International Journal of Information Technology and Web Engineering
Volume 17 • Issue 1

Biometric Cloud Services for Web-Based Examinations:
An Empirical Approach

Meennapa Rukhiran, Rajamangala University of Technology Tawan-OK, Thailand.
https://orcid.org/0000-0002-3880-8991

Sorapak Pukdesree, Rangsit University, Thailand

Paniti Netinant, Rangsit University, Thailand*
https://orcid.org/0000-0001-8376-0440

ABSTRACT

Biometric recognition may be used in conjunction with human authentication on a smartphone to improve accuracy, reliability, and simplicity, and to aid in fraud prevention and user authentication. While single biometric authentication addresses environmental degradation and sensor noise limitations, and the single point of failure scenario in biometric systems can result in more robust biometric systems, multimodal biometric authentication can improve the accuracy of identification and recognition. The purpose of this research is to propose a facial and speech authentication system that is cloud-based and supports a web-based examination approach. The system enables students' biometrics to be registered, students to be recognized, and student recognition results to be reported. The confusion matrix is used to compare the results of positive and negative detection in various ways, including accuracy score, precision value, and recall value. Adaptive multimodal biometric authentication should be designed and evaluated for further research using the optimal weights for each biometric.

KEYWORDS

Authentication, Cloud Services, Face Recognition, Multimodal Biometric, Speech Recognition

INTRODUCTION

The mobile revolution has resulted in the development of portable and convenient data manipulation and data transfer devices. Authentication is a well-known method of securing a user's access to services. Unlocking devices, authorizing transactions, and verifying users' signatures are all examples of authentication services (Wojtowicz & Joachimiak, 2016). For both service providers and users, the traditional authentication method prioritizes using a username and password (Czeskis et al., 2012). However, physical characteristics combined with one or more biometrics allow for the precise identification of an individual user (Casanova et al., 2021). Biometric recognition utilizes user

DOI: 10.4018/IJITWE.299022 *Corresponding Author

characteristics such as hands, eyes, faces, mouth, fingerprints, and ears to identify users automatically. The unimodal biometric system's limitations include a lack of data, low accuracy, and vulnerability to attack.

Biometric authentication is defined as the process of automatically recognizing physiological characteristics to provide secure identification and verification solutions (Selwal et al., 2016). Five modules comprise the biometric system: 1) a multi-sensor system collects primary biometric data, 2) a preprocessor for the necessary feature extractor methods, 3) templates generate patterns for biometric extracts, 4) decision fusion reconciles disparate patterns, and 5) identifying and authorizing the results by matching the input and enrolled patterns (Yadav et al., 2011). The multimodal biometric system expands the number of biometric inputs from users to more than two, allowing for more reliable authentication. Multiple physical characteristics can be used to authenticate users. Multimodal biometrics integrates and improves user recognition with increased accuracy, security, reliability (Purohit & Ajmera, 2021), and fault tolerance (Khoo et al., 2018), as well as consolidating data. The multimodal biometric system requires multiple parallel systems to detect the same or distinct biometric features at various layers (Smith & Brooks, 2013). Human physiological biometrics have been studied practically in a variety of areas using multimodal biometric systems, including parallel feature fusion of periocular biometrics and touch (Casanova et al., 2021), unequal feature portions of faces and fingerprints (Yang et al., 2019), and novel techniques and algorithms for palm, fingerprint, and ear recognition (Purohit & Ajmera, 2021).

Pukdesree and Netinant (2016) proposed a biometric authentication conceptual framework and developed a cloud-based biometric authentication service; thus, the entire process of data input, processing, and output can express the multimodal biometric authentication layering architecture. The framework provided a layered design for the client, application, and cloud database. The actual authentication system is still being developed and evaluated. While biometric authentication has evolved to incorporate multiple physiological biometrics with the possibility of a single point of failure, the multimodal biometric authentication system built on this framework can be enhanced by adding a security access system to protect fraud detection services.

This paper proposes a design and implementation of multimodal biometric cloud services for authentication of web-based examinations to bridge the gap between face and voice recognition multimodal biometric applications. During the coronavirus (COVID-19) pandemic, students could verify their identities and access the exam scheduling system. The system is unburdened within acceptable responsiveness scores to exam schedules, and the system was replaced with more flexible and superior securities. A confusion matrix is used to compare nonmembers and members who have registered for the examination system. The system outcomes from this biometric authentication research can be used to define system requirements and development scopes, as well as improve the reliability and accuracy of practical web-based applications.

RELATED WORK

Errattahia et al. (2018) reviewed the methods for detecting and correcting automatic speech recognition (ASR) errors. The researchers concentrated on ASR error correction, which resulted in increased efficiency, usability, and robustness. Bah and Ming (2020) proposed a novel method for improving the precision of face recognition systems by combining the Local Binary Pattern algorithm with various image processing techniques, such as contrast, brightness, or histogram equalization. These techniques can also help improve the accuracy, reliability, and robustness of the face recognition system. According to Shakil et al. (2021), patient information is extremely valuable and should be stored, accessed, and managed with the utmost care. The researchers proposed behavioral biometric authentication via a cloud-based system based on signatures. Mason et al. (2020) reported that biometric technology adoption in the healthcare industry is accelerating. They proposed an approach

for digesting the individual patient by combining periocular biometrics and the patient index in healthcare information systems.

A single-modal biometric system has limitations, and each method has a rating based on the seven values proposed by Jain and Ross. Each biometric modality also has limitations due to environmental degradation, sensor noise, and so on. Multimodal biometrics combine multiple biometric modalities, addressing the single point of failure scenario in biometric systems and resulting in more robust biometric systems. Their multimodal biometric was a combination of speech and face. Naidu and Babu (2018) presented a multimodal biometric recognition system that utilizes face, finger, and voice recognition biometrics. When compared to existing single biometric identification systems, the system provided increased security. The results incorporated these characteristics via score-level fusion. Choudhury et al. (2021) proposed an adaptive rank-level biometric merging framework. To ensure optimal performance, the rank-level merging was implemented using the ant colony optimization technique. The article utilized the multimodal biometric by extracting three fingernail plates from the index, middle, and ring fingers. AlexNet, ResNet-18, and DenseNet-201 algorithms are used to extract these three nail plates.

Fei et al. (2021) proposed using the joint multi-instance hand-based biometric feature for biometric recognition. The researchers used preliminary aspect data derived from multiple biometric image instances. The extracted features of multi-instance biometric characteristics and the collaborative demonstrations of multi-instance biometric characteristics are thus combined to produce the final ordinary. Sarier (2021) proposed multimodal biometric authentication for mobile edge computing (MBA-MEC), a multimodal biometric authentication technique based on mobile technology. MBA-MEC is a new multimodal system that defends against invaders by utilizing the secure protocol of privacy-preserving biometric authentication (PPBA). MBA-MEC matching is carried out exhaustively in an encrypted format, and then the finalized merged matching score is hidden from other computers. Kumari and Thangaraj (2020) proposed a cloud-based system framework for rapid feature selection in multimodal biometrics. These biometric compounds of facial and fingerprint recognition are multimodal in nature. The proposed technique for feature selection uses ant colony optimization. Particle swarm optimization is used for feature extraction and classification processes.

Chang et al. (2021) proposed a biocryptosystem level fusion framework known as BIOFUSE, a multimodal biometric fusion framework that combines fuzzy commitment and fuzzy vault. These techniques were used to create an encryption pattern that preserves the format. This framework makes it extremely difficult for an attacker to gain unauthorized access to the system without simulating all of the genuine user's biometric inputs. Vijay and Indumathi (2021) proposed a multimodal biometric consisting of three traits: iris, ear, and finger vein, the features of which are extracted using the BiComp masking method. The recognition score is then calculated for each of the three traits using a multi-support vector neural network (multi-SVNN) classifier.

A single modal biometric system can be improved by applying other methodologies. Kausar (2021) mentioned biometrics in healthcare to protect patients' private data. This biometric deploys an iris-based cancelable crypto system on a smart card. The patient's data is secured by deploying symmetric key cryptography, with healthcare data stored in an encrypted format on the smart card. Piciucco et al. (2021) proposed integrating biometric recognition and wearable devices to prevent unauthorized usage of these devices. This methodology uses the fusion of electrodermal activity (EDA) and blood volume pulse (BVP) spectrograms into MobileNet v2. The study also shows that biometric recognition can be integrated with wearable devices for identifying an authorized user.

Bisogni et al. (2021) proposed a novel secured biometric system for authorizing and signing blockchain transactions. This methodology uses face recognition as a biometric, encoded using a convolutional neural network, then the encoding is fused with the Rivest-Shamir-Adleman (RSA) key. The results show that the combined key can ensure authorizing in blockchain transactions with preserving the user's privacy. Brundhaelci et al. (2019) proposed face recognition on closed-circuit television (CCTV), also known as surveillance cameras, to detect and quickly respond to criminal

recognition and person tracking to reduce the crime rate. The project uses deep learning neural networks to detect and recognize criminals and person tracking. Cherifi et al. (2021) proposed a continuous and real-time authentication system by capturing the user's activation using the sensors of the smartphones (e.g., gyroscope or accelerometer) to gather the positions or the coordinates. The overall processes of continuous and real-time authentication provide the real-time user's activation, feature extraction, train the HMM model, and affirm the user's entity.

Falmari and Brindha (2021) proposed a new encrypted biometric-based approach that provides more security for the biometric authentication system. The biometric information may be stored on a remote storage server on the network. Therefore, biometric information may be stolen during send or pass on the network. This methodology encrypts the biometric information, such as images of the iris, face, or fingerprint, using a secure 256-bit hash algorithm before sending the biometric information onto the network. The encryption keys are generated from the biometric images. Consequently, it is difficult to get the encrypted key without the original biometric image.

Yang et al. (2019) proposed a feature-adaptive random projection-based approach. The projection is the matrix that is derived from the local feature gathering with the basic matrix. This projection matrix will be left after use to prevent the reuse of this projection matrix, making it more difficult to get into information stored in the projection matrix.

Saeed (2021) proposed a new approach that combines soft biometric features with conventional facial features. The soft biometric features are used to model the micro-expressions from the image. On the other hand, conventional facial features were used to model facial conformation. This approach can improve the facial recognition system by approximately five percent.

Stylios et al. (2021) proposed a continuous behavioral biometric authentication technique using mobile phones. This paper provides a diagnosis of the gathering and feature extraction methodology. This paper also shows the weakness of machine learning models in preventing defiant assaults and the related preventive measures. Behera et al. (2021) focus on the new concept of person re-identiðcation on the internet of biometrics things (IoBT), a biometric authentication system on cloud computing. The proposed system tracks the person‘s movement on multiple and different surveillance cameras, which can help to reduce the complexity of re-identiðcation on multiple and different surveillance cameras. In smart cities scenarios, the IoBT is more widely used with intelligent surveillance cameras, which produce more network traffic.

Ajish and AnilKumar (2021) proposed an election voting system using a biometric authentication that operated on a secured mobile application for voters. The system provides secure information while transporting data on a mobile network by encrypting the voter's image. The mobile application processes the encrypted image by extracting features and storing it as a biometric template, then sends the template to the server to process the next step. The encryption process uses a wavelet-based based on advanced encryption standard (AES) algorithm, which provides better performance than the other two algorithms.

Lee et al. (2021) presented one of the most intriguing biometric authentication systems ever proposed. The study introduced Biometric Database Authentication System (BDAS), a novel biometric authentication system based on blockchain technology. BDAS offers decentralized and distributed gimmicks such as blockchain-based biometric authentication and auditing. By comparing the BDAS to some other methodologies, the researchers demonstrate that it can provide a reliable and secure biometric mechanism authentication.

Kumar et al. (2021) proposed encrypting biometric templates in two stages. To begin, the group representation of biometric templates was decomposed using two-dimensional discrete wavelets. Finally, substitution and permutation were performed using the three-dimensional Lorenz-chaotic system. Each level of decomposition consumed the encryption process, while the decryption process occurred in reverse order. The experimental results indicate that the proposed methodology can enhance security while maintaining robustness against attackers.

Jia et al. (2021) concentrated on dorsal hand vein biometric authentication, which was referred to as an urgent need for biometric technology authentication. They comprehensively survey dorsal hand veins (DHV) biometrics. The article discusses the results of the DHV biometric processes, including data collection, database structure, preprocessing, feature extraction, matching, score fusions, and the future of DHV biometrics technology.

Lee and Jeong (2021) set out to create one of the most intriguing biometric authentication systems possible. The study introduces BDAS, a novel biometric authentication system based on blockchain technology. BDAS offers decentralized and distributed gimmicks such as blockchain-based biometric authentication and auditing. By comparing the BDAS to some other methodologies, the researchers demonstrate that it can provide a reliable and secure biometric mechanism authentication.

Srivastva et al. (2021) developed a biometric recognition system based on electrocardiogram data that represents the electrical activity of the heart via electrode devices placed on the individual's skin. The researchers created PlexNet, a stacking model, by fusing the results of four fine-tuned models. PlexNet is evaluated on the basis of two publicly available datasets. According to the experimental results, the proposed biometric recognition technique has an accuracy score of up to 99.66 percent. Additionally, this methodology is robust.

Cui et al. (2021) focused on the electrocardiogram as a method for human biometric recognition, noting that this method is difficult to counterfeit. The researchers collected electrocardiogram (ECG) data during both exercise and rest. The evaluations were performed on the ECG dataset using a variety of algorithms. They conclude that the evaluation results are satisfactory for the specified circumstances, even if they are not as robust as other experimental results obtained in a different environment.

Marquez et al. (2021) focused on the use of behavioral biometrics and infrared thermography to monitor dairy cow estrus in farms. This research develops an estrus alert system that can assist farmers in detecting their cows' estrus. The research issue is that low estrus rates are associated with prolonged calving duration, low economic profit, and cow longevity. The skin temperature of dairy cows is measured using infrared thermography, and the indicator of ovulation is determined by the disappearance of the dominant follicle. Liu et al. (2021) primarily concerned themselves with biometric authentication for wearable devices.

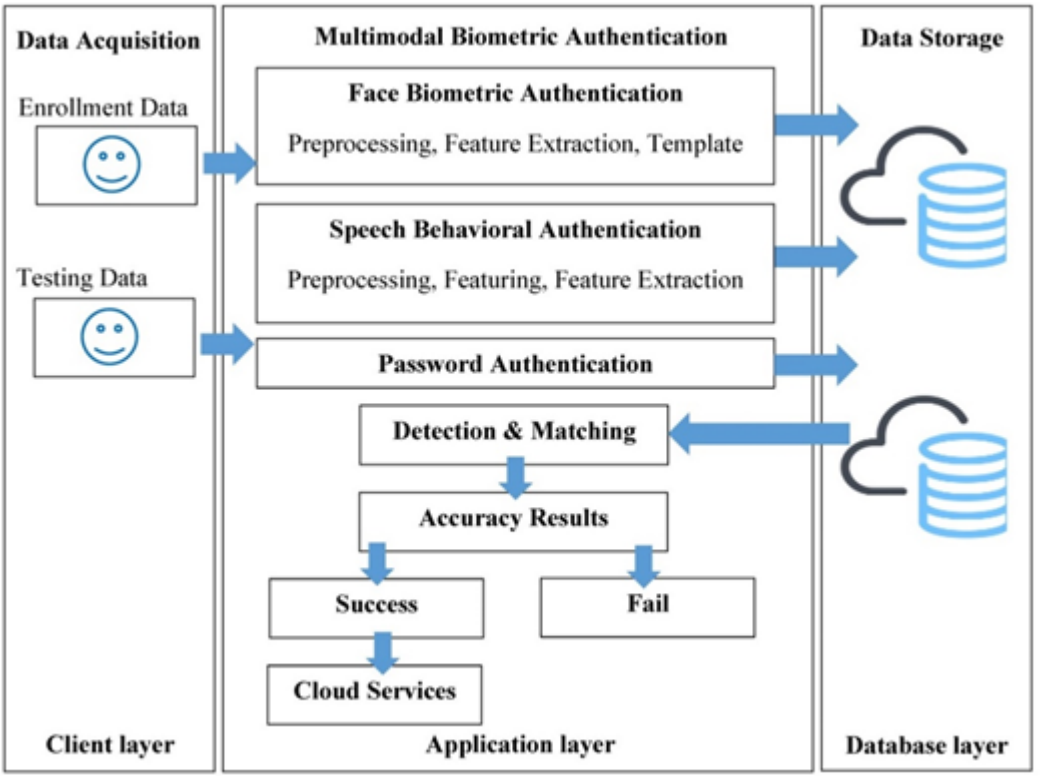
At the moment, wearable technology is more prevalent in people's daily lives. As a result, the researchers examine current state-of-the-art user authentication for wearable devices. According to the researchers, biometrics are classified into two categories based on their frequency of use: physiological biometrics and behavioral biometrics. The researchers' objective is to establish a framework for future research in this field. Kute et al. (2021) advocated for the use of fingerprints to identify a person's facial image, particularly in criminal investigations. In forensic investigations, both face recognition and fingerprint recognition are frequently used. This methodology learns and trains using Bregman divergence regularization from fingerprint biometrics and then transfers the learning to face biometrics. The results indicate that transferring can enhance biometric identification performance and assist in identifying the correct suspect.

PROPOSED DEVELOPMENT SYSTEM

Figure 1 details the extended framework for parallel biometric authentication for a cloud-based biometric service. The system is divided into three tiers: end-user, application, and database. A system's end-user layer is the layer with which the user interacts or utilizes. Initially, the research concentrated solely on smartphone devices, as they are a highly specialized platform. As a result, the framework remains cross-platform compatible with smartphones and other devices. The application layer consists of the system application, which includes face and speech recognition components. A user may choose between biometric authentication and password authentication. Additionally, the system can authorize user recognition based on the average score of multiple biometric authentication methods. If any recognition score fails, the user can still immediately log in to the system using a

username and password. Thus, the database layer is responsible for database administration functions such as data inserting, updating, accessing, and deletion.

Figure 1. Extended Framework of biometric authentication cloud service



While Pukdesree and Netinant's (2016) conceptual framework outlines the design of a single security access system for detecting fraud services, the framework does not yet include a cloud-based multimodal biometric implementation. Their research extends the framework for representing multimodal biometric authentication through the use of parallel recognition layering designs to facilitate the implementation of biometric authentication systems on web-based services. The benefits of a multimodal biometric authentication system are highlighted because it enables face and speech authentication via web-based detection during an examination. The client layer of the research includes experimental testing on the end-user device using an iPhone 11 running iOS version 15 to ensure that the proposed system device collects student information such as speech, face, password, and other information during registration and recognition. A Docker container deploys the application layer on a virtual machine and a cloud virtual private server. The system is built on a web-based platform compatible with cross-platform software. Additionally, the database layer is stored and managed in the cloud via a virtual private server. Due to the development of multimodal biometric recognition for student authentication services, the authentication system processes are divided into three phases.

Registration Phase

This process collects information from newly registered members. The information includes both essential and biometric data. Face biometric registration consists of three steps: face detection, face

preprocessing, and face extraction. Face detection in this study is accomplished using a Local Binary Patterns (LBP) technique. The LBP-based approach collates the pixel intensity of edges, corners, and flat regions using the histogram method. The LBP-based technique can be used to increase the rate of face detection while decreasing computing time. Additionally, face detection is unreliable in low light conditions. As a result, the face images are required to perform histogram equalization, which improves the contrast and brightness of the images. Equalization of histograms is also a critical step in the facial recognition process. Face preprocessing entails three steps: 1) eye search regions that emphasize eye alignment, which involves scaling, rotating, and translating the images; and 2) removing the forehead, chin, ears, and background from the images. 2) equalization of the histogram, which evenly distributes the brightness and contrast on the left and right sides of the face. 3) The elliptical mask will eliminate some of the remaining hairs and background from the facial image, leaving only the facial image. Speech biometric registration consists of three steps: Mel Frequency Cepstral Coefficients (MFCC) extraction, Delta calculation, and a combination of MFCC extraction and Delta calculation. For audio, the MFCC extraction algorithm generates twenty-dimensional feature vectors. For audio, the delta calculation will also use twenty-dimensional feature vectors. Thus, when MFCC extraction and Delta calculation are combined, forty-dimensional feature vectors for audio are created. Finally, biometric information will be extracted as biometric templates from the critical features. A cloud database will be used to store the templates. The registration process is depicted in Figure 2.

Training Phase

After obtaining the desired biometric information for each individual, this data must be trained using a machine-learning algorithm for facial and speech templates. Training data use eigenfaces for facial training because it is a straightforward method. Nonetheless, it is capable of performing as well as more sophisticated face recognition algorithms. The proposed system employs the Gaussian Mixture algorithm for speech training. The training phase's output will be machine learning models. Models can be derived from the machine learning algorithms used in this experiment using training data. The training data set is the collection of data used to educate the model. The training data will be labeled with the labels used for recognitions or decisions in this experiment. The training process is depicted in Figure 3.

Recognition Phase

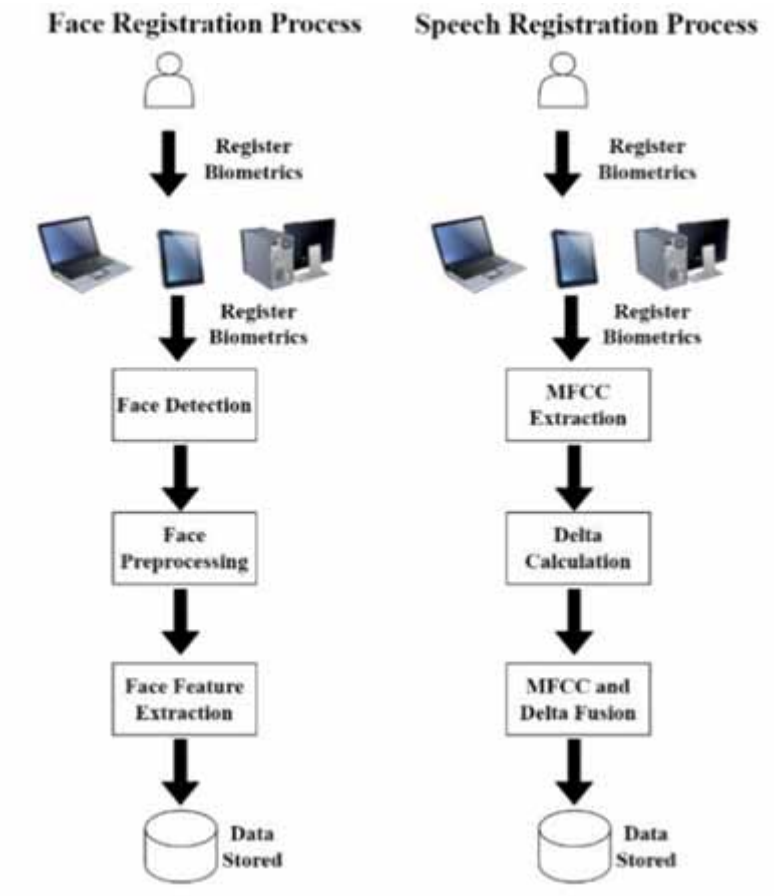
The recognition process can identify or verify an individual by comparing their biometric data to facial and speech features stored in a database. The design and development employ principal component analysis in this study, which employs eigenfaces for facial recognition. The eigenvectors are derived from the covariance matrix of the probability distribution for facial images in their high-dimensional vector space. For speech recognition, this study employs a Gaussian mixture model probability distribution. The outcome of these processes is the matching score for each biometric evaluation. The scores are combined using adaptive authentication's equality weight. The fused score will indicate whether or not the individual is a member of a system. The recognition process is depicted in Figure 4.

RESEARCH METHODOLOGY

Type of Research

This is experimental research that employs a systematic approach to studying, researching, and innovating. The purpose of this research is to create a web-based examination for undergraduate students that makes use of cloud-based biometric services. Due to the disruption in information technology today, students can learn from anywhere or anytime, as advanced network technology, particularly internet technology, has emerged. However, there would be a process in place to authenticate students taking online examinations. The purpose of this research is to use biometric

Figure 2. Face and speech biometric registration processes



cloud services to enable multimodal biometric authentication for a web-based exam for undergraduate students.

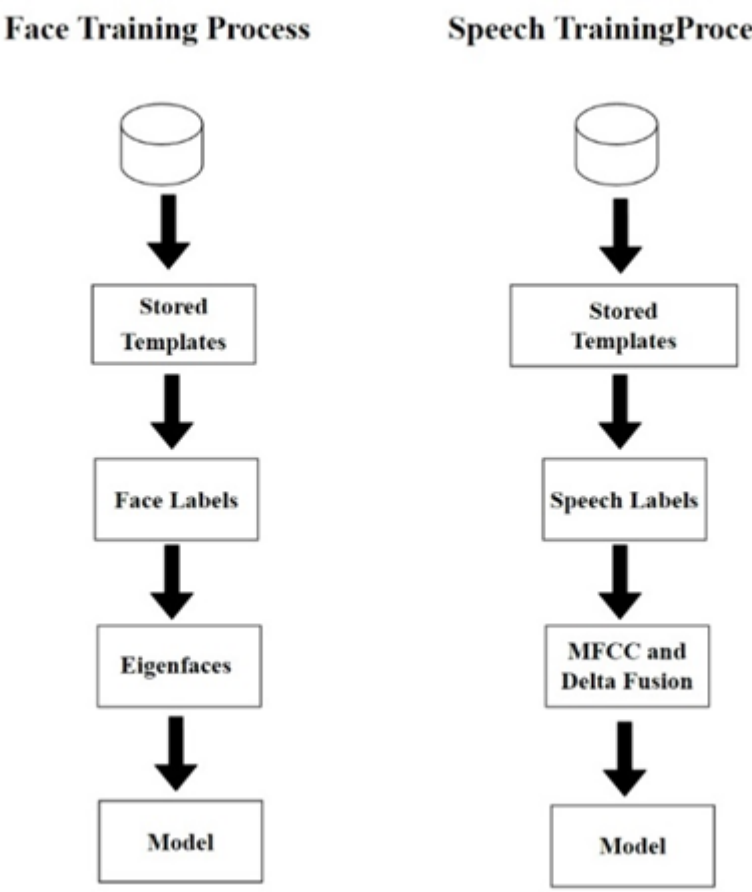
Research Sample

The population for this study is students enrolled in second semester 2020 courses in the department of computer science and technology at Bangkok University's school of information technology and innovation. The population is approximately 400 students. Purposive sampling was used in this study to select students from the computer organization course, which is appropriate for the current situation in our context. This course has approximately eighty students enrolled. The sampling is stratified into two categories: members and nonmembers.

Research Instrument and Procedure

The instrument of the study is a web application written in Python and using the Django framework. Sqlite3 is the database management system used by this web application. This web application can be accessed and used via an iPhone, an Android device, or a desktop computer equipped with a web browser. Researchers schedule appointments with our students before they take the final examinations via online examinations.

Figure 3. Face and speech biometric training process



Data Collection

This research collects data through experimental testing. The sampling will enable individuals to use the multimodal biometric authentication system on their devices. The sample will be provided with the necessary information to access the system on the specified date and time.

Data Analysis

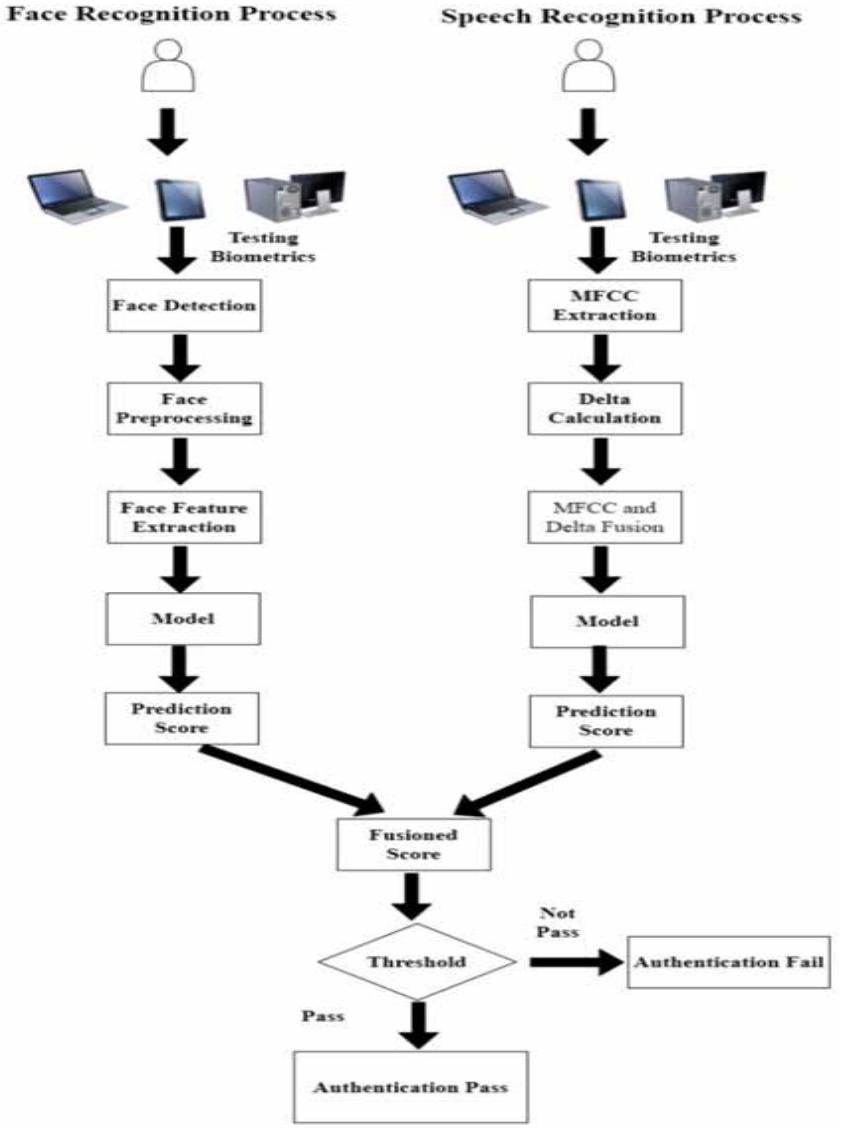
The collected data is an enumeration count of multimodal biometric authentication matches and mismatches. Qualitative data are gathered. As a result, the Chi-square test was used to analyze the data in this study, as it corresponds to the collected data. The Chi-square test is an appropriate method for determining the statistical relationship between two independent sampling groups.

SYSTEM IMPLEMENTATION

System Design

The system was designed by researchers using a variety of design tools. This article, on the other hand, discusses design tools such as use case diagrams, Entity Relation (ER) diagrams, data dictionaries, and flow diagrams. According to the use case diagram depicted in Figure 5, the system involves three

Figure 4. Face and speech biometric recognition processes

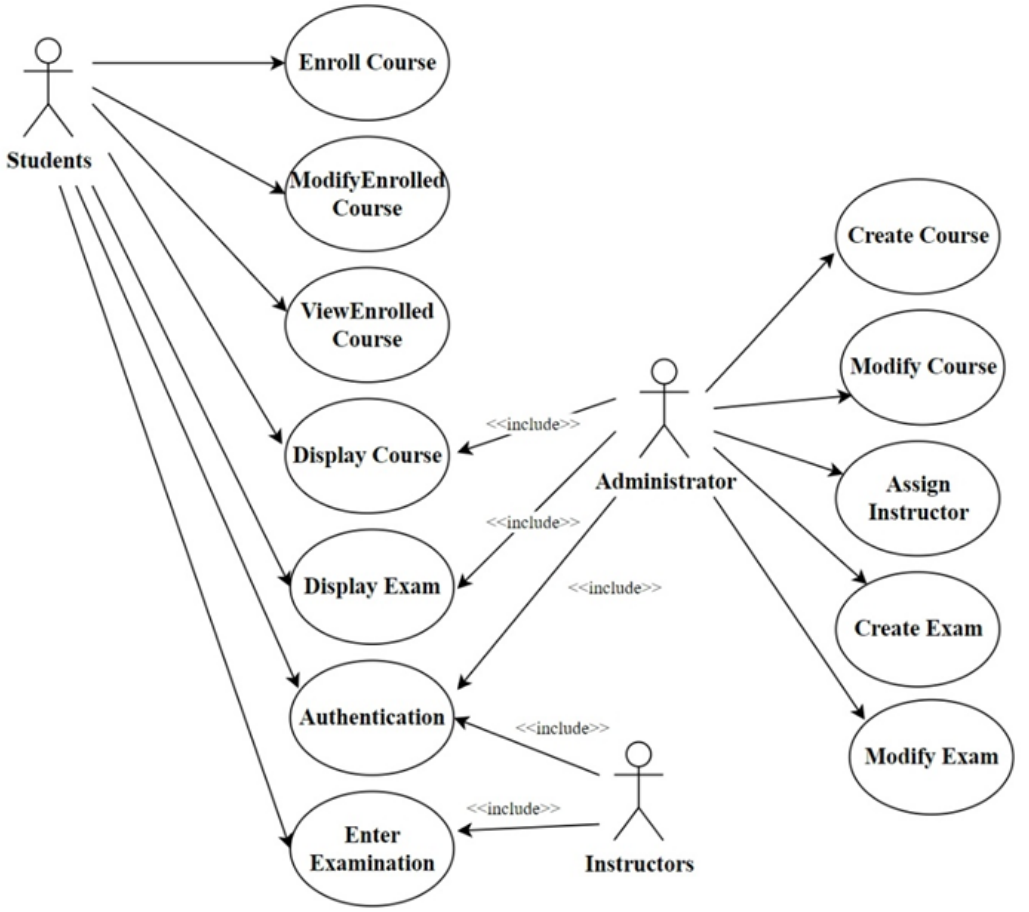


actors: students, instructors, and administrators. Students can enroll in courses, modify previously registered courses, view previously enrolled courses, display examinations, login to tests, and enter examinations through this system. Instructors can perform various functions in this system, including displaying courses, displaying examinations, logging into tests, and entering examinations. Finally, administrators can perform a variety of functions in this system, including displaying courses, displaying examinations, logging into examinations, creating and modifying courses, assigning instructors, generating examinations, and modifying tests.

As illustrated in Figure 6, the system's ER diagram contains seven entities: students, instructors, administrators, courses students, courses, examinations, and examinations students. Each entity is connected to other entities in some way. Students can enroll in the same courses that are offered during the indifference semester and academic years. As a result, a many-to-many relationship exists.

Students can sit for the same examination for courses that span multiple semesters and academic years. As a result, a many-to-many relationship exists. As a result, these entities will be normalized to at least the third standard form. Finally, the normalized form will be converted to a data dictionary, used to create database tables.

Figure 5. Use case diagram of multimodal biometric authentication for web-based examination



Consider the flow diagram of the student's activities depicted in Figure 7. To begin, students can log in to the examination system using their devices such as iOS smartphones, Android smartphones, personnel computers, or notebook computers. Students will be required to enter their facial biometrics into the system via the built-in or web camera. The facial biometrics will be stored on the server in a temporary folder. Then, using a microphone, students will enter their speech biometrics into the system. The speech biometric will be stored on the server in a temporary folder. When students click the login button, the system extracts facial biometric features and compares them to those extracted from previously enrolled facial extractions. The system will assign a personal score to the result of the comparison based on the comparison's similarity. Following that, when students click the login button, the system extracts biometric speech features and compares them to the extracted features of

Figure 6. The entity-relationship diagram of multimodal biometric authentication for examination systems

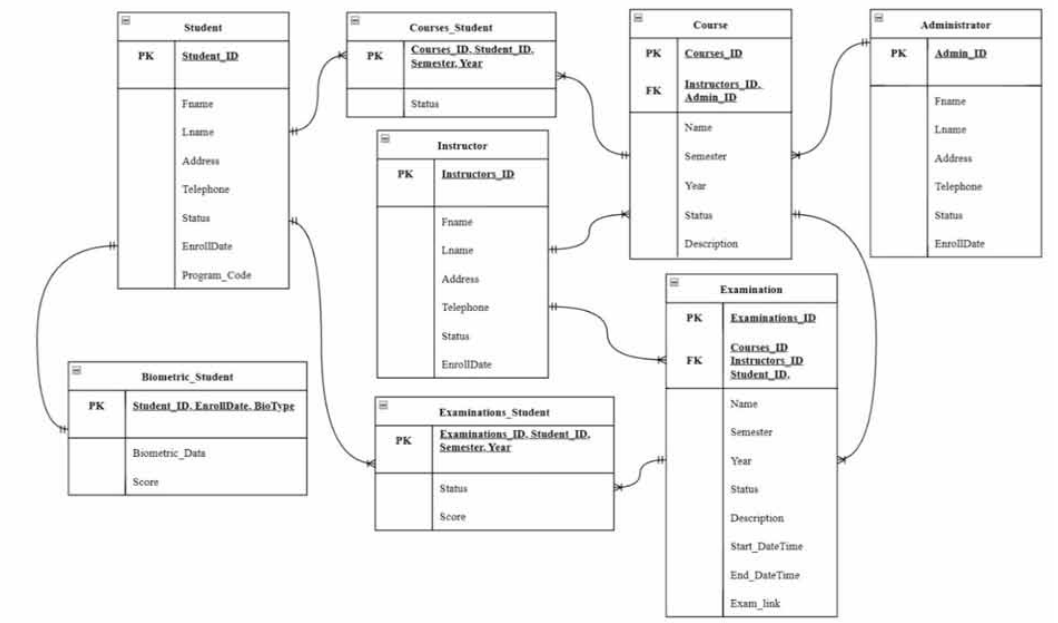
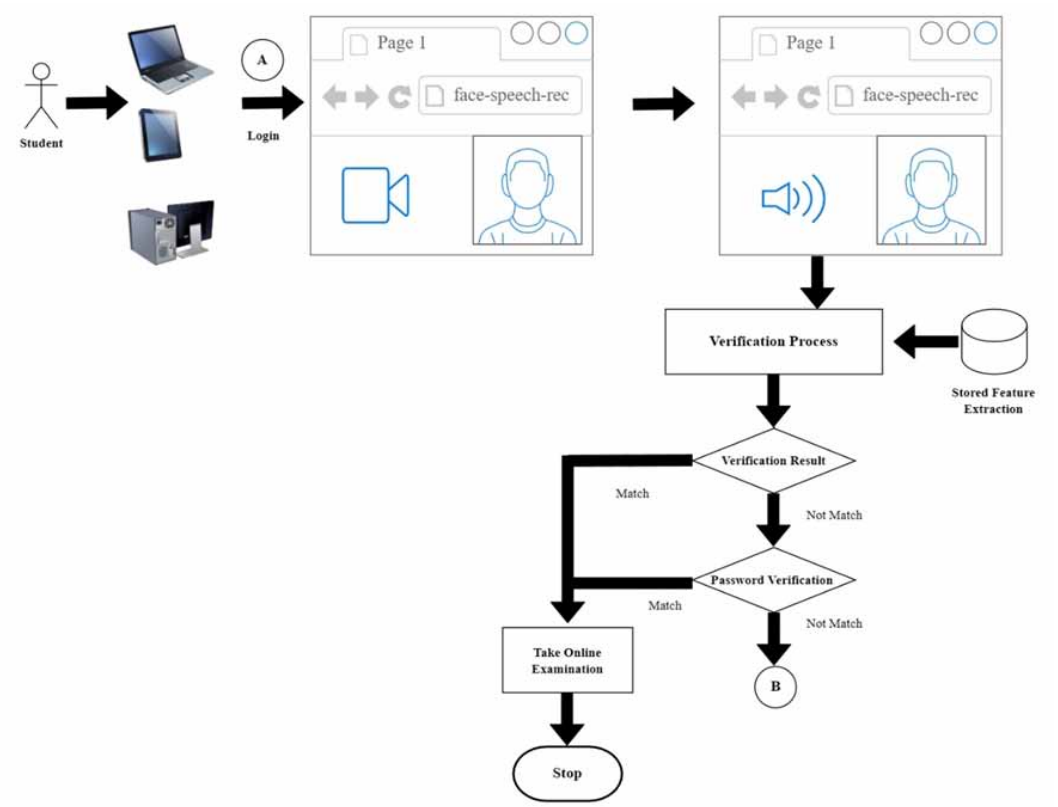


Figure 7. Flow Diagram of multimodal biometric authentication for web-based examination



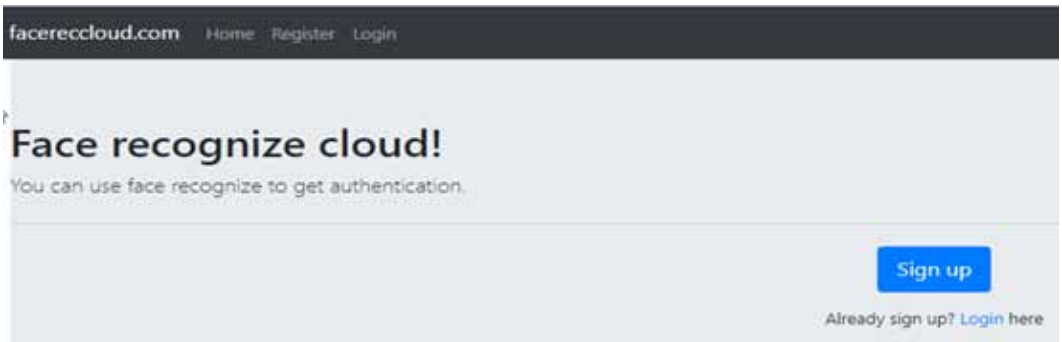
previously enrolled speech extractions. The system will provide a confidential score for the comparing result that reflects the similarity of the comparing. The system will then compute the fusion score by combining the confidential facial biometric and speech biometric scores. Finally, the system will decide on multimodal biometric authentication using the fusion score. If the student's fusion score falls within the specified range of values, the system will admit the student to the online examination. On the other hand, if the fusion score does not fall within the scope of acceptable values, the system will refuse to admit the student to the online examination. The student also has the option of using their password in the traditional manner.

Web-based Implementation

This multimodal biometric authentication system employs speech and face recognition and is deployed on a Docker container running on a virtual machine on a cloud virtual private server. The system was developed using web technology that is cross-platform compatible. Figure 8 illustrates the system's home page, from which students can register as a new user or log in as an existing user. A student must register as a new user by entering their basic information, including one speech recording and twenty face recordings, as illustrated in Figures 9 and 10. All data will be securely stored in a cloud-based database.

Additionally, the system will extract speech features and store them in a folder designated for the training process. The system will extract facial features and perform pre-processing before storing them in a specified folder for use during the training process. The paper borrows the specifics of this process as described in (Pukdesree & Netinant, 2018). Finally, the system administrator will be responsible for batch processing the training process.

Figure 8. Home pages of authentication notification and services



To log into the system during the recognition phase, a student will enter their speech recording and take a facial picture, as illustrated in Figure 11. If the multi-modal biometric result score exceeds the threshold, the system will permit the student to access online testing services, as illustrated in Figure 12. On the other hand, if the student's multi-modal biometric result falls below the threshold, the system will deny online testing services. However, if a device fails or the environment becomes uncertain, a student can enter a password to access the system. Additionally, adaptive student authentication systems, compared to Pukdesree and Netinant (2016), can support parallel recognition. The extended framework has the potential to increase security and efficiency at a low cost significantly. Password authentication is used when multimodal biometrics are deemed too complex or do not authenticate students during accurate online testing.

Figure 9. Registration process

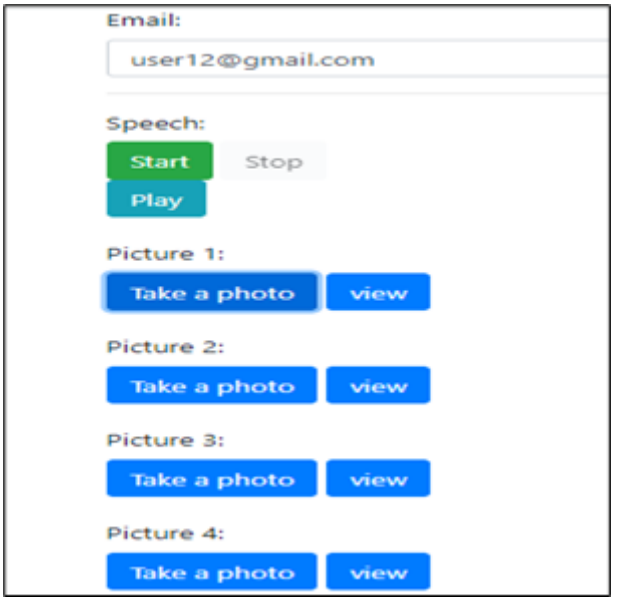


Figure 10. Facial enrollment

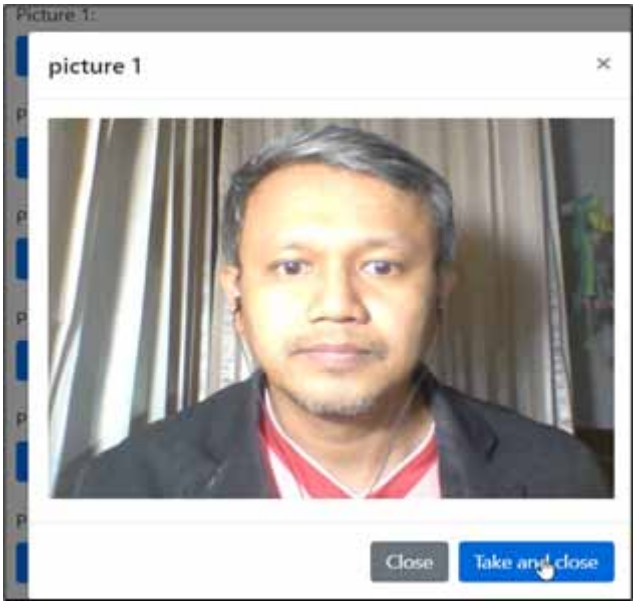


Figure 11. Testing processes

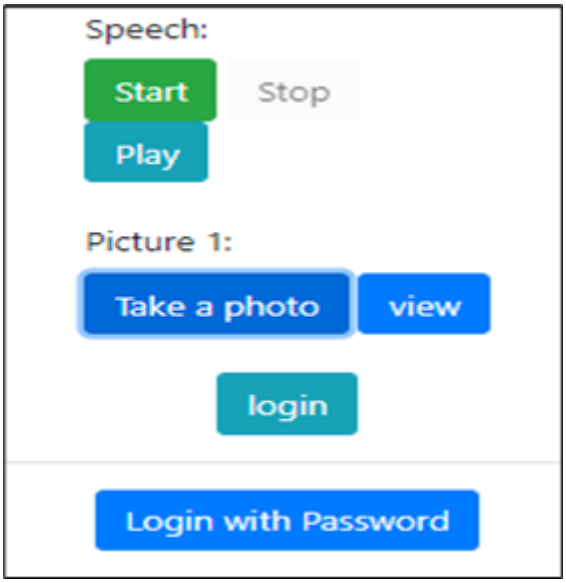


Figure 12. Authentication accurate results

The online testing system supports three user roles: student, instructor, and administrator. The administrator role has the ability to manage student and instructor data. As illustrated in Figures 13 and 14, the instructor can manage courses exams and generate reports. The student role is entirely responsible for managing their information and taking tests.

Figure 13. Course management

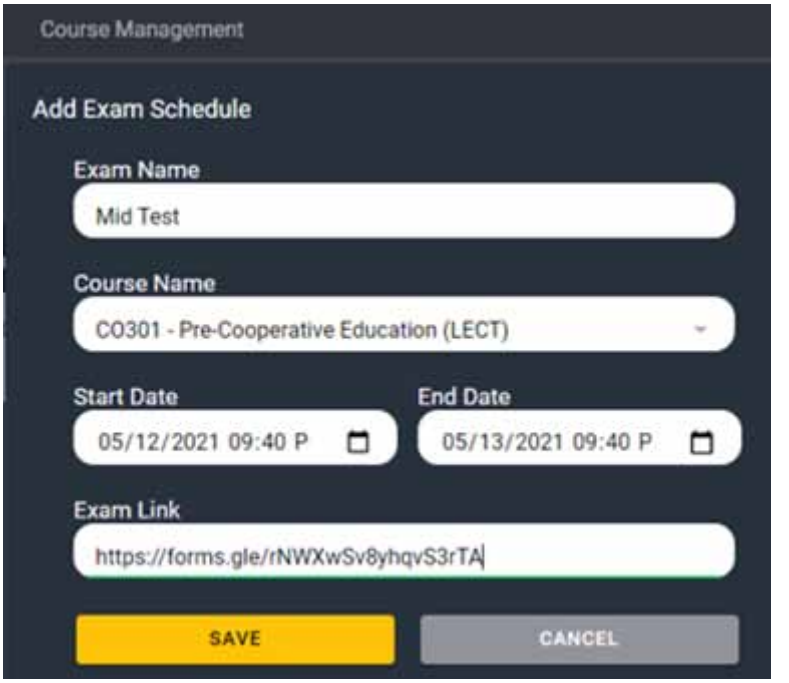


Figure 14. Examination management

EVALUATION METHODOLOGY

The confusion matrix is a table that is used to compare the model's predictions to the actual values. This matrix is used in predictive analytics, a branch of statistics that uses data to extract information and forecast trends and behavior patterns. Predictive analytics is a type of statistics. Predictive analytics is comprised of algorithms for deep learning, data modeling, and data mining. The framework was evaluated using the following metrics (Tharwat, 2018; Chicco & Jurman, 2020; Piryonesi & El-Diraby, 2020; Chicco et al., 2021).

1. The accuracy score is a statistical measure calculated as the ratio of genuine prediction results to the total number of tests. The following Equation (1) is used to calculate the accuracy score.

$$\text{Accuracy} = \frac{\sum\left(\text{True}_{\text{positive}}\right) + \sum\left(\text{True}_{\text{negative}}\right)}{\sum\left(\text{Total\_population}\right)} \tag{1}$$

2. Precision is a term that refers to the accuracy with which predictions are made. Precision is a two-sided coin: it can be viewed positively or negatively. The precision positive value indicates the precision with which the member aspect prediction was made. The precision minus sign indicates the likelihood of correctly predicting the nonmember aspect. The precision score formula is expressed in Equations (2) and (3).

$$\text{Precision\_Positive} = \frac{\left(True_{positive}\right)}{\left(True_{positive} + False_{positive}\right)} \tag{2}$$

$$\text{Precision\_Negative} = \frac{\left(\text{True}_{\text{negative}}\right)}{\left(\text{True}_{\text{negative}} + \text{False}_{\text{negative}}\right)} \tag{3}$$

3. The recall value indicates the prediction results' accuracy compared to the actual values, which can be expressed as the percentage of correcting predictions made by members with recall positive and nonmembers with recall negative. Thus, the formula can represent the data in Equations (4) and (5).

$$\text{Recall\_Positive} = \frac{\left(\text{True}_{\text{positive}}\right)}{\left(\text{True}_{\text{positive}} + \text{False}_{\text{negative}}\right)} \tag{4}$$

$$\text{Recall\_Negative} = \frac{\left(\text{True}_{\text{negative}}\right)}{\left(\text{True}_{\text{negative}} + \text{False}_{\text{positive}}\right)} \tag{5}$$

4. By estimating the average precision and recall values, the F1 score quantifies performance. Additionally, the F1 score is referred to as the harmonic mean. The F1 score has two possible

values: negative and positive. Assume that the F1 score is high, indicating that the model performs satisfactorily. Equation (6) can be used to express the F1 score mathematically.

$$\text{F1 Score} = \frac{2\text{PR}}{\left(\text{P}+\text{R}\right)} \tag{6}$$

EXPERIMENTAL RESULTS

Around one hundred students participate in this study, registering their information into the system, including biometrics such as speech and facial recognition. Each student will enter basic information, one speech proposition, and twenty faces during the registration process. The data will be stored on a virtual private server hosted in the cloud. Eighty times, the system's authentication was evaluated by allowing registered and unregistered members to authenticate themselves to access online testing services. Additionally, the system provides a password for authentication if multimodal biometrics are deemed too complicated or fail to authenticate students during accurate online testing.

This study evaluates a multimodal biometric authentication method that combines face and speech recognition for cloud service access. The confusion matrix's results are summarized in Table 1.

The True Positive value is 49, indicating that the prediction results are valid for system member authentication. 2) The True Negative value is 8, indicating the probability of correctly predicting a non-member of the system. 3) The False Positive value is 9, indicating that the authentication of a non-member of the system failed due to a false prediction. 4) False Negative value is 14, indicating a prediction by an incorrect system member. The confusion matrix is depicted in Figure 15.

Table 1. Confusion matrix table of multimodal biometric using face and speech recognition

	N=80	Nonmember /Negative (0)	Member /Positive (1)
Actual	**Nonmember /Negative (0)**	8	9
	Member /Positive (1)	12	51

The confusion matrix results can explain in several ways, such as accuracy score, precision values, recall values, and F1 scores, as shown in Table 2 and Figure 16. The accuracy score in this experimental evaluation is 0.712500 or 71.25 percent, representing the ratio of valid prediction results to total testing numbers. This accuracy rating is on the moderate side. One factor affecting the system's accuracy is that the environment enters biometric data, such as when speech or face information is entered, as mentioned in several research papers.

Precision refers to the accuracy with which results are predicted. Precision can be viewed in two ways: positively or negatively. Precision positive refers to the accuracy with which the member aspect is expected. The precision negative represents the probability of correctly predicting the nonmember aspect. In this experimental evaluation, the precision positive value is 0.844828, indicating that the actual member's correct result prediction is 84.4828 percent. The precision negative value is 0.363636, indicating that the nonmember's accurate result prediction is 36.3636 percent.

Figure 15. Graph of confusion matrix

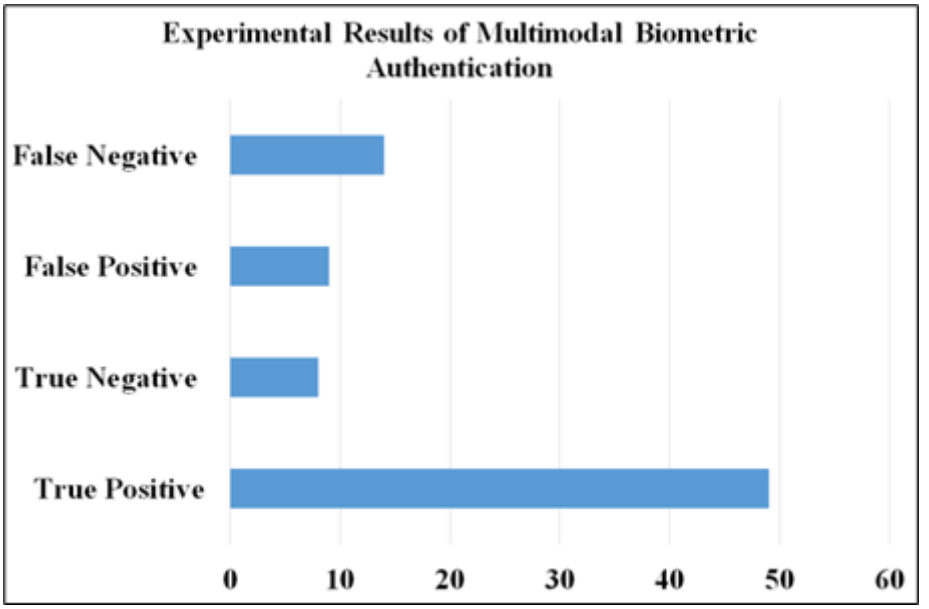


Figure 16. Graph evaluation scores

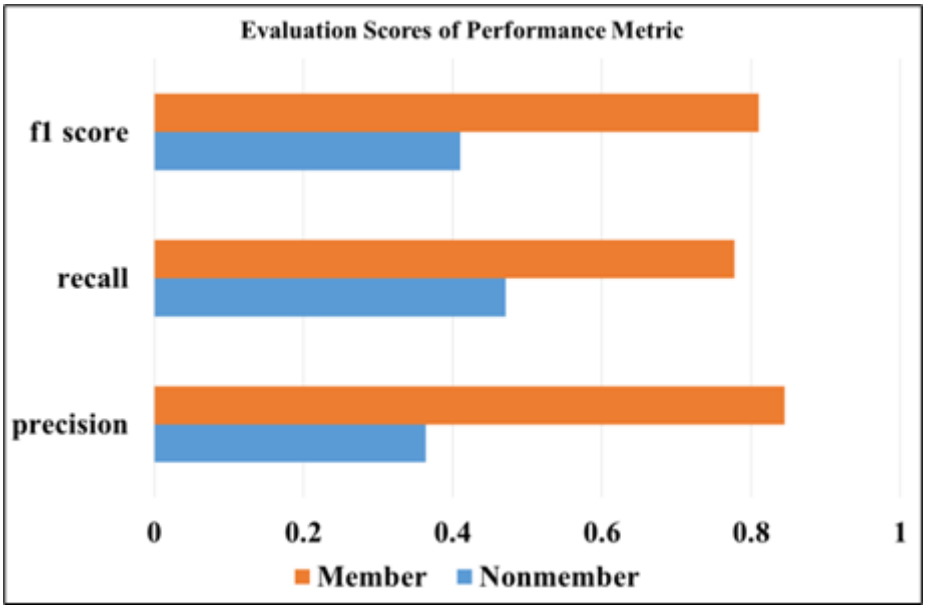


Table 2. Evaluation scores of multimodal biometrics using face and speech recognition

Accuracy Score	0.712500			
	Precision	**Recall**	**F1 Score**	**Support**
Nonmember	0.363636	0.470588	0.410256	17
Member	0.844828	0.777778	0.809917	63

The recall value indicates how accurately the results were predicted in comparison to the actual values, taking into account the percentages of correcting prediction and actual members, as well as the percentages of correcting prediction and nonmembers. The recall positive value is 0.777778, which represents the actual member's percentage of correct predictions. In this experiment, there are 63 actual members and 49 correct predictions of the actual member. As a result, the recall positive will be 49 out of 63, or 77.7778 percent accurate prediction. The recall negative value is 0.470588, which indicates the nonmember's percentage of correct predictions. The nonmembers in this experiment have some 17, while the prediction has eight accurate predictions of the nonmember's faces. As a result, the recall negative will be eight out of seventeen, or 47.0588 percent correct.

The F1 score represents performance by averaging the precision and recall values. The F1 score may also be referred to as the harmonic mean if it contains high values, indicating the model's superior performance. The positive value for the F1 score is 0.809917, or 80.9917 percent. The negative value of the F1 score is 0.410256 or 41.0256 percent.

Additionally, the results from the confusion matrix table using Pearson's Chi-square statistic to determine the research hypothesis's validity as illustrated in Table 3. The Chi-square statistic can be used with either quality or classification variables. Variables can be classified into k groups based on their value. Then, the frequency of each group could be specified. Chi-square is a nonparametric statistic. Independent of two variables testing can be used to evaluate research hypotheses involving two group variables. The test can be used to determine the independence of two populations' properties. If the observed and expected frequencies are almost identical, the observed frequency will be compared to the expected frequency. If the observed frequency is different from the observed frequency, it can be concluded that these two frequencies are independent. If the observed frequency is different from the observed frequency, it can be concluded that these two frequencies are dependent.

Table 3. Confusion matrix table and Pearson's Chi-square statistic

	N=80	**Nonmember /Negative (0)**	**Member /Positive (1)**	**Total**
Actual	**Nonmember /Negative (0)**	8 (4.25)	9 (12.75)	17
	Member /Positive (1)	12 (15.75)	51 (47.25)	63
	Total	20	60	80

Step 1: Identifying the statistical hypotheses H0 and H1:

Hypothesis Zero (H0): The proposed multimodal authentication does not rely on the user's authentication for an undergraduate web-based examination.

Hypothesis One (H1): The proposed multimodal authentication is predicated on the user's authentication for an online examination for undergraduate students.

Step 2: Establishing that the significance level is equal to 0.05.
Step 3: Statistic calculation Chi-square analysis

The Chi-square test value for this scenario is 3.841, which can be found in the Chi-square test table. In this experiment, the Chi-square test value can be calculated using the Chi-square test formula, which equals 5.602241. Since the degree of freedom is equal to one, the Chi-square test value must be optimized using Yate's continuity correction. Then the Chi-square value is equal to 4.465842. The Chi-square test formula is denoted by Equation (7).

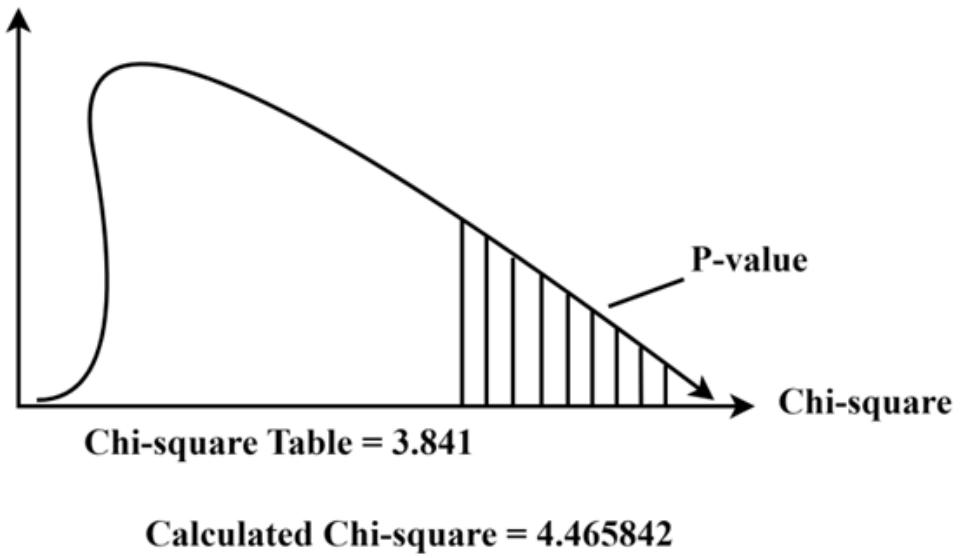
$$\text{Chi-square test} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{\left(\left|\text{Oij-Eij}\right|-0.5\right)^2}{\text{Eij}} \tag{7}$$

Step 4: Establish a critical region

The Chi-square test value can obtain from the predefined table with a significance level of 0.05 and *df* equal to 1. From the predefined table, the Chi-square test result is 3.841. The value of 4.465842 is the calculated Chi-square test value. As a result, the area of the experiment's critical region is more significant than 3.841. Additionally, the probability value (*p*-value) is equal to 0.03458.

Moreover, the calculated Chi-square test value is 4.465842, which is more significant than the Chi-square test value of 3.841 for the predefined table. As a result, H0 is rejected at the 0.05 level of significance. Additionally, one can deduce the *p*-value. The *p*-value is 0.03458, which is less than the 0.05 level of significance. The Chi-square test computed falls within the bounds of the rejected hypothesis H0. The findings suggest that either the research hypothesis is correct or that the proposed multimodal authentication is conditional on the user authenticating for a web-based examination for undergraduate students. Figure 17 illustrates the critical region of the Chi-square test.

Figure 17. Critical region of Chi-square test



CONCLUSION

This paper aims to propose a framework for multimodal biometric authentication for student examinations that utilize cloud computing services and conduct both development and experimental research on a smartphone. The framework aims to enhance the security and robustness of biometric authentication while also making it easier to deploy in cloud computing environments. This system was developed using web technology to enable students to register, authenticate, and take online exams using their biometrics. As a result, the web-based system is compatible with smartphones and platforms, enhancing facial image and speech data compression capabilities. The research outcome is devoted to evaluating multimodal biometric authentication services, particularly face and speech recognition. The confusion matrix compares the model's predictions to observed recognition values, including an accuracy score of 71.25 percent, a precision positive value of 84.48 percent, a recall value of 77.78 percent, and an F1 score of 77.78 percent (80.99 percent). As a result, the overall scores from the experimental evaluation can be used in practice. Additionally, practical evaluation is conducted through experimental testing. During Thailand's coronavirus pandemic in 2020, students who took online examinations could automatically authenticate themselves using the proposed multimodal biometric authentication system. The optimal detection and recognition parameters for the multimodal biometric authentication system can be adjusted and evaluated for future research. The adaptive multimodal biometric authentication technique could be implemented, and the adaptation weight associated with each biometric recognition could be determined. Furthermore, the system can increase security using encrypted data transmitted across a network using a secure socket layer, preventing eavesdropping and tampering. The designs can be configured to utilize various encryption techniques for additional investigation, including public-key cryptosystems and symmetric keys.

REFERENCES

Ajish, S. (2021). Secure mobile internet voting system using biometric authentication and wavelet based AES. *Journal of Information Security and Applications*, *61*, 102908. doi:10.1016/j.jisa.2021.102908

Bah, S. M., & Ming, F. (2020). An improved face recognition algorithm and its application in attendance management system. *Array*, *5*, 100014. doi:10.1016/j.array.2019.100014

Behera, N. K. S., Behera, T. K., Nappi, M., Bakshi, S., & Saa, P. K. (2021). Futuristic person re-identiðcation over internet of biometrics things (IoBT): Technical potential versus practical reality. *Pattern Recognition Letters*, *151*, 163–171. doi:10.1016/j.patrec.2021.08.007

Bisogni, C., Iovane, G., Landi, R. E., & Nappi, M. (2021). ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions. *Journal of Information Security and Applications*, *59*, 102814. doi:10.1016/j.jisa.2021.102814

Brundhaelci, J., Punith, R., Gowda, S. C., Shivaprasad, B. M., & Buvaneshwaran, V. S. (2019). Criminal recognition and tracking system. *International Research Journal of Computer Science*, *6*(6), 118–125. doi:10.26562/IRJCS.2019.JNCS10095

Casanova, A., Cascone, L., Castglione, A., Meng, W., & Pero, C. (2021). User recognition based on periocular biometrics and touch dynamics. *Pattern Recognition Letters*, *148*, 114–120. doi:10.1016/j.patrec.2021.05.006

Chang, D., Garg, S., Ghosh, M., & Hasan, M. (2021). BIOFUSE: A framework for multi-biometric fusion on biocrypto system level. *Information Sciences*, *546*, 481–511. doi:10.1016/j.ins.2020.08.065

Cherifi, F., Omar, M., & Amroun, K. (2021). An efficient biometric-based continuous authentication scheme with HMM prehensile movements modeling. *Journal of Information Security and Applications*, *57*, 102739. doi:10.1016/j.jisa.2020.102739

Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, *21*(6), 6. Advance online publication. doi:10.1186/s12864-019-6413-7 PMID:31898477

Chicco, D., Toetsch, N., & Jurman, G. (2021). The Matthews correlation coefficient (MCC) is more reliable than balanced accuracy, bookmaker informedness, and markedness in two-class confusion matrix evaluation. *BioData Mining*, *14*(13), 13. Advance online publication. doi:10.1186/s13040-021-00244-z PMID:33541410

Choudhury, S. H., Kumar, A., & Laskar, S. H. (2021). adaptive management of multimodal biometrics-A deep learning. *Applied Soft Computing*, *106*, 107344. doi:10.1016/j.asoc.2021.107344

Cui, W., Wang, Z., & Li, Y. (2021). ECG-Based biometric recognition under exercise and rest situations. *Biomedical Engineering Advances*, *2*, 100008. doi:10.1016/j.bea.2021.100008

Czeskis, A., Dietz, M., Kohno, T., Wallach, D., & Balfanz, D. (2012). Strengthening user authentication through opportunistic cryptographic identity assertions. In *Proceedings of the 2012 ACM conference on Computer and communications security (CCS'12)*. ACM. doi:10.1145/2382196.2382240

Errattahia, S., Hannania, A. E., & Ouahmane, H. (2018). automatic speech recognition errors detection and correction: A review. *Procedia Computer Science*, *128*, 32–37. doi:10.1016/j.procs.2018.03.005

Falmari, V. R., & Brindha, M. (2021). Privacy preserving biometric authentication using chaos on remote untrusted server. *Measurement*, *177*, 109257. Advance online publication. doi:10.1016/j.measurement.2021.109257

Fei, L., Zhang, B., Tian, C., Teng, S., & Wen, J. (2021). Jointly learning multi-instance hand-based biometric descriptor. *Information Sciences*, *562*, 1–12. doi:10.1016/j.ins.2021.01.086

Jia, W., Xia, W., Zhang, B., Zhao, Y., Fei, L., Kang, W., Huang, D., & Guo, G. (2021). A survey on dorsal hand vein biometrics. *Pattern Recognition*, *120*, 108122. doi:10.1016/j.patcog.2021.108122

Kausar, F. (2021). Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal*, *22*(4), 447–453. doi:10.1016/j.eij.2021.01.004

Khoo, Y., Goi, B., Chat, T., Lai, Y., & Jin, Z. (2018). Multimodal biometrics system using feature-level fusion of iris and fingerprint. In *Proceedings of the 2nd International Conference on Advances in Image Processing (ICAIP'18)*. ACM. doi:10.1145/3239576.3239599

Kumar, D., Joshi, A. B., & Singh, S. (2021). A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system. *Results in Optics*, *5*, 100146. doi:10.1016/j.rio.2021.100146

Kumari, P., & Thangaraj, P. (2020). A fast feature selection technique in multi modal biometrics using cloud framework. *Microprocessors and Microsystems*, *79*, 103277. doi:10.1016/j.micpro.2020.103277

Kute, R., Vyas, V., & Anuse, A. (2021). (in press). Transfer learning for face recognition using ðngerprint biometrics. *Journal of King Saud University -. Engineering and Science*. Advance online publication. doi:10.1016/j.jksues.2021.07.011

Lee, M. J., Teoh, A. B. J., Uhl, A., Liang, S., & Jina, Z. (2021). A tokenless cancellable scheme for multimodal biometric systems. *Computers & Security*, *108*, 102350. doi:10.1016/j.cose.2021.102350

Lee, Y. K., & Jeong, J. (2021). Securing biometric authentication system using blockchain. *ICT Express*, *7*(3), 322–326. doi:10.1016/j.icte.2021.08.003

Liu, S., Shao, W., Li, T., Xu, W., & Song, L. (2021). Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, *7*, 103120. doi:10.1016/j.dsp.2021.103120

Marquez, H. J. P., Ambrose, D. J., Schaefera, A. L., Cook, N. J., & Bench, C. J. (2021). Evaluation of infrared thermography combined with behavioral biometrics for estrus detection in naturally cycling dairy cows. *Animal*, *15*(7), 100205. doi:10.1016/j.animal.2021.100205 PMID:34171567

Mason, J., Dave, R., Chatterjee, P., Allen, I. G., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. *Array*, *8*, 100042. doi:10.1016/j.array.2020.100042

Naidu, B. R., & Babu, M. S. P. (2018). Biometric authentication data with three traits using compression technique, HOG, GMM and fusion technique. *Data in Brief*, *18*, 1976–1986. doi:10.1016/j.dib.2018.03.115 PMID:29900333

Piciucco, E., Lascio, E. D., Maiorana, E., Santini, S., & Campisi, P. (2021). Biometric recognition using wearable devices in real-life settings. *Pattern Recognition Letters*, *146*, 260–266. doi:10.1016/j.patrec.2021.03.020

Piryonesi, S. M., & El-Diraby, T. E. (2020). Data analytics in asset management: Cost-effective prediction of the pavement condition index. *Journal of Infrastructure Systems*, *26*(1), 1–25. doi:10.1061/(ASCE)IS.1943-555X.0000512

Pukdesree, S., & Netinant, P. (2016). Conceptual framework: The adaptive biometrics authentication for accessing cloud computing services using iPhone. *Advances in Intelligent Systems and Computing*, *463*, 209–216. doi:10.1007/978-3-319-40415-8_20

Pukdesree, S., & Netinant, P. (2018). Reviewed: The face authentication processes for accessing cloud computing services using iPhone. *TEM Journal*, *7*(3), 475–479. doi:10.18421/TEM73-01

Purohit, H., & Ajmera, P. K. (2021). Optimal feature level fusion for secured human authentication in multimodal biometric system. *Machine Vision and Applications*, *32*(1), 1–12. doi:10.1007/s00138-020-01146-6

Saeed, U. (2021). Facial micro-expressions as a soft biometric for person recognition. *Pattern Recognition Letters*, *143*, 95–103. doi:10.1016/j.patrec.2020.12.021

Sarier, N. D. (2021). Multimodal biometric authentication for mobile edge computing. *Information Sciences*, *573*, 82–99. doi:10.1016/j.ins.2021.05.036

Selwal, A., Gupta, S. K., Jangra, S., & Rautela, A. (2016). Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry. *Perspectives in Science*, *8*, 705–708. doi:10.1016/j.pisc.2016.06.065

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University - Computer and Information Sciences, 32*(1), 57–64. .10.1016/j.jksuci.2017.07.001

Smith, C. L., & Brooks, D. J. (2013). Integrated identification technology. *Security Science: The Theory and Practice of Security*, *7*, 153–174. doi:10.1016/B978-0-12-394436-8.00007-2

Srivastva, R., Singh, A., & Singh, Y. N. (2021). PlexNet: A fast and robust ECG biometric system for human Recognition. *Information Sciences*, *558*, 208–228. doi:10.1016/j.ins.2021.01.001

Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion*, *66*, 76–99. doi:10.1016/j.inffus.2020.08.021

Tharwat, A. (2018). Classification assessment methods. *Applied Computing and Informatics*, *17*(1), 168–192. doi:10.1016/j.aci.2018.08.003

Vijay, M., & Indumathi, G. (2021). Deep belief network-based hybrid model for multimodal biometric system for futuristic security applications. *Journal of Information Security and Applications*, *58*, 102707. doi:10.1016/j.jisa.2020.102707

Wojtowicz, A., & Joachimiak, K. (2016). Model for adaptable context-based biometric authentication for mobile devices. *Personal and Ubiquitous Computing*, *20*(2), 195–207. doi:10.1007/s00779-016-0905-0

Yadav, S. S., Gothwal, J. K., & Singh, R. (2011). Multimodal biometric authentication system: Challenges and solutions. *Global Journal of Computer Science and Technology*, *11*(16), 56–60.

Yang, W., Wang, S., Zheng, G., & Valli, C. (2019). Impact of feature proportion on matching performance of multi-biometric systems. *ICT Express*, *5*(1), 37–40. doi:10.1016/j.icte.2018.03.001

Meennapa Rukhiran is an assistant professor in the Department of Computer Science at the Rajamangala University of Technology Tawan-OK, Chanthaburi Campus, Thailand. She received her Ph.D. degree in Information Technology from Rangsit University, Thailand. Her research interests lie in information technology applications, information retrieval, information services, and quality of information design. She has published international journals such as the Journal of Information and Communication Technology, TEM Journal, and Journal of Current Science and Technology.

Sorapak Pukdesree is a senior lecturer in the computer science department at Bangkok University in Thailand. He earned a Master of Science in Computer Science from the University of Tennessee at Chattanooga, Tennessee, United States of America. He is currently pursuing a doctorate in information technology from Rangsit University in Thailand. His research interests include information modeling and frameworks, software development and cloud computing, and the Internet of Things. He has published in international journals such as the TEM Journal, WSEAS Computer Transactions, and Advances in Intelligent Systems and Computing.

Paniti Netinant is an associate dean of the graduate school and an associate professor in Rangsit University's Department of Information Technology. He earned his M.S. and Ph.D. in Computer Science from Illinois Institute of Technology in the United States of America. His research interests include information modeling and frameworks, information technology design and development, the Internet of Things, and the layers and services of information. He has published in various international journals, including ACM Communications, ACM Computing Surveys, Journal of Information and Communication Technology, TEM Journal, and Journal of Current Science and Technology. He is the corresponding author of this article.