International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I12P102

Volume 72 Issue 12, 14-29, December 2024

Original Article

Two-Factor Authentication Application Using Artificial Intelligence to Support Academic Information Systems

Thipwimon Chompookham[1], Wongpanya S. Nuankaew[2], Pratya Nuankaew[3]

[1]*Department of Computer Technology and Digital, Faculty of Information Technology, Rajabhat Maha Sarakham University, Maha Sarakham, Thailand.*
[2]*Department of Computer Science, School of Information and Communication Technology,University of Phayao, Phayao, Thailand.*
[3]*Department of Digital Business, School of Information and Communication Technology, University of Phayao, Phayao, Thailand.*

[3]*Corresponding Author : pratya.nu@up.ac.th*

Received: 14 August 2024 Revised: 14 November 2024 Accepted: 18 November 2024 Published: 25 December 2024

Abstract *- Integrating facial recognition technology is crucial for enhancing the security of online learning and consultation platforms, particularly in computer technology and engineering education. This project aims to synthesize components and technologies to develop a prototype of a two-factor authentication system that leverages artificial intelligence technology. The goal is to enhance the efficiency and capacity of identification verification. Moreover, a comprehensive evaluation will be carried out to determine the prototype's performance and level of acceptance. A purposive random sampling strategy was employed to select 40 participants from the Computer Technology and Digital Program at Rajabhat Maha Sarakham University, including students and faculty members. The research instruments comprised a thorough questionnaire encompassing several facets of the academic information system's development, a prototype of a two-factor authentication system, a quality assessment form, and a questionnaire to gauge the information system's acceptance. The performance criteria comprised accuracy, precision, recall, f1-score, average, and standard deviation. The findings indicated that the authorized prototype comprised four distinct modules: an authentication module, a member module, an information module, and a management module. The evaluation results for identifying faces, using CNN Face Detector, VGG-Face net, and classification by Logistic Regression, attained a remarkable accuracy of 83.54%. The precision and recall values were 0.84 and 0.88, respectively. The evaluation findings indicate that the overall quality is quite acceptable, with a mean score of 4.44 and a standard deviation of 0.55. Similarly, the user satisfaction with the 2FA system prototype is high, as indicated by a mean score of 4.54 and a standard deviation of 0.51.*

Keywords *- AI in Education, Facial recognition technology, Mobile learning support, Pedagogical prototype, Two-factor authentication.*

1. Introduction

In the present era, characterized by the dominance of the digital sphere, human existence is primarily influenced by online activities, which are directly connected to daily behaviors. These activities include various behaviors, such as doing online transactions, making purchases, paying for products and services, communicating with colleagues, documenting client information, and monitoring account balances via online banking. The Internet has had a significant influence on human existence and has witnessed a worrisome surge in patterns. However, the Internet is commonly recognized as an extensive repository of information, providing online venues for users to engage in conversation, exchange their experiences, and avail themselves of a diverse array of convenient services. Due to these concerns, data security is imperative for individuals and companies. There exist specific crucial pieces of knowledge that are not suitable for public disclosure. To access computer systems, computer system security must diligently identify and address potential vulnerabilities that may compromise particular data, such as ID card information, credit card information, usernames, and passwords. Therefore, authentication is crucial and essential when entering any system to confirm the identity of the data owner. Authentication is the procedure of verifying and validating the accuracy and legitimacy of an individual's information. This can be achieved by directly communicating with the data owner or employing computer systems or artificial intelligence to analyse the data. Authentication is a crucial and necessary element of security protocols. During the authentication process, the user provides evidence of authorization to access the system or data. Presently, there are multiple forms and protocols for authentication, such as user

IDs, usernames, passwords, and biometric authentication. Each technique has its advantages and disadvantages. The predominant method of authentication in contemporary society is the utilization of usernames and passwords, which has been broadly embraced and firmly established as a customary procedure for a substantial duration. The main concern with username and password authentication is the vulnerability of user information to interception.

Furthermore, individuals are unaware that their data has been taken, and service providers are unsure about the user's ownership of the data. When the system has a significant impact, relying solely on username and password authentication is deemed inadequate and insufficient in terms of security, as it only involves a single authentication step to access the system. In order to resolve the problem mentioned before, researchers utilize a two-step verification method called Two-Factor Authentication (2FA) when users log in. 2FA is a security measure that requires two keys to access a system, much like having two doors. This signifies that the system has enforced a prerequisite for verifying at least two criteria to access the data or system. Usually, individuals are required to verify their identity by inputting their user ID and password to gain access to the system.

Subsequently, the system proceeds to authenticate the user's identity at the second tier, utilizing diverse techniques that align with the capabilities of the created system. Current examples of two-step verification methods include the transmission of a One-Time Password (OTP) by SMS, the encryption of code through emails, the use of a second verified device, the utilization of fingerprints, and other comparable approaches. Due to the improved efficiency of contemporary communication technologies, users now possess the capacity to transmit greater quantities of information across networks. Consequently, two-step verification has progressed to include facial recognition as a security feature. Facial recognition is an artificial intelligence approach that can assess and make comparisons between the facial features of individuals.

Facial recognition technology can swiftly and precisely recognize persons in photos or videos containing their faces. Afterwards, it compares the faces in the database to determine the identification of the detected face and then analyzes its unique facial features. Moreover, using facial recognition technology for unlocking or logging in reduces the user's need for physical contact with objects or surfaces that may transmit diseases like COVID-19. Facial recognition technology has become widely popular in several businesses and people's everyday routines. It is utilized to verify identities to gain access to highly secure places, monitor staff entry and exit times, record entry permissions for telephone systems, and validate users for online banking security systems. Facial recognition systems offer a straightforward and fast method of verifying someone's identity by quickly differentiating their face. This approach is more convenient and efficient than using cards and fingerprints for identification. To improve student achievement, educational institutions and organizations should prioritise creating information systems for education, even though there may be limited use of information technology and a lack of student engagement since many instructors heavily rely on cognitive teaching methods. Maximizing the capabilities of driving pupils is a step-by-step procedure, particularly given the transition from conventional classroom environments to online platforms, while encouraging sustainable learning. Academic instructors and educational institutions require the development of academic expert systems and educational technologies that improve the advancement of student learning. Currently, learners necessitate an information system that functions as a learning tool and is compatible with their learning behavior. Blended online learning and online mentoring are crucial elements in fulfilling the requirements of students. Moreover, concerns regarding the system's trustworthiness generate apprehension among children, discouraging them from accessing the system to seek help. Based on the observations reported earlier, the researchers proposed using facial recognition technology to improve instructional technologies. They accomplished this by creating a prototype for identification purposes, aiming to enhance the security of information systems that facilitate learning and provide online guidance for counselors and students. The researchers conducted a study and created a preliminary version of a two-factor authentication system. They employed two approaches to authenticate individuals, utilizing artificial intelligence technology incorporating facial recognition into the login process.

The prototype may verify users' identity by requiring the input of a username and password during the initial stage. The system will capture a facial image from a camera or webcam, which will be utilized for identity authentication in the subsequent stage to enhance security during system usage, as depicted in Figure 1 of the study framework. Figure 1 illustrates a study framework that uses two-factor authentication (2FA) to improve the functionality of academic information systems (AIS). The framework consists of two distinct study eras. The first phase entails constructing the two-factor authentication (2FA) login prototype. There are two elements, as depicted in Figure 2 and Figure 3.

The last phase entails implementing the two-factor authentication (2FA) login prototype to streamline access to academic information systems (AIS). This research proposal exclusively addresses the preliminary phase of the investigation, while the research has a wide-ranging reach. Assessing the efficacy of academic information systems requires conducting tests with actual users, who are the primary target audience based on research data. Figure 2 comprehensively describes the initial two-factor authentication (2FA) element that aids academic information systems (AIS).

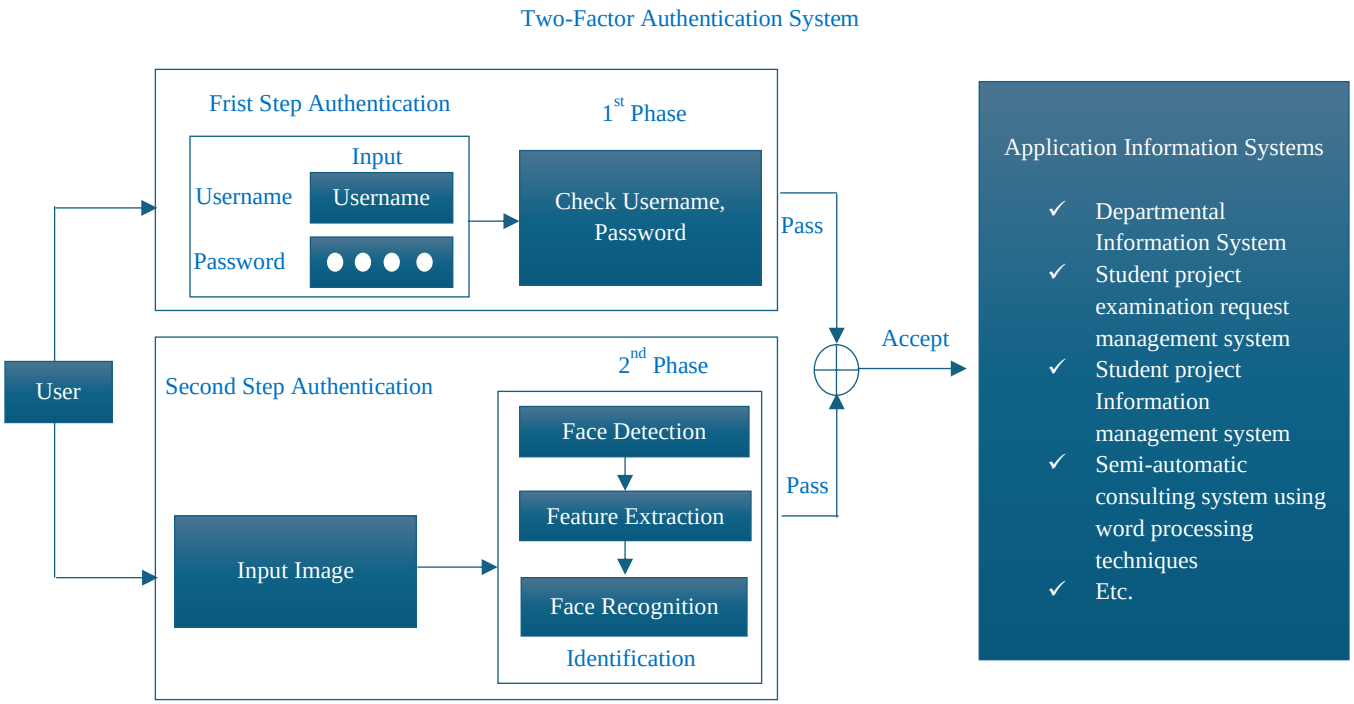

Fig. 1 The research framework

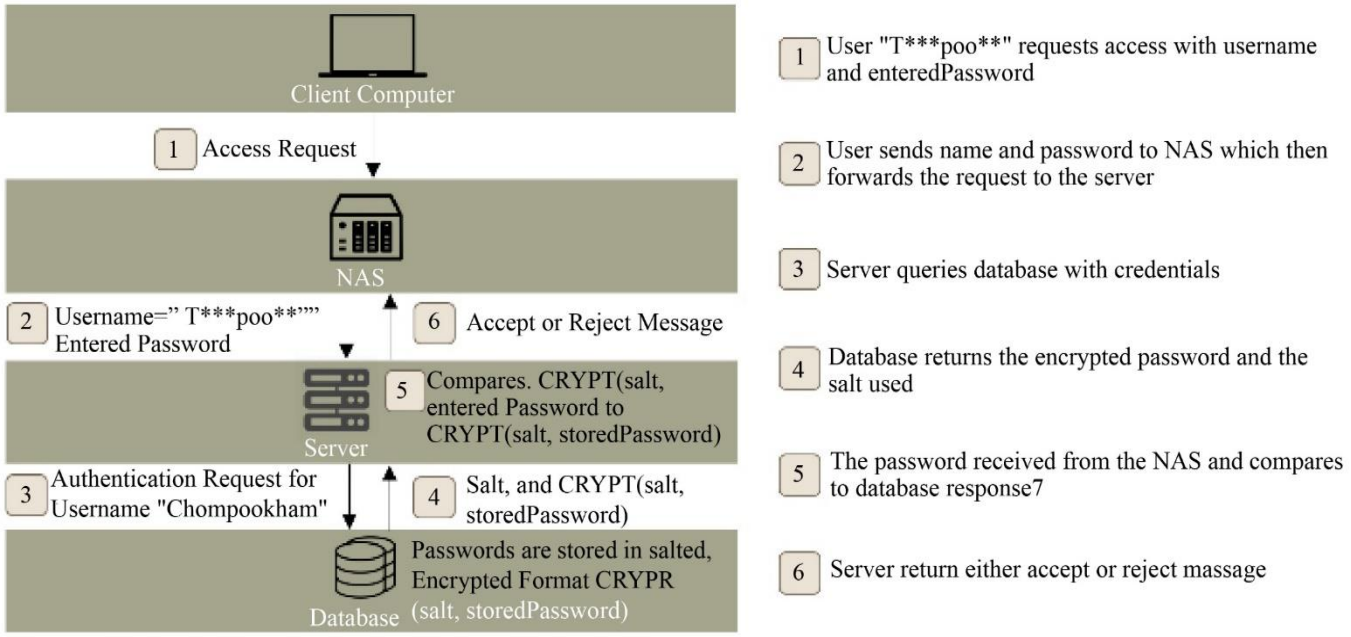

Fig. 2 The initial component of the two-factor authentication (2FA) system

The primary objective of this component is to create a robust authentication system that requires a username and password for secure login. The process comprises six sequential stages, elaborated in the materials and methods part and Pseudo Code, as specified in Table 4. Figure 3 provides a complete description of the second component of two-factor authentication (2FA), specifically designed to improve the security of academic information systems (AIS).

The main objective of the second phase is to incorporate facial recognition into the prototype of the two-factor authentication system with artificial intelligence. This integration will enhance the functionality of academic information systems, as described in the materials and techniques section, and will adhere to the Pseudo Code provided in Table 5. Significantly, it defined the study objectives, encompassing three main aims.

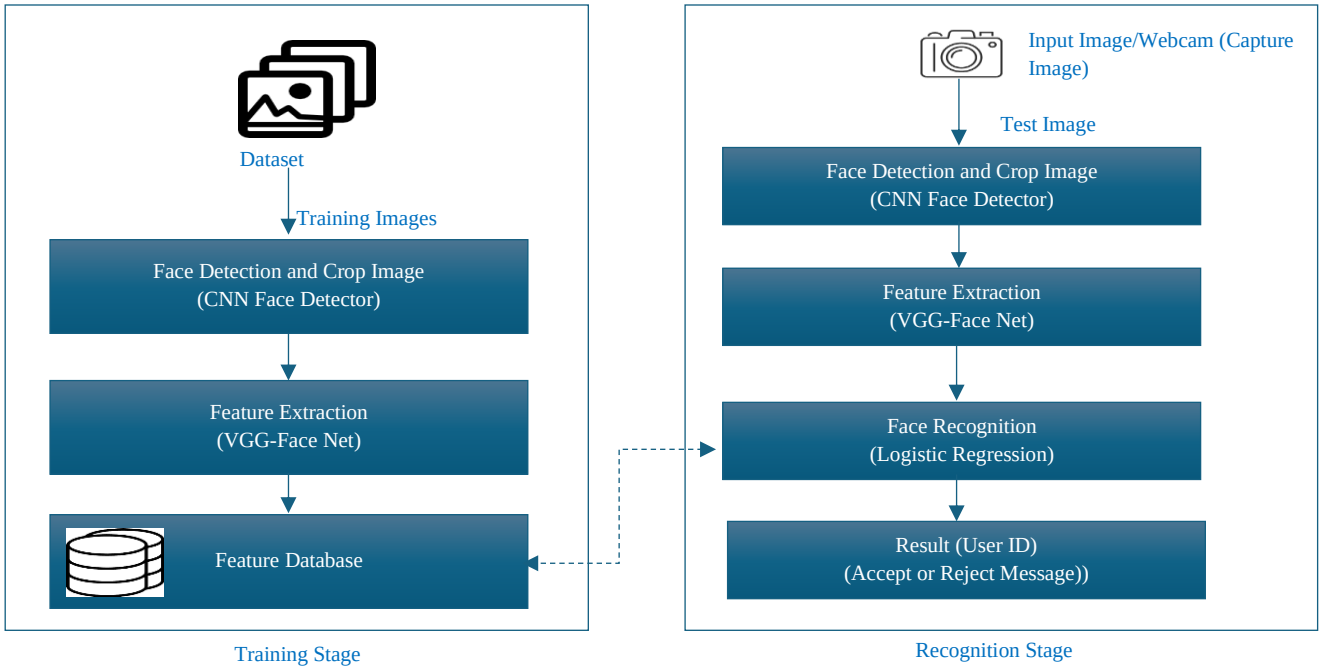

Fig. 3 The second component of the two-factor authentication (2FA) system

The study aimed to integrate the essential elements and technologies to prototype a two-factor authentication system that utilizes artificial intelligence technology. The second study objective was to prototype a two-factor authentication system using artificial intelligence technologies. This system would optimize the effectiveness and capability of identity verification while integrating robust security measures for system access. The third research objective involved evaluating the efficacy and studying the user response to the prototype of the two-factor authentication system utilizing artificial intelligence technology. The researchers are confident that this discovery will significantly benefit education, computer science, computer engineering, and related academic subjects in the future. Their unwavering will and diligent efforts will guarantee a substantial and enduring influence.

2. Literature Review and Related Works

2.1. Authentication System

Authentication systems must meet three fundamental criteria [1]: The primary criterion is to possess ample system resources for authorized users and the capability to deliver uninterrupted services to users with dependability. The second requirement is that the system must be able to preserve the integrity of the data, thereby preventing any unauthorized individuals from modifying it and safeguarding against unauthorized infiltration and manipulation of the data. The last determinant is confidentiality, which concerns the capacity to maintain the concealment and privacy of users. The system should incorporate safeguards to deter illegal access to data. Data encryption technology ensures the secrecy and accuracy of data within the system [2]. Adhering to these criteria is crucial when creating, implementing, and maintaining an authentication system to ensure reliability. The level of protection against unauthorized use and data access is determined by requirements, resources, priorities, and environment, which are established by suitable authentication [3].

2.2. Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an authentication principle that is applied to the login process by providing an additional layer of authentication to the system or a means of verifying at least two factors to increase the security of the system even more [4], [5], [6] There are three authentication factors.

- What you know, what you have, and who you are. What you know may be using passwords [7], [8], digital signatures [9], or personal data.
- What you have might be a smartcard [10], [11], Radio-Frequency Identification (RFID) [12], and Near-Field Communication (NFC) [13]
- Who you are is biometric identity [14], [15], [16] such as fingerprint, face, hand geometry, voice, and retina. Two-factor authentication means using an authentication method organized into two different authentication factors.

2.3. Face Recognition for User Authentication

Face recognition technology for authenticating users increases system security and prevents potential vulnerabilities [17]. Some features of facial authentication systems are that they utilize different people's facial

characteristics to create unique identities, increasing security and reducing the risk of unauthorized access through facial recognition technology. Facial recognition has the advantage of being easy to use and convenient, not disturbing users, and having no hardware requirements [18], [19]. Facial recognition requires image processing techniques and machine learning algorithms for face detection and identification. Rameswari et al. [20] present a method to encode faces in the input image using the Histogram Object Gradient (HOG) method and detecting faces using the Facenet algorithm. Then, the Support Vector Machine (SVM) method compares and classifies faces. Chen et al. [21] presented an efficient convolutional neural network model called Mobile Facenets, which uses less than 1 million parameters and can efficiently detect real-time faces on mobile devices. Sagar and Narasimha [22] developed a thoughtful and robust face detection-based lock system using facial detection and recognition algorithms, including the application of Principal Component Analysis(PCA), Histogram Equalization, and Linear Discriminant Analysis (LDA) where the system decides which algorithm to use to detect and recognize faces based on the current light intensity. Kim et al. [23] present a practical algorithm to improve recognition accuracy using a hierarchical deep neural network structure by extracting features from the appearance of a feature-based network fused with the geometric feature in a hierarchical structure.

2.4. Academic Information System (AIS)

The swift advancement of information technology presents a notable difficulty in implementing information systems [24]. It is necessary to carefully assess and implement suitable measures to guarantee results that align with the requirements and goals of technology users. Data processing in information technology includes acquiring, processing, storing, and managing data in diverse formats to derive high-quality information. An Academic Information System (AIS) is a data storage and management system that offers academic information services within educational institutions. Typically, it encompasses student details such as personal information, academic background, grades, and other information about the student's education at that institution [25]. Indrayani's study [26] defines AIS as a collection of methods and activities employed in higher education institutions to arrange, handle, and utilize information. AIS serves multiple purposes, including generating reports on activity performance, addressing hypothetical scenarios, facilitating decision-making, and assessing results in institutional development. AIS must address the requirements of various users, such as students, teachers, administrative personnel, and executives.

3. Materials and Methods

The prototype two-factor authentication system was developed by combining artificial intelligence, face recognition technology, and the conventional technique of validating identity using a login and password.

3.1. Population and Sampling

The study focuses on the attributes of the sample population and the process employed to choose participants. The study analysed the demographic characteristics of students, teachers, and staff associated with the Department of Computer Technology and Animation at the Faculty of Information Technology, Rajabhat Maha Sarakham University.

The study utilized purposive sampling methods, explicitly targeting a cohort of 40 individuals comprising students, lecturers, and staff affiliated with the Department of Computer Technology and Digital at the Faculty of Information Technology, Rajabhat Maha Sarakham University, for the academic year 2022. Participants granted their informed consent to utilize their data for research purposes. The researchers will abstain from disseminating or disclosing the acquired data without getting agreement from the individuals.

3.2. Data Collection

The data underwent three distinct phases. The initial stage involved gathering data to analyse and combine the many components of the academic information system. The second stage involved gathering data to create and construct a prototype two-factor authentication system utilizing artificial intelligence technologies. The third step involved collecting data to assess the system's quality and studying user approval of the prototype.

3.2.1. Academic Information Systems Synthesis Data

The purpose of the Data collection for the synthesis of academic information systems was to identify critical factors for creating a prototype of a two-factor authentication system utilizing artificial intelligence to enhance academic information systems.

This technique consisted of four steps.

- Step 1: The design of the research framework for developing a two-factor authentication system was a collaborative effort. In consultation with experts from various fields, including system development, context analysis, documentation, and research, researchers analyzed the system's boundaries, constraints, and issues.

- Step 2: We synthesized suitable components for a prototype of a two-factor authentication system that utilizes artificial intelligence to enhance academic information systems.

- Step 3: The synthesized elements were distributed to five experts to solicit their arguments and acceptance of the cumulative generalization of the elements for a prototype of a two-factor authentication system that utilizes artificial intelligence to enhance academic information systems. This process is elaborated in Table 1.

- Step 4: They analysed and summarised the results of synthesizing suitable components for the prototype of a two-factor authentication system using artificial intelligence. These findings are presented in Table 6.

3.2.2. Data for Designing and Development

The data-collecting process for prototype design and development was conducted by analysing the results and conclusions derived from synthesizing the relevant system components, with input from five experts. The results of the design and development of the prototype system were separated into two components. The initial element consisted of a sign-in system, as depicted in the operational architecture illustrated in Figure 2. The second element consisted of a facial recognition two-factor authentication system prototype, as described in the functional framework illustrated in Figure 3. The research tools section provides a comprehensive overview of the development process for each framework.

3.2.3. Data for Prototype Evaluation

The purpose of gathering data for testing and evaluating the prototype's effectiveness was to examine the level of satisfaction and acceptability toward the two-factor authentication system prototype, which utilizes artificial intelligence to assist academic information systems. Our team of dedicated researchers undertook this task with five meticulous steps, outlined below.

- Step 1: Our team of researchers meticulously developed a comprehensive and robust prototype for a two-factor authentication system trial, ensuring its quality and reliability.

- Step 2: The researchers created detailed questionnaires to evaluate the system's quality, as described in Table 2, and to provide a comprehensive analysis of user approval, as described in Table 3, of the prototype for the two-factor authentication system.

- Step 3: Researchers organized and requested collaboration from sample groups and experimented on the system prototype. During this phase, the researchers exercised control over, explained, clarified, and assisted the samples throughout the testing process.

- Step 4: Questionnaires were gathered and assessed for acceptability based on their sample questionnaires, and a prototype system was developed for testing activities with the samples.

- Step 5: The researchers condensed the questionnaire responses, summarized the reaction results, analysed the level of acceptability among the sample groups, assessed the performance of the system prototype, and deliberated on the findings, as documented in the assessment reports presented in Tables 10 and 11.

3.3. Research Tools

Four instruments were used for the research. The first instrument used was a questionnaire designed to assess the effectiveness of the prototype components of a two-factor authentication system that utilizes artificial intelligence technology to enhance academic information systems.

The initial questionnaire was created for assessment by specialists, as outlined in Table 1, and the results are presented in Table 7. The second instrument refers to the prototype of a two-factor authentication system that utilizes artificial intelligence to enhance academic information systems. This prototype is described and outlined in the part dedicated to its production.

The third instrument employed was a questionnaire designed to assess the efficacy of the prototype two-factor authentication system, which utilizes artificial intelligence to enhance academic information systems. This questionnaire was arranged for specialist assessment, as specified in Table 2, and the result is displayed in Table 10.

The fourth instrument was a questionnaire designed to assess the acceptance of the prototype two-factor authentication system, which incorporates artificial intelligence to enhance academic information systems. This survey was conducted to investigate the level of acceptance among a selected group, as outlined in Table 3, and yielded Table 11.

3.4. Prototype Construction and Quality of Tools

The conceptual notion of developing a prototype for a two-factor authentication system employing artificial intelligence to assist academic information systems is depicted in the study framework, shown in Figure 1. The structure and components comprised two primary elements. The primary element is creating and manufacturing a secure login system that requires a username and password, as depicted in the workflow illustrated in Figure 2.

The second element involves integrating a prototype of a two-factor authentication system that utilizes artificial intelligence to enhance the functionality of academic information systems, as described in Figure 3 of the framework. This section offers a comprehensive explanation of both frameworks.

3.4.1. Development of the 2FA System Prototype

The development of the 2FA system prototype commenced by incorporating a login mechanism that required the user to enter both a username and password.

The researchers developed an initial iteration of a two-factor authentication (2FA) system utilizing the Systems Development Life Cycle (SDLC) framework, which encompasses five distinct stages.

- Step 1: Planning

The system's development has been methodically and extensively planned. An extensive investigation was conducted to collect various user requirements, meticulously evaluate the details, and pinpoint the underlying reasons for the problems. Subsequently, these discoveries were crucial in creating and implementing the login system.

- Step 2: Performing system analysis

The data collected in Step 1 was analyzed to incorporate user requirements by developing a framework that addresses the varied system needs.

- Step 3: The procedure of system design.

The data acquired from the system analysis process was employed to build the database system and its associated procedures, influencing its design.

- Step 4: System development.

A fresh technique was developed by utilizing appropriate technologies. Information was acquired from the first round of data gathering, which involved the participation of five specialists. The precise research inquiries may be located in Table 1, while the accompanying analytical discoveries are displayed in Table 7.

The data in this section was employed to evaluate and select the most appropriate technology. Afterwards, the system underwent thorough testing, which included developing its installation, assessing its compatibility with the current system, and providing training to equip system users with the required information.

The login system is activated by entering a username and password. Figure 2 illustrates the arrangement, while Table 4 displays the Pseudo code.

- Step 5: System Maintenance

The researchers were following the completion of tests using the prototype of the 2FA system. Multiple modifications were implemented to complete and assemble a guidebook to improve system efficiency.

Table 1. Questionnaire to evaluate the suitability of 2FA prototype components

Stage	Details
CP1. Suitability of system components	
CP1.1	Suitability of members
CP1.2	Suitability of information
CP1.3	Suitability of user management
CP1.4	Suitability of two-factor authentication
CP1.5	Suitability of user permission
CP2. Suitability of technological components in system development	
CP2.1	Suitability of hardware
CP2.2	Suitability of code and programming
CP2.3	Suitability of database management system
CP2.4	Suitability of software for two-factor authentication
CP2.5	Suitability of reports via browser and platform

Table 2. Questionnaire for quality assessment

Stage	Details
AC1. Function test	
AC1.1	Completeness of prototype components
AC1.2	Completeness of prototype data presentation
AC1.3	Completeness of the prototype's data retrieval
AC1.4	Capabilities of signing in to the system
AC1.5	Two-factor authentication capabilities
AC2. Result test	
AC 2.1	Correctness of the system in adding data
AC 2.2	Correctness of the system in editing data
AC 2.3	Correctness of the system in deleting data
AC 2.4	Correctness of the system in two-factor authentication
AC 2.5	Correctness according to the framework of the system
AC3. Usability test	
AC3.1	Usability to access the data
AC3.2	Arrangement of system complexity
AC3.3	Overview of usability testing with the system

AC4. Security test	
AC4.1	Appropriateness to assign permissions to access data
AC4.2	Security in accessing data
AC4.3	Appropriateness of the overall security system

Table 3. Questionnaire for acceptance

Stage	Details
AC1. Perceived usefulness	
AC1.1	The system can effectively verify the identity of factor 1
AC1.2	The system can effectively verify the identity of Factor 2
AC1.3	The system can link information efficiently.
AC1.4	The system processes overall identity verification information correctly.
AC1.5	The identity verification system helps secure the work.
AC2. Perceived ease of use	
AC 2.1	Manual for recommending use
AC 2.2	The usage process is flexible and not complicated.
AC 2.3	Information systems can quickly access information.
AC 2.4	The information system uses visual explanations, content, and appropriate organization of elements to make it easy to understand
AC 2.5	The information system can be used anywhere and anytime via web browsers from many devices and all platforms.
AC3. Attitude towards use	
AC3.1	The user is satisfied with the system overall.
AC3.2	The user is satisfied with the system's process.
AC3.3	The user is satisfied with the stability of the system.
AC3.4	The user is satisfied with the manual that guides them using the system.
AC3.5	The user is satisfied with the manual that guides them using the system.

Table 4. Pseudo code for the first 2FA component

Pseudocode for the initial step of the authentication system
Input Username EnteredPassword
Process Authenticate by providing a Username and the corresponding EnteredPassword. The user sends their username and entered password to the Network-Attached Storage (NAS), which relays the request to the server. The server queries data from the database using authentication credentials. The database returns the encrypted password and the corresponding permissions. If the encrypted password in the database response matches the encrypted EnteredPassword returned from NAS, Then Server returns the accept Proceed to the second step authentication **Else** Server returns the reject Username or Password may be invalid or wrong
Try again

3.4.2. Second Stage of Development 2FA System Prototype

The second stage of creating the 2FA system prototype entailed integrating facial recognition technology into the existing 2FA system prototype.

A facial verification system was implemented by combining a human image recognition model into the 2FA system prototype. The system follows a five-step process, as depicted in Figure 4.

- Step 1: Data Preparation

The stage obtained image data of the provided sample groups. The dataset comprised 400 photographs, with ten images for each of the 40 students and teachers affiliated with the Faculty of Information Technology at Rajabhat Maha Sarakham University.

These photographs depicted the unique ambiance and overall surroundings.The data owner has explicitly granted permission to collect and utilize the data for research purposes.

The data was partitioned into two segments, with 80% allocated for evaluating the prototype system's performance and 20% designated for split testing.

Thus, 80% of the resources were spent on developing the prototype, while the remaining 20% were dedicated to testing its performance.

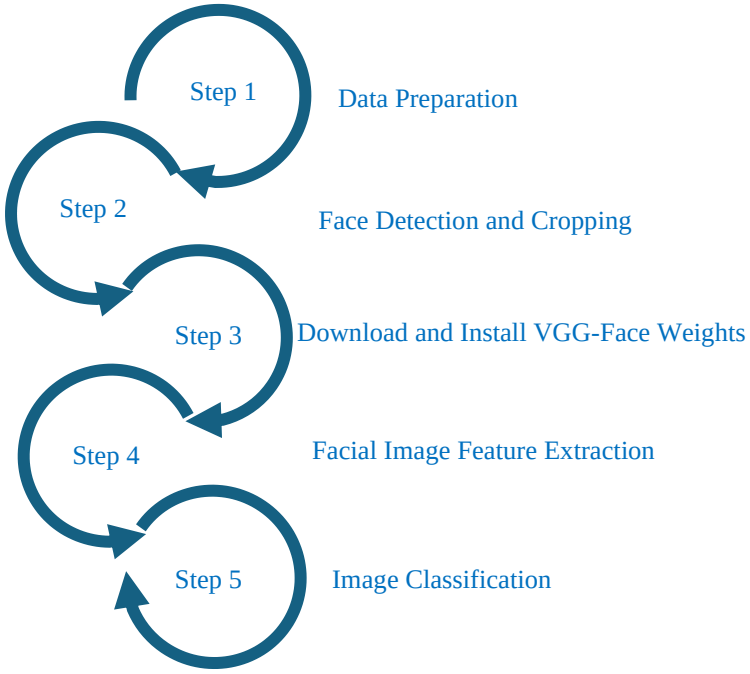

Fig. 4 Constructing a facial recognition module

- Step 2: Face Detection and Cropping.

At this stage, facial pictures were collected and analyzed. Researchers utilized the CNN-Face Detector, a powerful tool that accurately detects and locates faces in photographs and then returns this information to the system. Afterwards, the researchers cropped the facial photos for facial recognition.

- Step 3: Download and Install VGG-Face Weights.

It acquired pre-trained neural networks. The experiment utilized VGG-Face Net, a neural network that has undergone rigorous training on a vast dataset of facial photos to recognize human faces precisely.

- Step 4: Facial Image Feature Extraction.

The VGG-Face Net model extracted picture features from the generated pages. Subsequently, each image was assigned the name of the data owner.

- Step 5: Image Classsification.

In this step, a machine learning algorithm was employed to generate and categorize photographs by randomly splitting the experimental data into two distinct datasets. The datasets were later used to create and evaluate a "Split Test" model, with 80% of the data used for development and 20% used for testing. 80% of the initial dataset was utilized to build a model, with the data being divided into two smaller segments. During the initial stage, 70% of the resources were allocated towards developing the prototype model.

The subsequent portion assigned 10% of the resources to validate the model. An equivalent of 20% of the remaining data was allocated to evaluate the prototype's efficiency. The data was classified, and then a machine learning model was created using four classifiers: K-Nearest Neighbors (K-NN), Logistic Regression (LR), Multi-Layer Perceptron (MLP), and Support Vector Machine (SVM). The results of the prototype development, utilizing the four strategies, are outlined in the part dedicated to the prototype development report. The second element of the 2FA system prototype demonstrates the functioning of the process in the Pseudo code, as depicted in Table 5.

Table 5. Pseudo code for the second 2FA

Pseudo code the Second Step Authentication System
Input Username Image (from computer) or capture image (from webcam)
Process Face detection and crop image by CNN face detector Face image feature extraction will use the VGG-Face-Net model. Classify image using a trained Logistic Regression model. **If** the model return classification results (Username) and Username input are the same, Then Server return accept Enter academic information system: AIS **Else** Server return reject
Try again

Table 6. The Confusion matrix

	Actually Positive	Actually Negative
Predicted Positive	True Positive (TP)	False Positive (FP)
Predicted Negative	False Negative (FN)	True Negative (TN)

After developing the two-component subsystems, a prototype system was created for testing. The test target group consisted of two parts: 5 experts and 40 students and instructors. Tables 10 and 11 display the test results and satisfaction study data.

3.5. Model Performance Assessment

The confusion matrix technique and four indicators—accuracy, precision, recall, and F1-Score—were used to evaluate the machine learning models' performance with four classifiers. From the confusion matrix shown in Table 5, the four indicators used to determine the model performance are displayed in Equation (1) to (4).

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1-Score = 2 * (\frac{Precision*Recall}{Precision+Recall}) \quad (4)$$

Where, True Positive (TP) and True Negative (TN) mean what was predicted matches what happened. In contrast, False Positive (FP) and False Negative (FN) mean what was predicted miss-matches what happened.

3.6. Research Analysis and Interpretation

The Statistics used in data analysis. The collected data was analysed, and results were summarized as mean and Standard Deviation (S.D.). A rating scale used in the study of acceptance and satisfaction consisted of 5 levels. A score of 5 = very satisfied; 4 = somewhat satisfied; 3 = neither satisfied nor dissatisfied; 2 = slightly dissatisfied; 1 = very dissatisfied. The rating scale was used with experts and sample groups, as shown in the questionnaire details in Table 1 and Table 2.The acceptance and satisfaction levels data were interpreted using five interval levels. A mean result between 1.00 and 1.80 at level 1 indicates a highly undesirable state. A mean value falling from 1.81 to 2.60 is deemed unsatisfactory at level 2. If the average number falls between 2.61 and 3.40 at level 3, it suggests a neither acceptable nor unacceptable state. A mean value falling within the range of 3.41 to 4.20 was deemed sufficient for level 4. A mean number between 4.21 and 5.00 at level 5 signifies a high level of acceptability. The data analysis and interpretation of acceptance and satisfaction levels were condensed and shown in Tables 7, 10, and 11.

4. Results

The investigation and construction of a prototype 2FA system utilizing artificial intelligence to enhance academic information systems yielded three key findings, documented in sections 4.1, 4.2, and 4.3. The first aspect pertains to the study's findings and the synthesis of components inside the information system. The second aspect pertains to the results derived from designing and creating the prototype for the 2FA system. The third aspect involves the experts' and sample groups' acceptance of the 2FA system prototype.

4.1. Synthesis of the 2FA System Prototype Components

The experts' input on the components necessary for constructing the 2FA system prototype was summarized and utilized to design the system process, as depicted in Figure 5. The findings of their evaluation of the acceptability of the 2FA system prototype module were reported and summarized in Table 7. Figure 5 illustrates that the 2FA system prototype comprised four modules. The Authentication Module is a component that offers authentication functionality for system access. Users are required to complete a two-step login process. Initially, the user must input a username and password.

As part of the second phase, users must authenticate their identity by capturing a photo using a camera. To log in, users must complete both stages. The Member Module is a component designed to store and manage data related to members. The recorded data includes information about both students and instructors. The individuals capable of documenting information are students and instructors. The Information Module is designed to contain many components of information from the Academic Information System (AIS). Only instructors are allowed to record information. The purpose of the Management Module is to streamline the process of managing member data access permissions. According to Table 7, the experts expressed that the components utilized in developing the 2FA prototype system were highly acceptable.

4.2. Results of the 2FA Prototype Systems' Development

The development results of the 2FA prototype system, which utilizes artificial intelligence to enhance academic information systems, are categorized into two sections. The initial section comprehensively analyses the progress in creating the facial recognition model. The second section entails a comprehensive report detailing the execution of the prototype system.

4.2.1. Facial Recognition Model

The development results of the prototype model of the human face verification system using the facial recognition module were tested for model performance with the steps shown in Figure 4. To test the performance of the facial recognition module, it was run on Google Colab. The experiment used A CNN-Face Detector to detect faces and

crop facial images. Following that, VGG-Face Net was used to extract image features and assign labels to the images. Once the facial image data was prepared, the data was divided into two parts for testing: a training set with 80% of the data and a testing set with 20% of the data.

The researchers used the first 80% of the data to develop a model using four classifiers: K-Nearest Neighbours (K-NN), Logistic Regression (LR), Multi-Layer Perceptron (MLP), and Supports Vector Machine (SVM), as detailed parameters in the experiment as shown in Table 8. Once the models from each technique were obtained, the remaining 20% of the data was tested with a confusion metric technique and four indicators. The test results for each classifier are reported in Table 9. The data in Table 9 demonstrates that the categorization efficiency test produced results with an accuracy surpassing 80 percent. The Logistic Regression (LR) classifier achieved an accuracy of 83.54%, while the Support Vector Machine (SVM) classifier achieved an accuracy of 81.01%. Therefore, the Logistic Regression (LR) model was chosen to be integrated into the login system in the facial recognition module because of its exceptional precision.

4.2.2. Implementing the Prototype System

Facial recognition technology in the 2FA prototype system has effectively streamlined user authentication in deploying Academic Information Systems (AIS) that require a login and password.

AIS development involves utilizing code programs written in PHP, Python, HTML5, CSS3, JavaScript, and a MySQL database system. To evaluate the effectiveness of the facial recognition authentication system, researchers utilized OKER-A229 cameras with a resolution of 1920×1080 pixels (Full HD-1080p). The system categorizes users into two distinct groups: students and teachers. Each user group possesses distinct permissions. Figures 6 and 7 depict the whole two-part login system. Upon accessing the system, users are granted access to all academic information systems within the Department of Computer Technology and Digital, Faculty of Information Technology, Rajabhat Maha Sarakham University.

4.3. Performance and Acceptance of the 2FA System

After the two systems were integrated, the system underwent testing, and arrangements were established to ssess the quality of the 2FA system prototype, which was separated into two groups.Group one comprised five experts, whereas group two was a specifically chosen sample of 40 students and instructors, as documented in Tables 10 and 11.

Table 10 indicates that the experts expressed high satisfaction and rated the overall quality of the 2FA system prototype as strongly acceptable. Upon careful evaluation, it was determined that the security and functionality testing components of the 2FA system prototype were highly satisfactory. The test results on the performance and ease of use of the 2FA system prototype met the acceptable criteria. Table 11 shows that the samples' satisfaction and acceptance of the overall quality of the 2FA system prototype is at a strongly acceptable level. When considering each aspect, it was found that the perceived usefulness, ease of use aspects, and attitude towards using the 2FA system prototype are strongly acceptable.

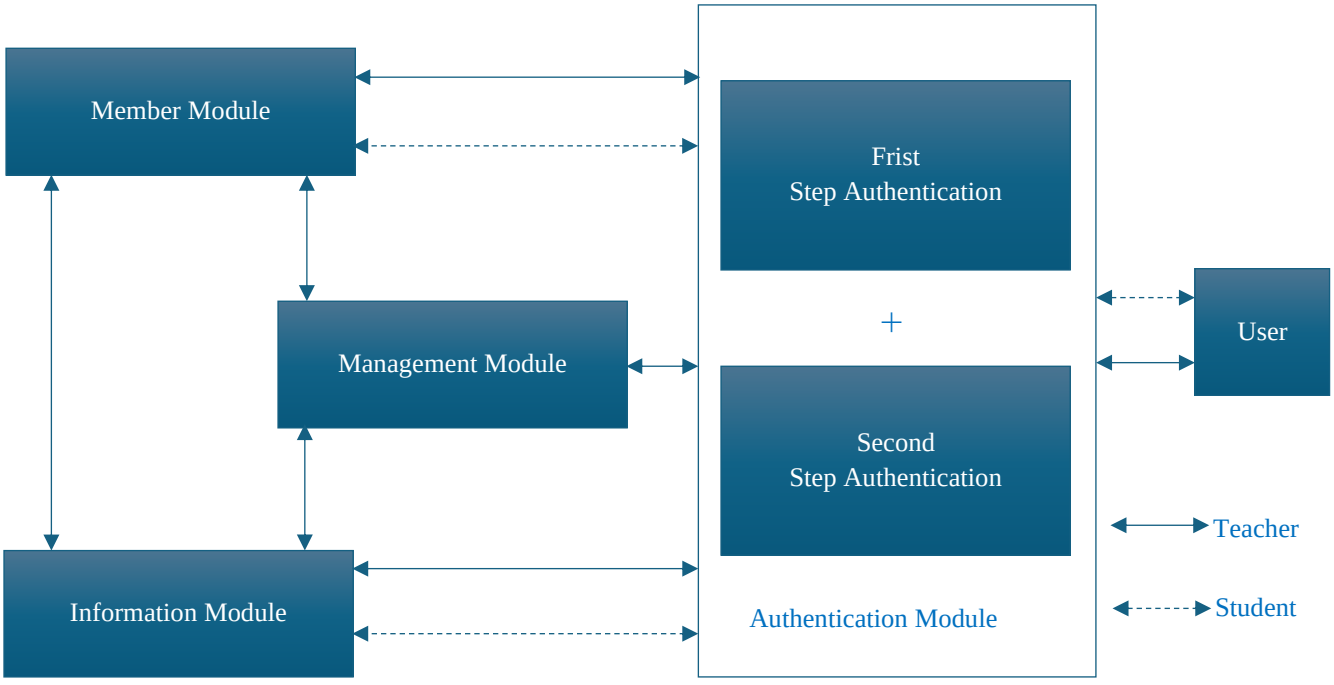

Fig. 5 The components of the 2FA system prototype

Table 7. Summary of the Experts' acceptance of the 2FA prototype components

Stage	Mean	S.D.	Interpretation
CP1. Suitability of system components			
CP1.1	4.40	0.55	Strongly Acceptable
CP1.2	4.60	0.55	Strongly Acceptable
CP1.3	4.40	0.55	Strongly Acceptable
CP1.4	4.80	0.45	Strongly Acceptable
CP1.5	4.60	0.55	Strongly Acceptable
Average:	4.56	0.51	Strongly Acceptable
CP2. Suitability of technological components in system development			
CP2.1	4.20	0.45	Acceptable
CP2.2	4.40	0.55	Strongly Acceptable
CP2.3	4.60	0.55	Strongly Acceptable
CP2.4	4.60	0.55	Strongly Acceptable
CP2.5	4.60	0.55	Strongly Acceptable
Average:	4.48	0.51	Strongly Acceptable
Total Average:	4.52	0.50	Strongly Acceptable

Table 8. Parameter in the experiment

Classifiers	Hyperparameters	Search Space	Bast Parameters
K-Nearest Neighbors (K-NN)	n-neighbors	[1, 15]	1
Logistic Regression (LR)	solvers penalty c_values max_iters	['lbfgs', 'newton-cg', 'sag', 'saga', 'liblinear'] ['l2', 'l1', 'none'] [100, 10, 1.0, 0.1, 0.01] 100 - 2000	Sag none 1.0 500
Multi-Layer Perceptron (MLP)	max_iters beta alpha activation solver	100 - 2000 0.1 - 0.9 0.0001 - 0.1 ['sigmoid', 'relu', 'Tanh'] ['lbfgs', 'sgd', 'adam', default='adam']	200 0.9 0.0001 relu adam
Supports Vector Machine (SVM)	c gamma kernel	[0.1 - 50] [0.0001 - 1] ['liner', 'rbf']	20 0.001 rbf

Fig. 6 Login with a username and password

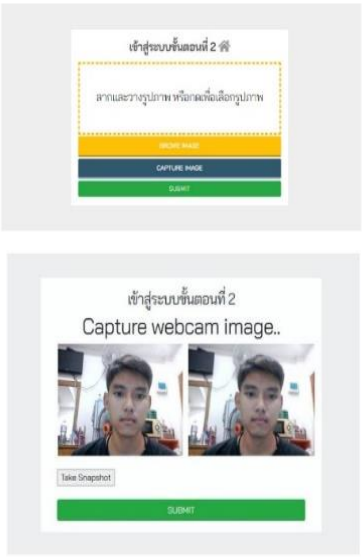

Fig. 7 Login with facial recognition

Table 9. Performance for each classifier

Classifiers	Accuracy (%)	Precision	Recall	F1-Score
K-NN	75.94	0.76	0.74	0.73
LR	83.54	0.84	0.88	0.83
MLP	78.48	0.78	0.81	0.76
SVM	81.01	0.81	0.84	0.80

Table 10. Acceptance from experts

Stage	Mean	S.D.	Interpretation
AC1. Function test			
AC1.1	4.60	0.55	Strongly Acceptable
AC1.2	4.40	0.55	Strongly Acceptable
AC1.3	4.60	0.55	Strongly Acceptable
AC1.4	4.60	0.55	Strongly Acceptable
AC1.5	4.40	0.55	Strongly Acceptable
Average:	4.52	0.51	Strongly Acceptable
AC2. Result test			
AC 2.1	4.20	0.84	Acceptable
AC 2.2	4.60	0.55	Strongly Acceptable
AC 2.3	4.20	0.45	Acceptable
AC 2.4	4.60	0.55	Strongly Acceptable
AC 2.5	4.40	0.55	Strongly Acceptable
Average:	4.40	0.58	Strongly Acceptable
AC3. Usability test			
AC3.1	4.00	0.71	Acceptable
AC3.2	4.40	0.55	Strongly Acceptable
AC3.3	4.40	0.55	Strongly Acceptable
Average:	4.27	0.59	Acceptable
AC4. Security test			
AC4.1	4.40	0.55	Strongly Acceptable
AC4.2	4.80	0.45	Strongly Acceptable
AC4.3	4.40	0.55	Strongly Acceptable
Average:	4.53	0.52	Strongly Acceptable
Total Average:	4.44	0.55	Strongly Acceptable

Table 11. Acceptance from sample groups

Stage	Mean	S.D.	Interpretation
AC1. Perceived usefulness			
AC1.1	4.50	0.51	Strongly Acceptable
AC1.2	4.40	0.50	Strongly Acceptable
AC1.3	4.55	0.50	Strongly Acceptable
AC1.4	4.55	0.55	Strongly Acceptable
AC1.5	4.65	0.48	Strongly Acceptable
Average:	4.53	0.51	Strongly Acceptable
AC2. Perceived ease of use			
AC 2.1	4.58	0.55	Strongly Acceptable
AC 2.2	4.45	0.55	Strongly Acceptable
AC 2.3	4.50	0.55	Strongly Acceptable
AC 2.4	4.50	0.51	Strongly Acceptable
AC 2.5	4.68	0.47	Strongly Acceptable
Average:	4.54	0.53	Strongly Acceptable
AC3. Attitude towards use			
AC3.1	4.65	0.48	Strongly Acceptable
AC3.2	4.53	0.51	Strongly Acceptable
AC3.3	4.50	0.51	Strongly Acceptable

AC3.4	4.58	0.50	Strongly Acceptable
AC3.5	4.65	0.48	Strongly Acceptable
Average:	4.56	0.50	Strongly Acceptable
Total Average:	4.54	0.51	Strongly Acceptable

5. Discussion

Three issues emerge from this work and require discussion.

- Evaluation of the component quality of the 2FA system prototype, which incorporates artificial intelligence technology specifically developed to improve academic information systems (AIS). Table 7 indicates that experts agree that the components and technologies used in the development process are very suited.

- The assessment of the efficiency of constructing a facial recognition model, as indicated in Table 9, resulted in the maximum degree of accuracy, reaching 83.54%. The error in evaluating efficiency can be ascribed to the limited availability of image datasets and the utilization of particular images in the experiment. The photos had diminutive dimensions and exhibited subpar resolution, leading to inaccuracies in identifying human faces and compromising the efficacy of image recognition. It is recommended that high-resolution pictures be used for future investigations and to explore the application of deep learning or other more efficient approaches.

- The data summary from the quality evaluation and acceptance study of the 2FA system prototype, which uses artificial intelligence technology created for academic information systems, is shown in Tables 10 and 11. Experts highly praised the system's overall quality, and consumers likewise strongly accepted the system's general use. The researcher has examined the factors contributing to identity verification challenges to integrate them into the development and design of information systems. The result is the creation of a prototype for a 2FA system that employs artificial intelligence technologies specifically tailored to assist academic information systems. By using the SDLC method, artificial intelligence technology can be used for two-factor authentication, improving the efficiency of identity verification and guaranteeing secure access to academic information systems. This academic information system efficiently manages, analyzes, and supervises activity data and offers responses to inquiries within the Department of Computer Technology and Digital, Faculty of Information Technology, Rajabhat Maha Sarakham University.

6. Conclusion

This article describes the research and development of the 2FA system prototype, which uses artificial intelligence technology developed to support academic information systems. The prototype consists of three main parts.

- Part 1. Studying the components of the 2FA system prototype to support academic information systems development, which consists of 4 modules: 1) Authentication Module, 2) Member Module, 3) Information Module, 4) Management Module, and experts agreed that the components and technology used in system development were overall strongly acceptable level.

- Part 2. The design and development of the 2FA system prototype, which uses artificial intelligence technology to emphasize accuracy, completeness, and security in verifying identity before accessing academic information systems, was divided into two phases. The first phase was developing a face recognition model consisting of a CNN Face Detector, VGG-Face net, and classification with Logistic Regression (LR), which achieved the highest accuracy of 83.54% compared to other methods. The second phase developed an Academic Information System (AIS) for username and password login combined with a facial recognition model to authenticate users through two-factor authentication. It was developed using PHP, Python, HTML5, CSS3, JavaScript, and a database system with MySQL. The developed system consisted of 2 types of users: teachers and students.
- Part 3. Evaluating system quality and inquiring about user acceptance of the 2FA system prototype to support academic information systems was divided into two components. - 1) Evaluation of the quality of the system by experts found that the opinions of the experts on the overall quality of the system were at the strongly acceptable level, and 2) Acceptance of the use of the 2FA system prototype to support academic information systems overall in a strongly acceptable level.

7. Limitations and Suggestions

7.1. Suggestions for Applying the Research Results

This research has produced a 2FA system prototype that used artificial intelligence technology and emphasized accuracy, completeness, and security in verifying identity before accessing academic information systems. However, suppose the results of this research are to be used practically. In that case, there is a need to collect more data used in facial recognition and training the facial image recognition module to recognize individuals.

7.2. Suggestions for Future Research

Future research should study the nature of identity verification by additional methods such as fingerprint scanning or personal voice recognition or increase recognition efficiency and combine each classification result obtained (ensemble method).

Acknowledgments

This research project was supported by the Rajabhat Maha Sarakham University, the Thailand Science Research and Innovation Fund, and the University of Phayao. In addition, this research was supported by many advisors, academics, researchers, staff, and students. The authors would like to thank all of them for their support and collaboration in making this research possible.

References

[1] Yasser M. Hausawi, William H. Allen, and Gisela Susanne Bahr, "Choice-Based Authentication: A Usable-Security Approach," *In Universal Access in Human-Computer Interaction, Design and Development Methods for Universal Access*, Heraklion, Crete, Greece, pp. 114-124, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[2] Vashek Matyáš, and Zdeněk Říha, "Security of Biometric Authentication Systems," *In 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*, Krakow, Poland, pp. 19-28, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[3] Sarah Abdulkader, Ayman Atia, and Mostafa-Sami Mostafa, "Authentication Systems: Principles and Threats," *Computer and Information Science*, vol. 8, no. 3, pp. 155-179, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[4] Tance Suleski et al., "A Review of Multi-Factor Authentication in The Internet of Healthcare Things," *Digital Health*, vol. 9, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Zigang Chen et al., "FSMFA: Efficient Firmware-Secure Multi-Factor Authentication Protocol for IoT Devices," *Internet Things*, vol. 21, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Tok Yen Xin, Norliza Katuk, and Ahmad Suki Che Mohamed Arif, "Smart Home Multi-Factor Authentication Using Face Recognition and One-Time Password on Smartphone," *International Journal of Interactive Mobile Technologies (IJIM)*, vol. 15, no. 24, pp. 32-48, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mariam. M. Taha et al., "On Password Strength Measurements: Password Entropy and Password Quality," *In 2013 International Conference on Computing, Electrical and Electronics Engineering (ICCEEE)*, Khartoum, Sudan, pp. 497-501, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[8] Eliana Stavrou, "Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools," *In 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, Glasgow, UK, pp. 1-4, 2018.

[9] Zahoor Ahmed Alizai, Noquia Fatima Tareen, and Iqra Jadoon, "Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures," *In 2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, Taxila, Pakistan, pp. 1-5, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Franck Favier, "Smart Cards and Healthcare," *Card Technology Today*, vol. 19, no. 11-12, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[11] T. İ. Gündem, and Ö. Armağan, "Efficient Storage of Healthcare Data in XML-Based Smart Cards," *Computer Methods and Programs in Biomedicine*, vol. 81, no. 1, pp. 26-40, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[12] Junbin Kang et al., "An Ultra-Light Weight and Secure RFID Batch Authentication Scheme for IoMT," *Computer Communications*, vol. 167, pp. 48-54, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Sakhaa B. Al-Saedi, and Mohamed Mostafa A. Azim, "Radio Frequency Near Communication (RFNC) Technology: An Integrated RFID-NFC System for Objects' Localization," *In 2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, Manama, Bahrain, pp. 1-5, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[14] Anu Rathi et al., "Improvement of Existing Security System by Using Elliptic Curve and Biometric Cryptography," *In International Conference on Computing, Communication & Automation*, Greater Noida, India, pp. 994-998, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[15] Philip Black, "Building A Trusted Guardian for Our Biometric Identities," *Biometric Technology Today*, vol. 2021, no. 6, pp. 7-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Chunhua Jin et al., "EBIAC: Efficient Biometric Identity-Based Access Control for Wireless Body Area Networks," *Journal of Systems Architecture*, vol. 121, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Yasmin Makki Mohialden, Nadia Mahmood Hussien, and Doaa Muhsin Abd Ali, "Enhancing User Authentication with Facial Recognition and Feature-Based Credentials," *Journal La Multiapp*, vol. 4, no. 6, pp. 243-252, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohammed Abdulhakim Al-Absi et al., "Real-Time Access Control System Method Using Face Recognition," *In Proceedings of International Conference on Smart Computing and Cyber Security*, Springer, Singapore, pp. 101-108, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Gabit Tolendiyev, Hyotaek Lim, and Byung-Gook Lee, "A Margin-based Face Liveness Detection with Behavioral Confirmation," *International Journal of Internet, Broadcasting and Communication*, vol. 13, no. 2, pp. 187-194, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] R. Rameswari, "Automated Access Control System Using Face Recognition," *Materials Today: Proceedings*, vol. 45, pp. 1251-1256, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Sheng Chen et al., "MobileFaceNets: Efficient CNNs for Accurate Real-Time Face Verification on Mobile Devices," *In Biometric Recognition, In Lecture Notes in Computer Science*, Springer, Cham, pp. 428-438, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] D. Sagar, and Murthy K. R. Narasimha, "Development and Simulation Analysis of a Robust Face Recognition Based Smart Locking System," *In Innovations in Electronics and Communication Engineering, in Lecture Notes in Networks and Systems*, Springer, Singapore, pp. 3-14, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Ji-Hae Kim et al., "Efficient Facial Expression Recognition Algorithm Based on Hierarchical Deep Neural Network Structure," *IEEE Access*, vol. 7, pp. 41273-41285, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[24] Melda Agnes Manuhutu, Lulu Jola Uktolseja, and Sherly Gaspersz, "Academic Information System for Student (Case Study: Victory University of Sorong)," *International Journal of Computer Applications*, vol. 180, no. 43, pp. 26-33, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] H. P. Utomo, A. T. Bon, and M. Hendayun, "Academic Information System Support in the Era of Education 3.0," *International Research and Innovation Summit (IRIS2017)*, Melaka, Malaysia, vol. 226, no. 1, pp. 1-9, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] Etin Indrayani, "Management of Academic Information System (AIS) at Higher Education in the City of Bandung," *Procedia - Social and Behavioral Sciences*, vol. 103, pp. 628-636, 2013. [CrossRef] [Google Scholar] [Publisher Link]