researchers [47], [74] have confirmed the experimental findings that biometric verification techniques are more accurate, efficient, and stable than conventional methods.

Contrary to the results of this study, hypothesis H3 is rejected. A multimodal biometric system is more expensive than a unimodal system. Several studies have demonstrated that multimodal protocols are superior to unimodal protocols in terms of complex human verification and

security [75], [76], regarding those studies showing that multimodal protocols are superior to unimodal protocols. The multimodal biometric system is superior to the unimodal biometric system in terms of reliability criteria. Employing the IoT-based biometric system to verify exam candidates in educational institutions presents constructive challenges depending on the institution's existing systems. Some higher education institutions have extensive information and communication technology. Others, however, were unable to afford IoT-based biometric systems to verify exam candidates.

This research aims to not only compare the effectiveness of various unimodal and multimodal biometric technologies for identity verification systems of exam candidates but also to provide a methodology for developing an IoT-based biometric system used by higher education institutions to verify exam candidates. The biometric quality metric may employ a variety of criteria to implement the exam taker verification system in accordance with institution-specific requirements. Table 5 illustrates the comparative analysis of proposed identity verification methods based on this practical evaluation of IoT-based biometric recognition systems. Face + Finger, Two Faces, Two Fingers, and Face then Finger or Finger then Face approaches have the potential to increase the security of the identification and verification process, as indicated by the comparative results. However, they are more complex and costly than a single form of identification. In contrast, the single form of recognition is user-friendly, inexpensive, and susceptible to a few errors.

Nevertheless, the biometric quality metrics have demonstrated that unimodal, multimodal, and semi-multimodal biometric verifications depend on numerous factors, including accuracy, error rate, reliability, processing time, and cost.

Because the proposed factors are calculable, the unimodal approach to face recognition has the highest overall score compared with the alternatives. This study strongly suggests that contemporary universities should at least offer the unimodal biometric approach as an alternative to traditional methods of verifying the identity of exam-taking students.

VI. CONCLUSION

The IoT hardware, system development, and evaluation of the actual use of examination management and identity verification for exam candidates in education were among the most significant findings of this empirical study. Utilizing face and fingerprint biometric devices, an IoT-based biometric verification system has been developed to facilitate the collection, storage, detection, and verification of student information, including examination details, identification, identity, and biometric data. The proposed system design and development can recognize test-takers identities without identification documents using multiple biometric recognition techniques. In addition, this study describes different algorithms for IoT-based biometric verification of exam takers. A novel biometric quality metric is proposed for scoring biometric exam taker verification systems based on ISO/IEC 25000

and software quality models. By investigating and evaluating the biometric quality metric in the IoT-based biometric verification system, the findings of this study could have a direct impact on whether biometric technologies are used in education. Using the proposed architecture and system, this study compared the biometric technologies of unimodal, semi-multimodal, and multimodal approaches for recognizing exam-takers identities. Using the biometric quality metric to compare a combination of traditional proctoring and several biometric verification protocols, the effectiveness and efficiency criteria are defined as accuracy rate, error rate, processing time, and cost.

The results revealed that the two-fingers multimodal biometric system had the highest average accuracy of 96.67 percent and the lowest error rate of 1.9 percent. The traditional proctoring system, known as a zero biometric system, had the lowest average accuracy of 66.67 percent, resulting in the highest average error rate of 21.29 percent. With an average processing time of 2.49 seconds, the face unimodal biometric system was the most responsive, while the traditional proctoring system was the least responsive. The face unimodal biometric system had the lowest estimated cost for a 3-hour examination class at \$4.56, while the conventional proctoring system had the highest estimated cost at \$34.29.

To summarize the optimal IoT-based biometric systems, the triangular law was used to reformat the results of all system testing comparisons. The findings indicated that the unimodal face biometric is the most effective scoring system. The multimodal face and fingerprint biometric system, the multimodal fingerprint biometric system with two scanners, and the semi-multimodal face then fingerprint biometric system received the second-highest scores. The two-camera, multimodal face biometric system received the third-highest score.

A biometric system based on the Internet of Things promises to verify exam candidates accurately and could replace the traditional proctoring method for student identity verification. In addressing the research hypothesis, the evaluation results of the quality metrics demonstrate that unimodal, multimodal, and semi-multimodal biometric verification systems outperform the conventional proctoring system in terms of reliability, validity, processing time, and investment. In education, the unimodal face biometric system exhibited the highest overall system quality for examiner identity verification.

This study has several implications and applications. The findings enable educational institutions to more effectively use biometric technologies for the identity verification of exam takers by selecting a biometric technology suited to their objectives. Comparing the outcomes of various biometric technologies aided organizations in determining their preferred trade-offs between the number of resources and the consideration factors of desired accuracy, error rate, processing time, and cost to meet requirements. This research not only conserves time, resources, risk, and investment

but also demonstrates a greater understanding of biometric recognition for identity verification to reduce application failures. In addition, the results of this study can serve as recommendations for implementing biometric technologies in educational settings.

The study of an IoT-based biometric verification system demonstrates the proposed design and development, compares various biometric techniques, and determines the efficacy and efficiency of each biometric technique. This study has some limitations that can be addressed in future studies, including system development (hardware and software), user behavioral intentions (sociodemographic factors), and biometric quality metrics for varying biometric recognition. This study is based on Raspberry Pi 4, biometric devices, OpenCV, and wireless networks, whereas other researchers may use different hardware, software libraries, implementation strategies, and networks. Thus, future development systems should investigate the effects of changes. In addition, it is necessary to validate and analyze the impact of technology acceptance factors on user perceptions of actual system use. In addition, the biometric quality metric can be adapted to support additional biometric recognition.

REFERENCES

- [1] M. Rukhiran, N. Phaokla, and P. Netinant, "Adoption of environmental information chatbot services based on the Internet of Educational things in smart schools: Structural equation modeling approach," *Sustainability*, vol. 14, no. 23, p. 15621, Nov. 2022, doi: [10.3390/su142315621](https://doi.org/10.3390/su142315621).
- [2] D. Shah and V. Haradi, "IoT based biometrics implementation on Raspberry Pi," *Procedia Comput. Sci.*, vol. 79, pp. 328–336, 2016, doi: [10.1016/j.procs.2016.03.043](https://doi.org/10.1016/j.procs.2016.03.043).
- [3] M. Rukhiran and P. Netinant, "IoT architecture based on information flow diagram for vermiculture smart farming kit," *TEM J.*, vol. 9, no. 4, pp. 1330–1337, Nov. 2020, doi: [10.18421/TEM94-03](https://doi.org/10.18421/TEM94-03).
- [4] A. George, A. Ravindran, M. Mendieta, and H. Tabkhi, "MEZ: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge," *IEEE Access*, vol. 9, pp. 21457–21473, 2021, doi: [10.1109/ACCESS.2021.3055775](https://doi.org/10.1109/ACCESS.2021.3055775).
- [5] S. Taheri and J.-S. Yuan, "A cross-layer biometric recognition system for mobile IoT devices," *Electronics*, vol. 7, no. 2, p. 26, Feb. 2018, doi: [10.3390/electronics7020026](https://doi.org/10.3390/electronics7020026).
- [6] P. Bellmann, P. Thiam, and F. Schwenker, "Person identification based on physiological signals: Conditions and risks," in *Proc. ICPRAM*, Valletta, Malta, 2020, pp. 373–380, doi: [10.5220/0008865503730380](https://doi.org/10.5220/0008865503730380).
- [7] A. Phokajang and P. Netinant, "Developing software architecture for a smart school digital framework," in *Proc. ICSIM*, Yokohama, Japan, 2021, pp. 22–27, doi: [10.1145/3451471.3451475](https://doi.org/10.1145/3451471.3451475).
- [8] R. A. Hamid, U. A. Mokhtar, M. M. Yusof, and A. Warland, "Electronic records management in schools: The case study of school examination analysis system," *J. Pengurusan*, vol. 57, pp. 142–154, May 2019, doi: [10.17576/pengurusan-2019-57-10](https://doi.org/10.17576/pengurusan-2019-57-10).
- [9] O. A. Abass, S. A. Olajide, and B. O. Samuel, "Development of web-based examination system using open source programming model," *Turk. Online J. Distance Educ.*, vol. 18, no. 2, pp. 30–42, 2017, doi: [10.17718/TOJDE.306555](https://doi.org/10.17718/TOJDE.306555).
- [10] C. Bohmer, N. Feldmann, and M. Ibsen, "E-exams in engineering education—Online testing of engineering competencies: Experiences and lessons learned," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Santa Cruz de Tenerife, Spain, Apr. 2018, pp. 571–576, doi: [10.1109/educon.2018.8363281](https://doi.org/10.1109/educon.2018.8363281).
- [11] M. R. Hameed and F. A. Abdullatif, "Online examination system," *JARJSET*, vol. 4, no. 3, pp. 106–110, Mar. 2017, doi: [10.17148/iarjset.2017.4.321](https://doi.org/10.17148/iarjset.2017.4.321).
- [12] M. Rukhiran, S. Buarong, and P. Netinant, "Software development for educational information services using multilayering semantics adaptation," *Int. J. Service Sci., Manage., Eng., Technol.*, vol. 13, no. 1, pp. 1–27, Sep. 2022, doi: [10.4018/IJSSMET.307153](https://doi.org/10.4018/IJSSMET.307153).
- [13] V. S. Shamsi, "A survey paper on fingerprint recognition and cross matching," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 7, no. 5, pp. 573–575, May 2019, doi: [10.22214/ijraset.2019.5096](https://doi.org/10.22214/ijraset.2019.5096).
- [14] Y. Kortli, M. Jridi, A. A. Falou, and M. Atri, "Face recognition systems: A survey," *Sensors*, vol. 20, no. 2, p. 342, Jan. 2020, doi: [10.3390/s20020342](https://doi.org/10.3390/s20020342).
- [15] T. Kalisky, S. Saggese, Y. Zhao, D. Johnson, M. Azarova, L. E. Duarte-Vera, L. A. Almada-Salazar, D. Perales-Gonzalez, E. Chacon-Cruz, J. Wang, R. Graham, A. Hubenko, D. A. Hal, and E. Aronoff-Spencer, "Biometric recognition of newborns and young children for vaccinations and health care: A non-randomized prospective clinical trial," *Sci. Rep.*, vol. 12, Dec. 2022, Art. no. 22520, doi: [10.1038/s41598-022-25986-6](https://doi.org/10.1038/s41598-022-25986-6).
- [16] L. Y. Yugai, "The use of biometric identification in countering crime," *Berlin Stud. Transnational J. Sci. Humanities.*, vol. 2, nos. 1–4, pp. 3–14, 2022, doi: [10.5281/zenodo.5831922](https://doi.org/10.5281/zenodo.5831922).
- [17] J. Zywolek, A. Sarkar, and M. S. Sial, "Biometrics as a method of employee control," in *Proc. IMCOM*, Seoul, South Korea, 2022, pp. 1–5, doi: [10.1109/IMCOM53663.2022.9721809](https://doi.org/10.1109/IMCOM53663.2022.9721809).
- [18] M. A. Hossain and M. A. Al Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *Int. J. Comput. Appl.*, vol. 44, no. 5, pp. 455–464, May 2022, doi: [10.1080/1206212X.2020.1809177](https://doi.org/10.1080/1206212X.2020.1809177).
- [19] M. Zhang and Q. Luo, "A systematic literature review on the influence mechanism of digital finance on high quality economic development," *J. Risk Anal. Crisis Response*, vol. 12, no. 1, pp. 45–54, Apr. 2022, doi: [10.54560/jracr.v12i1.321](https://doi.org/10.54560/jracr.v12i1.321).
- [20] O. Tomohide, I. Kazuo, I. Atsushi, T. Satoshi, H. Noriyuki, and T. Risa, "Fast travel: Using face recognition to improve airport services with a view towards wide scale implementation," *Intell. Logistics Mobility*, vol. 15, no. 1, pp. 52–56, Jan. 2021.
- [21] A. Karagianni and V. Papakonstantinou, "Surveillance in schools across Europe: A new phenomenon in light of the COVID-19 pandemic? The cases of Greece and France," *Eur. J. Educ. Res.*, vol. 11, no. 2, pp. 1219–1229, Apr. 2022, doi: [10.12973/eu-jeer.11.2.1219](https://doi.org/10.12973/eu-jeer.11.2.1219).
- [22] K. N. Goud and K. Sindhuri, "Enhanced security for smart door using biometrics and OTP," in *Studies in Computational Intelligence*. Cham, Switzerland: Springer, 2022, pp. 517–526, doi: [10.1007/978-3-030-96634-8_47](https://doi.org/10.1007/978-3-030-96634-8_47).
- [23] I. Anikin and E. Anisimova, "Framework for biometric user authentication based on a dynamic handwritten signature," in *Cyber-Physical Systems: Intelligent Models and Algorithms*, vol. 417. Cham, Switzerland: Springer, 2022, pp. 219–231, doi: [10.1007/978-3-030-95116-0_18](https://doi.org/10.1007/978-3-030-95116-0_18).
- [24] N. M. Raharja, M. A. Fathansyah, and A. N. N. Chamim, "Vehicle parking security system with face recognition detection based on eigenface algorithm," *J. Robot. Control*, vol. 3, no. 1, pp. 78–85, Oct. 2021, doi: [10.18196/jrc.v3i1.12681](https://doi.org/10.18196/jrc.v3i1.12681).
- [25] O. Shlyakhetko, A. Braibant, E. Czechowska, M. Fryczka, and R. Hadrach, "IoT project: Smart parking," in *Developments in Information & Knowledge Management for Business Applications*, vol. 42. Cham, Switzerland: Springer, 2022, pp. 37–58, doi: [10.1007/978-3-030-95813-8_2](https://doi.org/10.1007/978-3-030-95813-8_2).
- [26] V. Singh and C. Kant, "Biometric-based authentication in Internet of Things (IoT): A review," *Adv. Inf. Commun. Technol. Comput.*, vol. 392, pp. 309–317, May 2022, doi: [10.1007/978-981-19-0619-0_27](https://doi.org/10.1007/978-981-19-0619-0_27).
- [27] L. Calderoni and A. Magnani, "The impact of face image compression in future generation electronic identity documents," *Forensic Sci. International, Digit. Invest.*, vol. 40, Mar. 2022, Art. no. 301345, doi: [10.1016/j.fsidi.2022.301345](https://doi.org/10.1016/j.fsidi.2022.301345).
- [28] R. Srivastava, D. Singh, R. Tomar, and Sarishma, "Three-layer multimodal biometric fusion using SIFT and SURF descriptors for improved accuracy of authentication of human identity," in *EAI/Springer Innovations in Communication and Computing*. Cham, Switzerland: Springer, 2022, pp. 119–142, doi: [10.1007/978-3-030-78284-9_6](https://doi.org/10.1007/978-3-030-78284-9_6).
- [29] M. A. Khan, I. Ud Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "G-RAT | a novel graphical randomized authentication technique for consumer smart devices," *IEEE Trans. Consum. Electron.*, vol. 65, no. 2, pp. 215–223, May 2019, doi: [10.1109/TCE.2019.2895715](https://doi.org/10.1109/TCE.2019.2895715).
- [30] A. A. Ahmed, "Future effects and impacts of biometrics integrations on everyday living," *Al-Mustansiriyah J. Sci.*, vol. 29, no. 3, pp. 139–144, Mar. 2019, doi: [10.23851/mjs.v29i3.642](https://doi.org/10.23851/mjs.v29i3.642).

- [31] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," *J. Inf. Secur. Appl.*, vol. 37, pp. 28–37, Dec. 2017, doi: [10.1016/j.jisa.2017.10.002](https://doi.org/10.1016/j.jisa.2017.10.002).
- [32] U. Gawande and Y. Golhar, "Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques," *Int. J. Biometrics*, vol. 10, no. 2, pp. 142–175, 2018, doi: [10.1504/ijbm.2018.091629](https://doi.org/10.1504/ijbm.2018.091629).
- [33] K. Nguyen, C. Fookes, S. Sridharan, M. Tistarelli, and M. Nixon, "Super-resolution for biometrics: A comprehensive survey," *Pattern Recognit.*, vol. 78, pp. 23–42, Jun. 2018, doi: [10.1016/j.patcog.2018.01.002](https://doi.org/10.1016/j.patcog.2018.01.002).
- [34] S. Dass, M. Sadrulhuda, N. Pasha, N. Nayan, and J. S. Nayak, "Real time face recognition using raspberry Pi," *Int. J. Comput. Appl.*, vol. 176, no. 33, pp. 1–4, Jun. 2020, doi: [10.5120/ijca.2020920387](https://doi.org/10.5120/ijca.2020920387).
- [35] Y. Zhao, J. Xu, J. Wu, J. Hao, and H. Qian, "Enhancing camera-based multimodal indoor localization with device-free movement measurement using WiFi," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1024–1038, Feb. 2020, doi: [10.1109/jiot.2019.2948605](https://doi.org/10.1109/jiot.2019.2948605).
- [36] S. Yadav and V. P. Vishwakarma, "Extended interval type-II and kernel based sparse representation method for face recognition," *Exp. Syst. Appl.*, vol. 116, pp. 265–274, Feb. 2019, doi: [10.1016/j.eswa.2018.09.032](https://doi.org/10.1016/j.eswa.2018.09.032).
- [37] M. Kas, Y. El Merabet, Y. Ruichek, and R. Messoussi, "Mixed neighborhood topology cross decoded patterns for image-based face recognition," *Exp. Syst. Appl.*, vol. 114, pp. 119–142, Dec. 2018, doi: [10.1016/j.eswa.2018.07.035](https://doi.org/10.1016/j.eswa.2018.07.035).
- [38] Y. Yaddaden, M. Adda, A. Bouzouane, S. Gaboury, and B. Bouchard, "User action and facial expression recognition for error detection system in an ambient assisted environment," *Exp. Syst. Appl.*, vol. 112, pp. 173–189, Dec. 2018, doi: [10.1016/j.eswa.2018.06.033](https://doi.org/10.1016/j.eswa.2018.06.033).
- [39] S. Awojide, O. S. Awe, and T. S. Babatope, "Biometric fingerprint system using an online based pattern recognition for candidates authentication in Nigeria institution examinations. The design perspective," *Int. J. Sci. Eng. Res.*, vol. 9, no. 5, pp. 1680–1694, May 2018, doi: [10.14299/ijser.2018.05.02](https://doi.org/10.14299/ijser.2018.05.02).
- [40] M. Taileb and S. Arabia, "Design and implementation of RFID and fingerprint-based student verification system," *Int. J. Recent Technol. Eng.*, vol. 8, no. 5, pp. 2084–2092, Jan. 2020, doi: [10.35940/ijrte.e5788.018520](https://doi.org/10.35940/ijrte.e5788.018520).
- [41] F. D. Tatar, "Fingerprint recognition algorithm," in *Proc. Comput. Sci. Inf. Syst.*, 2017, pp. 85–100, doi: [10.5121/csit.2017.70609](https://doi.org/10.5121/csit.2017.70609).
- [42] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018, doi: [10.1016/j.patcog.2018.01.026](https://doi.org/10.1016/j.patcog.2018.01.026).
- [43] X. Xi, L. Yang, and Y. Yin, "Learning discriminative binary codes for finger vein recognition," *Pattern Recognit.*, vol. 66, pp. 26–33, Jun. 2017, doi: [10.1016/j.patcog.2016.11.002](https://doi.org/10.1016/j.patcog.2016.11.002).
- [44] E. Noma-Osaghae, R. Okonigene, C. Okereke, O. J. Okesola, and K. O. Okokpujie, "Design and implementation of an Iris biometric door access control system," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, NV, USA, 2017, pp. 590–593, doi: [10.1109/csci.2017.102](https://doi.org/10.1109/csci.2017.102).
- [45] E. Emmanuel and O. T. Ogadimma, "A biometric authentication approach to examination conduct in Nigerian universities," *Int. J. Innov. Res. Sci., Eng. Technol.*, vol. 8, no. 3, pp. 2176–2182, Mar. 2019.
- [46] G. M. Mir, A. A. Balkhi, N. A. Lala, N. A. Sofi, M. M. Kirmani, I. A. Mir, and H. A. Hamid, "The benefits of implementation of biometric attendance system," *Oriental J. Comput. Sci. Technol.*, vol. 11, no. 1, pp. 50–54, Mar. 2018, doi: [10.13005/ojst.11.01.09](https://doi.org/10.13005/ojst.11.01.09).
- [47] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017, doi: [10.1016/j.patcog.2017.01.024](https://doi.org/10.1016/j.patcog.2017.01.024).
- [48] G. S. Walia, T. Singh, K. Singh, and N. Verma, "Robust multimodal biometric system based on optimal score level fusion model," *Exp. Syst. Appl.*, vol. 116, pp. 364–376, Feb. 2019, doi: [10.1016/j.eswa.2018.08.036](https://doi.org/10.1016/j.eswa.2018.08.036).
- [49] B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, "Face-iris multimodal biometric identification system," *Electronics*, vol. 9, no. 1, p. 85, Jan. 2020, doi: [10.3390/electronics9010085](https://doi.org/10.3390/electronics9010085).
- [50] K. Gunasekaran, J. Raja, and R. Pitchai, "Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images," *Automatika*, vol. 60, no. 3, pp. 253–265, Jul. 2019, doi: [10.1080/00051144.2019.1565681](https://doi.org/10.1080/00051144.2019.1565681).
- [51] M. Rukhiran, P. Netinant, and T. Elrad, "Effecting of environmental conditions to accuracy rates of face recognition based on IoT solution," *J. Current Sci. Technol.*, vol. 10, no. 1, pp. 21–33, 2020, doi: [10.14456/jcst.2020.2](https://doi.org/10.14456/jcst.2020.2).
- [52] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous student authentication in e-learning platforms," *Pattern Recognit. Lett.*, vol. 113, pp. 83–92, Oct. 2018, doi: [10.1016/j.patrec.2017.03.027](https://doi.org/10.1016/j.patrec.2017.03.027).
- [53] I. Traore, Y. Nakkabi, S. Saad, B. Sayed, J. D. Ardigo, and P. M. Quinan, "Ensuring online exam integrity through continuous biometric authentication," in *Information Security Practices*. Cham, Switzerland: Springer, 2017, pp. 73–81, doi: [10.1007/978-3-319-48947-6_6](https://doi.org/10.1007/978-3-319-48947-6_6).
- [54] I. B. Ahmed, M. A. Mohamed, and A. M. Noma, "A framework for secure online exam using biometric fingerprint and steganography techniques," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 32–35, 2018, doi: [10.14419/ijet.v7i3.28.20961](https://doi.org/10.14419/ijet.v7i3.28.20961).
- [55] K. O. Okokpujie, E. Noma-Osaghae, O. J. Okesola, S. N. John, and O. Robert, "Design and implementation of a student attendance system using iris biometric recognition," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, NV, USA, 2017, pp. 563–567, doi: [10.1109/csci.2017.96](https://doi.org/10.1109/csci.2017.96).
- [56] S. Wong-In and P. Netinant, "Revised software model design for biometric examiner personal verification system," in *Proc. ICIT*, Singapore, 2017, pp. 237–242, doi: [10.1145/3176653.3176678](https://doi.org/10.1145/3176653.3176678).
- [57] M. Moradi, M. Moradkhani, and M. B. Tavakoli, "Security-level improvement of IoT-based systems using biometric features," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–15, Feb. 2022, doi: [10.1155/2022/8051905](https://doi.org/10.1155/2022/8051905).
- [58] K. Pearson, "On lines and planes of closest fit to systems of points in space," *Philos. Mag.*, vol. 2, no. 6, pp. 559–572, 1901.
- [59] H. Hotelling, "Analysis of a complex of statistical variables into principal components," *J. Educ. Psychol.*, vol. 24, no. 6, pp. 417–441, Sep. 1933, doi: [10.1037/h0071325](https://doi.org/10.1037/h0071325).
- [60] M. M. Ahsan, Y. Li, J. Zhang, M. T. Ahad, and K. D. Gupta, "Evaluating the performance of eigenface, fisherface, and local binary pattern histogram-based facial recognition methods under various weather conditions," *Technologies*, vol. 9, no. 2, p. 31, Apr. 2021, doi: [10.3390/technologies9020031](https://doi.org/10.3390/technologies9020031).
- [61] A. Dube, D. Singh, R. K. Asthana, and G. S. Walia, "A framework for evaluation of biometric based authentication system," in *Proc. ICISS*, Thoothukudi, India, 2020, pp. 925–932, doi: [10.1109/iciss49785.2020.9315933](https://doi.org/10.1109/iciss49785.2020.9315933).
- [62] A. Kanak and I. Sogukpinar, "BioTAM: A technology acceptance model for biometric authentication systems," *IET Biometrics*, vol. 6, no. 6, pp. 457–467, Nov. 2017, doi: [10.1049/iet-bmt.2016.0148](https://doi.org/10.1049/iet-bmt.2016.0148).
- [63] Y. Zhou, "Evaluation of biometric recognition in the COVID-19 period," in *Proc. 2nd Int. Conf. Comput. Data Sci. (CDS)*, Stanford, CA, USA, Jan. 2021, pp. 243–248, doi: [10.1109/cds52072.2021.00049](https://doi.org/10.1109/cds52072.2021.00049).
- [64] J. Oh, U. Lee, and K. Lee, "Usability evaluation model for biometric system considering privacy concern based on MCDM model," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Mar. 2019, doi: [10.1155/2019/8715264](https://doi.org/10.1155/2019/8715264).
- [65] W. R. Malatji, R. Eck, and T. Zuva, "Acceptance of biometric authentication security technology on mobile devices," in *Proc. IMITEC*, Kimberley, South Africa, 2020, pp. 1–5, doi: [10.1109/imitec50163.2020.9334082](https://doi.org/10.1109/imitec50163.2020.9334082).
- [66] S. Siddique, M. Yasmin, T. B. Taher, and M. Alam, "The reliability and acceptance of biometric system in Bangladesh: Users perspective," *Int. J. Comput. Trends Technol.*, vol. 69, no. 6, pp. 1–6, Jun. 2021, doi: [10.14445/22312803/ijctt-v69i6p103](https://doi.org/10.14445/22312803/ijctt-v69i6p103).
- [67] M. El-Abed, C. Charrier, and C. Rosenberger, "Evaluation of biometric systems," in *New Trends and Developments in Biometrics*, vol. 7. London, U.K.: IntechOpen, 2012, pp. 149–169, doi: [10.5772/52084](https://doi.org/10.5772/52084).
- [68] *IEEE Standard for Information Technology—Systems Design—Software Design Descriptions*, Standard IEEE 1016-2009, 2009, doi: [10.1109/IEEESTD.2009.5167255](https://doi.org/10.1109/IEEESTD.2009.5167255).
- [69] *Systems and Software Engineering—Systems and Software Quality Requirements and Evaluation (SQuaRE)—Guide to SQuaRE*, Standards ISO/IEC 25000, 2014.
- [70] P. Kumari and P. Thangaraj, "A fast feature selection technique in multi modal biometrics using cloud framework," *Microprocessors Microsystems*, vol. 79, Nov. 2020, Art. no. 103277, doi: [10.1016/j.micpro.2020.103277](https://doi.org/10.1016/j.micpro.2020.103277).

- [71] A. Alshbtat, N. Zanoon, and M. Alfraheed, "A novel secure fingerprint-based authentication system for student's examination system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 515–519, 2019, doi: [10.14569/IJACSA.2019.0100968](https://doi.org/10.14569/IJACSA.2019.0100968).
- [72] M. Rukhiran, S. Pukdesree, and P. Netinant, "Development and evaluation of biometric authentication system based on facial and voice recognition," *ICIC Exp. Lett.*, vol. 16, no. 10, pp. 1027–1035, Oct. 2022, doi: [10.24507/icicel.16.10.1027](https://doi.org/10.24507/icicel.16.10.1027).
- [73] R. Pi. *MTBF Values of the Revolution Pi Modules*. Jan. 14, 2021. [Online]. Available: <https://revolutionpi.com/mtbf-revolution-pi-modules>
- [74] Y. Chen, J. Yang, C. Wang, and D. Park, "Variational Bayesian extreme learning machine," *Neural Comput. Appl.*, vol. 27, no. 1, pp. 185–196, Jan. 2016, doi: [10.1007/s00521-014-1710-1](https://doi.org/10.1007/s00521-014-1710-1).
- [75] A. S. Raju and V. Udayashankara, "A survey on unimodal, multimodal biometrics and its fusion techniques," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 689–695, 2018, doi: [10.14419/ijet.v7i4.36.24224](https://doi.org/10.14419/ijet.v7i4.36.24224).
- [76] S. Poria, N. Majumder, R. Mihalcea, and E. Hovy, "Emotion recognition in conversation: Research challenges, datasets, and recent advances," *IEEE Access*, vol. 7, pp. 100943–100953, 2019, doi: [10.1109/ACCESS.2019.2929050](https://doi.org/10.1109/ACCESS.2019.2929050).



MEENNAPA RUKHIRAN received the B.Sc. degree in computer information systems from Burapha University, Thailand, in 2006, and the M.S. degree in information technology management and the Ph.D. degree in information technology from Rangsit University, Thailand, in 2014 and 2020, respectively. She is currently an Assistant Professor of information technology with the Faculty of Social Technology, Rajamangala University of Technology Tawan-ok, Chanthaburi, Thailand. Her research interests include multidimensional software design, system software framework, technology acceptance models, the Internet of Things, aspect orientation, information systems with chatbots, web-based development, mobile development, implementation, data mining, and theory of computation.



SETHAPONG WONG-IN received the B.S. degree in applied statistics from the King Mongkut's University of Technology North Bangkok, Thailand, in 1997, and the M.S. degree in information technology from the King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 2000. He is currently pursuing the Ph.D. degree in information technology with Rangsit University, Pathum Thani, Thailand. He is also an Assistant Professor of information technology with Valaya Rajabhat University, Pathum Thani. His current research interests include software design, biometrics, the Internet of Things, data analysis, and software engineering.



PANITI NETINANT received the B.S. degree (Hons.) in computer science from Bangkok University, Thailand, in 1994, and the M.S. and Ph.D. degrees in computer science from the Illinois Institute of Technology, Chicago, IL, USA, in 1996 and 2001, respectively. He is currently an Associate Professor of computer science of the doctoral program in information technology and an Associate Dean with the Graduate School, Rangsit University, Thailand, where he is responsible for information technology and international affairs. His research interests include adaptive software architecture, operating systems, bot information systems, mobile development, the Internet of Things, compilers, object-oriented approach, aspect-oriented approach, and cloud computing services. He is a member of the international technical committee and a reviewer of IEEE and ACM conference papers.

...