Recent Science and Technology

Journal homepage: https:// www.tci-thaijo.org/index.php/rmutsvrj/index

ISSN: 3057-0786 (Online)

Research Article

Establishment of an Application for Student Activity Attendance at a Community College Using a Digital Identity Methodology

Werachart Muttitanon, Chumpol Mokarat * and Saowakhon Nookhao

Department of Information Technology, Faculty of Business Administration and Information Technology, Rajamangala University of Technology Tawan-Ok: Chakrabongse Bhuvanath, Din Daeng, Bangkok 10400, Thailand.

Article history:

Received: 2024-10-30
Revised: 2025-02-21
Accepted: 2025-03-03

Keywords:

activity attendance application;
digital Identity;
OAuth 2.0

ABSTRACT

This article presents the design and development of an application for student activity attendance at a community college using a digital identity methodology. The objective of this research is to facilitate the development of an application that leverages digital identity methodologies to streamline activity attendance tracking and enhance participant monitoring and reporting processes. That can assist community college instructors by allowing students to participate in attendance at activities and control their training and education through various types of flexible courses. The proposed application is a web application that incorporates responsive web design to ensure web pages render seamlessly on mobile devices. It utilizes server-side services powered by NodeJS programming, a Firebase database for data storage, and an interface driven by the React framework. We implemented OAuth 2.0 as a standard for user authentication and access to Google services to simplify working with system security. During the OAuth 2.0 user authentication evaluation it was discovered that testing 50 experiments users to test student activity registration, with five activities per person and each user contributing the response time, produced the desired results. The distance verification process had the longest testing duration, with completion times varying significantly depending on the user devices. On the other hand, the logout process consistently showed the shortest completion times. In addition, the findings from the users' evaluations of the system's use showed that the average score, as indicated by the evaluation, was very high ($\bar{X}$ =4.72, SD=0.39). In general, the majority agreed that the newly implemented approach was more practical and efficient than the previous recording approach.

1. Introduction

Information technology management plays a crucial role in the information operations of both public and private organizations. Various systems have integrated digital authentication models, such as the Digital Signature (The Bureau of Registration Administration, 2024). Examples include a prototype of seminar registration system using facial authentication (Sainui *et al*., 2021), two-factor authentication for web applications (Puntumnunt and Sompong, 2024), and the digital verification and authentication system in the ThaID application (ThaID) (The Bureau of Registration Administration, 2024). The operation of these models requires the integration of various technical aspects to

*** Corresponding author.**

E-mail address: *chumpol_mo@rmutto.ac.th*

Cite this article as:

Muttitanon, W., Mokarat, C. and Nookhao, S. 2025. Establishment of an Application for Student Activity Attendance at a Community College Using a Digital Identity Methodology. **Recent Science and Technology** 17(2): 265181.

ensure that the digital systems are utilized efficiently, effectively support operations, and maintain safety and reliability. Additionally, two-factor authentication (2FA) (Microsoft (Thailand) Co., Ltd., 2024) and multi-factor authentication (MFA) (Amazon Web Services, 2024) are implemented to enhance authentication accuracy and the security of identity management systems as well as to control access to essential resources, such as networks and databases. These measures also contribute to the implementation of information technology security protocols, including enhancements to the architectural design of OAuth 2.0 to address and mitigate common security vulnerabilities (Singh and Chaudhary, 2022). Furthermore, these authentication methods can be applied in various approaches to identity verification and authentication, including: the empirical measurement of systemic 2FA usability (Reynolds *et al.*, 2020); a systematic literature review on online banking user authentication methods (Karim *et al.*, 2023); and a comprehensive analysis of a multifactor authentication system for three-level security (Kantipudi *et al.*, 2024). This also includes enhancements to password storage through the integration of cryptarithmetic techniques and hash functions (Polpong *et al.*, 2024). Additionally, authentication, validation, and authorization within Forestry 4.0 using OAuth 2.0 are employed to manage the security of communication between devices in the IoT industry (Chen *et al.*, 2022). Furthermore, a study examines the implementation of OAuth 2.0 and OpenID Connect by popular service providers and top-ranked Android clients, analyzing their adherence to best practices for developing secure native applications to assist developers in ensuring the security of their applications (Sharif *et al.*, 2022). Moreover, a time attendance web application was developed using authentication with images and location within a private university to study staff acceptance of the system. The application was developed with PHP, JavaScript, and jQuery to enable authentication through photographs and geographic location, record work activities, and generate summary reports (Sittijuk and Sanchana, 2024). The application of these approaches has led to improvements in identity verification methods, including facial recognition, fingerprint verification, and the integration of new algorithms. Additionally, the adoption of multi-level authentication methods, management of communication security for IoT devices, the analysis of adherence to best practices in native app development, and the development of time attendance web applications contribute to enhancing the security and efficiency of systems at a higher level. Importantly, users experience reduced costs and operational burdens. Furthermore, adopting this approach to identity verification can also be seamlessly integrated into the information technology practices within organizations.

The Community College Institution is a government agency that provides sub-bachelor-level higher education and is managed by community colleges. Its objective is to offer academic and vocational education and training through curricula aligned with community needs. It plays a key role in promoting career development and enhancing the quality of life for individuals within the community (Office of the Higher Education Commission, Ministry of Education, 2003). In this project, implementation efforts aim to encourage student participation in activities and facilitate diverse and flexible educational and training programs. Currently, community colleges still record student's activity participation by requiring them to sign in with the staff responsible for monitoring the activity. This process involves verifying student ID cards and subsequently entering the information into a computer system. However, this method is prone to errors and the potential loss of documents, leading to issues in accurately recording students' activity participation. Therefore, implementing a digital authentication approach to manage student participation in activities offers a more efficient solution. This method incorporates identity verification data, including authentication details, date/time, and user location coordinates (calculated distance). Additionally, it facilitates tracking and enables the distribution of activity participation evaluations for further assessment. The previous system relied solely on paper-based operations, which imposed limitations on verification, tracking, and reporting of participant data for purposes such as identity verification and attendance records. This

process requires a digital identity verification and authentication system to validate user credentials and authorize access to various system services. It involves identifying the user's location, proximity, and device access. Additionally, digital identity verification is employed when participants engage in activities that require identity confirmation. Multi-factor authentication (MFA) is essential, involving a multi-step login process that requires users to provide additional information beyond just a password. This approach helps reduce security risks and protect both organizational and user personal data. (Microsoft (Thailand) Co., Ltd., 2024). The development process will utilize OAuth 2.0 as the protocol for authentication and authorization, enabling users to access Google APIs (Google, 2024b). This supports the system's security in data storage and enhances the organization's operational processes, ensuring efficiency in both areas.

Consequently, the researcher proposes a concept for designing and developing an application for community college student activity participation. The objective is to develop an application for activity attendance using digital identify methodology for user authentication, activity recording, and participant tracking and reporting. This approach benefits users by focusing on testing the reliability of system access performance for practical implementation. The study emphasizes the potential of leveraging information technology for management by incorporating smartphones and mobile network services, particularly in areas outside the coverage of the community college's Wi-Fi. It also considers factors that promote the use of a digital authentication model, such as OAuth 2.0, to address security issues related to users' personal data. Additionally, it aims to enhance organizational operational processes through the use of digital applications, thus improving efficiency and increasing convenience for stakeholders.

2. Materials and Methods

2.1 Materials

This research examines the resources, tools, and operational approaches used in system development. The specific aspects covered in the study are outlined as follows: OAuth 2.0, the React framework, the Node.js programming language, the Firebase database, the evaluation of user authentication methods, the usability evaluation method, and user requirements analysis, as detailed below.

2.1.1 OAuth 2.0

The OAuth 2.0 authorization framework allows a third-party application to gain restricted access to an HTTP service. This can be done either by facilitating an approval interaction between the resource owner and the HTTP service or by allowing the third-party application to access the service on its own behalf (Hardt, 2012). Furthermore, OAuth 2.0 is an authentication and authorization protocol that enables users to access Google APIs. It is designed to support interactions with web servers, client-side apps, installed applications, and devices, particularly in scenarios where inputting application data is restricted (Google, 2024b).

2.1.2 React framework

The React framework is a library for developing web applications and native user interfaces, with the following key programming features: Hooks are utilized for unique React functionalities, distinguishing them from class-based components; Components are modular elements provided within the documentation that can be used within JSX; APIs are useful tools for defining and managing components effectively; Directives are predefined instructions that enable grouping and integration, allowing smooth interoperability with server-side React components. Additionally, React-DOM includes features that support the functionality of web applications, processing within the browser environment under the DOM. (Meta Platforms, Inc., 2024), as shown in the example statements in Figure 1.

```
export default function Profile() {
  return (
    <img
      src="./images/MyProfile_U001.jpg"
      alt="Web Programming"
    />
  )
}
```

Figure 1 Creating a simple component with React for working with markup languages.

2.1.3 Node.js language

Node.js is an open-source runtime environment available at no cost, operating within a cross-platform JavaScript environment. It enables developers to create servers, web applications, command-line tools, and scripts, all powered by asynchronous processing within the JavaScript runtime. Node.js is designed specifically for building scalable network applications. (OpenJS Foundation, 2024), as shown in the example statements in Figure 2.

```
const { createServer } = require('node:http');
const hostname = '127.0.0.1';
const port = 3999;
const server = createServer((req, res) => {
  res.statusCode = 200;
  res.setHeader('Content-Type', 'text/plain');
  res.end('Hello My Research.');
});

server.listen(port, hostname, () => {
  console.log(`Server running at http://${hostname}:${port}/`);
});
```

Figure 2 Creating a simple web server using Node.js.

2.1.4 Firebase database

Firebase is a platform and backend service for app and web developers, offering tools and infrastructure to simplify the app development process. It combines various backend management tools into a single platform, making it easier to develop applications across different platforms. Firebase provides services that help developers save time and money on server-side development. It offers both free and paid tools, including APIs and cloud storage, for building real-time applications (Google, 2024a), as illustrated in Figure 3.

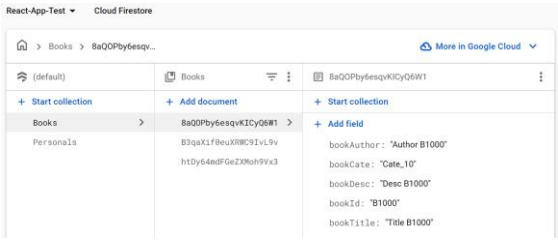

Figure 3 The JSON data structure stored in Firebase Firestore.

2.1.5 Evaluation of User Authentication Method

For systems designed and built using Google APIs, it is not sufficient to merely provide value to users and businesses. These systems and services must also ensure security and appropriate levels of privacy in accordance with user expectations. This policy is part of the Google APIs Terms of Service and applies to developers utilizing OAuth 2.0, including OpenID Connect for authentication purposes. While these are the minimum requirements, it is strongly recommended that developers take additional measures to ensure the system's security and maintain an adequate level of protection (Google, 2025).

2.1.6 Usability Evaluation Method

The criteria for system usability evaluation involve user testing, which is a critical step in the testing process. This approach relies on users to provide feedback and recommendations about the system. It may take the form of an informal process where users interact with new software products to assess whether the software meets their needs and expectations. Despite comprehensive system testing and deployment, the influence of users' working environments can significantly impact the system's reliability, performance, usability, and resilience (Sommerville, 2016). The evaluation approach incorporates the use of questionnaires and surveys to gather feedback and suggestions from users regarding the developed system.

2.1.7 User Requirements Analysis

Requirement Elicitation, where system requirements were identified by engaging with stakeholders and examining documents related to current operational procedures and practices; Requirement Analysis, during which the gathered requirements were categorized, prioritized, and analyzed for consistency, with models created to ensure a structured approach; Requirement Specification, where the requirements were documented in a formal specification supported by UML diagrams, followed by a thorough review, evaluation, and approval process to ensure accuracy and clarity; and Requirement Validation, where the specified requirements were assessed for correctness, completeness, and consistency through informal feedback from stakeholders to confirm alignment and accuracy. These steps collectively

established a comprehensive list of requirements to guide the subsequent phases of the development process.

2.2 Methods

The community college activity attendance application is being designed and developed as a web application utilizing a digital authentication methodology. The system's data is stored in Firebase (Google, 2024a). This platform, developed by Google, is designed to support application development with authentication via email and secure data storage. It enhances flexibility in configuring rules for protecting cloud-based database information from unauthorized access. The user interface and server-side services are built using the React framework (Meta Platforms, Inc., 2024) to facilitate the creation of interfaces and the efficient rendering of components when data changes and Node.js (OpenJS Foundation, 2024) this platform is used for developing server-side services and also aids in the development of both client-side and server-side applications using JavaScript. It reduces development time and, importantly, the program structure is simple to maintain. OAuth 2.0 is used to handle user data storage and authentication. The implementation consists of the following steps: Web application design and development, user authentication using OAuth 2.0, database design, and system users (clients), as illustrated in Figure 4.

From Figure 4, the figure presents a comprehensive overview of the application development methodology. The application is designed to allow community college students to test the event attendance system, while staff can verify and track student attendance. The application is tested on user devices, including the community college's Wi-Fi network and users' cellular networks. The study evaluates the response time of each task within the system workflow. The research methodology involves the following steps: web application design and development, user authentication using OAuth 2.0, database design, system user identification, and population selection.

2.2.1 Web Application design and development

Both frontend and backend development are used in the design and development of the web application for community college activity attendance that uses a digital authentication methodology. The user interface (frontend) is developed using the React framework, while Node.js is used for backend services. Firebase is employed for the system's data storage. The system supports two user roles: Student and Officer, with the following operational scope: activity registration, activity creation, verification and authentication of participant information, and reporting of participant data, as illustrated in Figure 5.

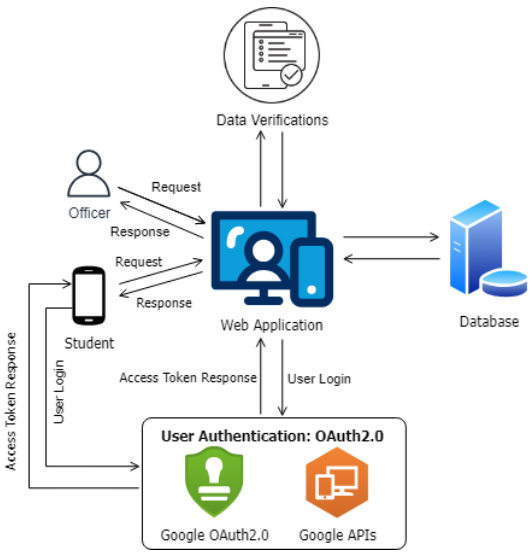

Figure 4 An overview of application approaches.

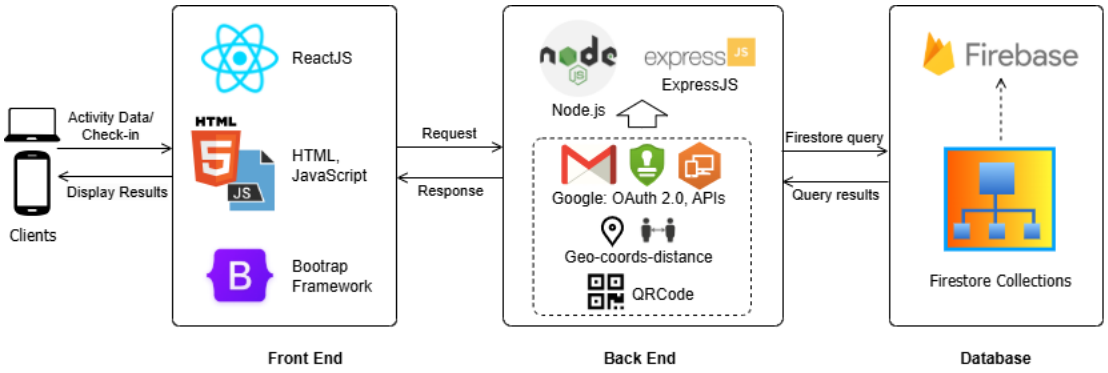

Figure 5 An overview of components of the application.

Figure 5 illustrates the system architecture, which comprises three main components: 1) a frontend layer developed with React, HTML, and Bootstrap, providing a user interface designed for seamless interaction across various devices, such as computers and smartphones; 2) a backend layer is built using the Express.js framework on Node.js, managing server-side operations such as user authentication (via email, OAuth 2.0, and geolocation-based distance verification for attendance tracking), activity data management, and interactions with the database; and 3) a Firebase database functions as the backend data repository, containing collections designed to store user attendance records. It provides real-time accessibility while ensuring the security of stored data.

2.2.2 User authentication using OAuth 2.0

User authentication with OAuth 2.0 is used as a protocol for verifying access rights and granting users access to Google APIs, which perform conditional checks in conjunction with student registration data for activities via the application. This includes email, registered location, and distance verification (with students eligible to register if they are within a specified range as determined by the institution for each activity) as illustrated in Figure 2. The aim is to reduce the burden on users in various aspects, such as filling in user information during initial registration, registering for activities via QR code scanning or with a single button click, and verifying student eligibility through email as a means of identifying the account owner. By linking with the institution's email service, which is supplied by Google, as illustrated in Figures 6-7, this allows for the verification of both the application users' registration data and student information at the educational facility.

The developed system integrates advanced security measures, utilizing OAuth 2.0 and Firebase to ensure user privacy through identity verification, access control, and real-time protection via Firebase security rules. The authentication process begins when users interact with the interface by selecting the "Sign in with Google" option, initiating GoogleAuthProvider to authenticate with Firebase. Once authentication is successful, Firebase generates user credentials and an ID token, which are transmitted to the backend for verification and securely stored in the database. As illustrated in Figures 6 - 7, this allows for the verification of both the application user registration data and student information at the educational facility.

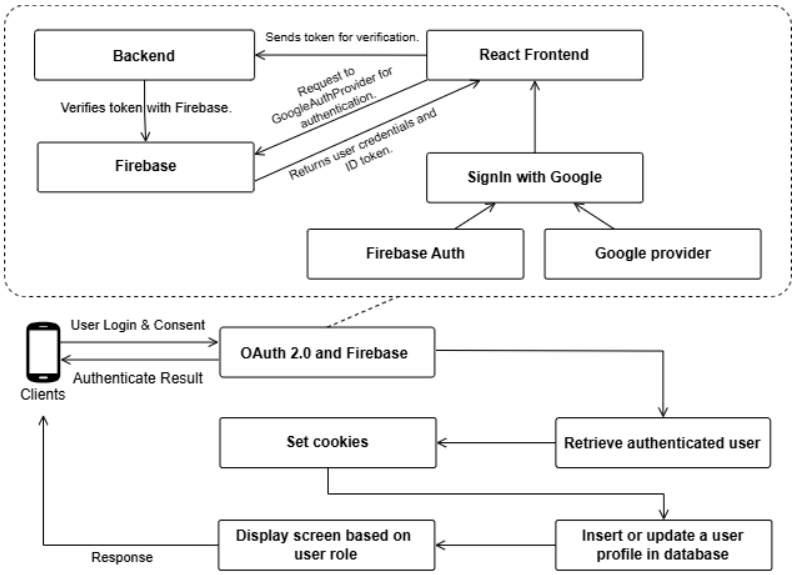

Figure 6 OAuth2.0 for user authentication in applications.

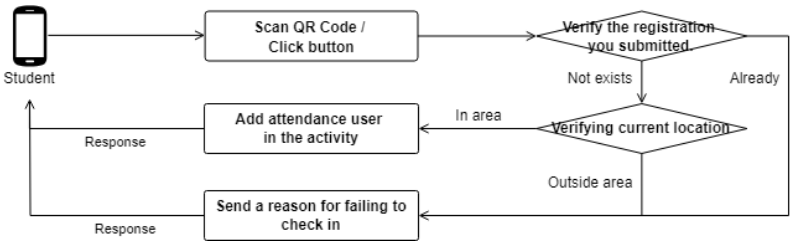

Figure 7 Attendance of students in an activity.

Activity

```
{
    "_id": String,
    "title": String,
    "description": String,
    "openQuantity": Number,
    "attQuantity": Number,
    "attendanceLogs": Array,
    "dtEnd": DateTime,
    "dtStart": DateTime,
    "location": {
      "address": String,
      "latitude": Number,
      "longitude": Number
    },
    "note": String,
    "organizedBy": String,
    "status": Number,
    "createdAt": DateTime,
    "createdBy": String,
    "updatedAt": DateTime,
    "updatedBy": String
}
```

College

```
{
    "_id": String,
    "name": String,
    "address": String
}
```

Department

```
{
    "_id": String,
    "name": String,
    "college": String
}
```

Users

```
{
    "_id": String,
    "studentCode": String,
    "address": String,
    "createdAt": String,
    "displayName": String,
    "eduProfile": {
      "class": Number,
      "college": String,
      "course": String,
      "level": String,
      "room": String,
      "numOfAct": Number,
      "yearOfStudy": String
    },
    "actAttendance": Array,
    "email": String,
    "phoneNumber": String,
    "photoURL": String,
    "role": Number
}
```

Figure 8 Database design in JSON format.

2.2.3 Database design

The database structure is presented in JSON format and designed for storage within the Firebase database. It consists of four collections: Activity, College, Department, and Users. These collections store information on activities, affiliated community colleges, departments within the community colleges, and system users, respectively. The database structure is shown in Figure 8.

2.2.4 System users (Clients)

System users are classified into two roles as follows: Students, who are required to use the platform to register for activities and check the list of activities they have participated in as specified by the institution; and Officers, who are staff members of the institution responsible for creating activities, verifying, and confirming participant information as outlined in the institution's curriculum, as illustrated in Figure 9.

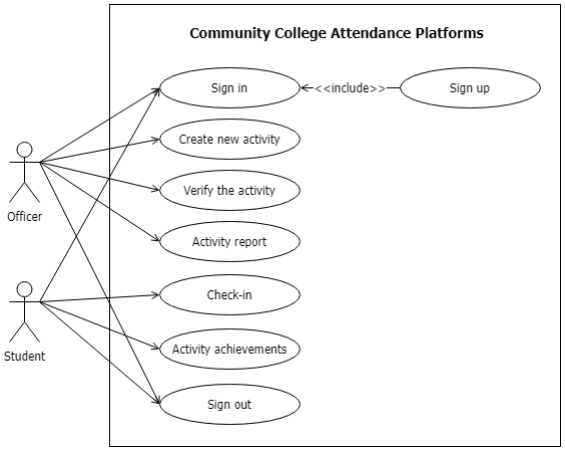

Figure 9 Use case diagram for displaying user roles.

2.2.5 Population

In this research, the test population was defined by selecting a sample group of first-year community college students, aged 17-18 years. These students are familiar with technology at a proficient level, primarily using smartphones as their main device to access the internet and communicate via social media platforms. Additionally, they possess a college email account for communication with both internal and external organizations that use services under the Google for Education platform.

3. Results and Discussion

The outcomes of the application design and development include the following: the user interface of the application, the evaluation of user authentication using OAuth 2.0, and the system usability evaluation, respectively.

3.1 User interface of the application

Participants will receive a QR code from the person in charge of each student activity. As illustrated in Figure 10, participants can scan or click the button to join the activity of their preference.

Figure 10 QR code to use for attendance into the activity.

In cases where the user has previously signed in, the system will proceed to verify the user's account and their current location for the purpose of registering for an activity. This information will then be recorded accordingly. In cases where the user has not yet signed in with their Google account, the application will redirect them to the main screen, prompting them to sign in with the designated institutional Google account. The user can initiate this process by clicking the 'Sign in with Google Account' button, as shown in Figure 11.

For signed-in users, the system will authenticate their account and check their current location to ensure eligibility for the desired activity. Upon successful verification, the system will record their participation and provide a confirmation on-screen. For users who haven't signed in, they will be directed to the main screen to log in with their institution-specific Google account. Once logged in, they can register for activities and access their personalized dashboard, which includes a list of available activities, their participation history, profile settings, and other relevant information, as illustrated in Figure 12.

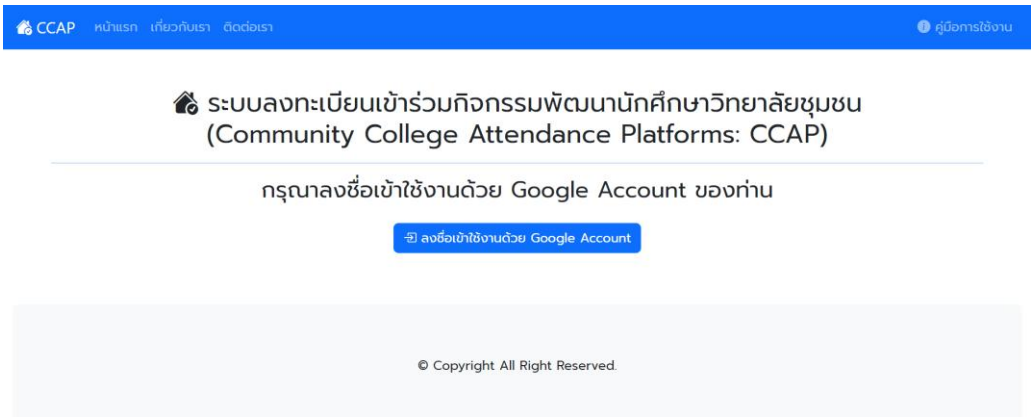

Figure 11 The main page of the application.

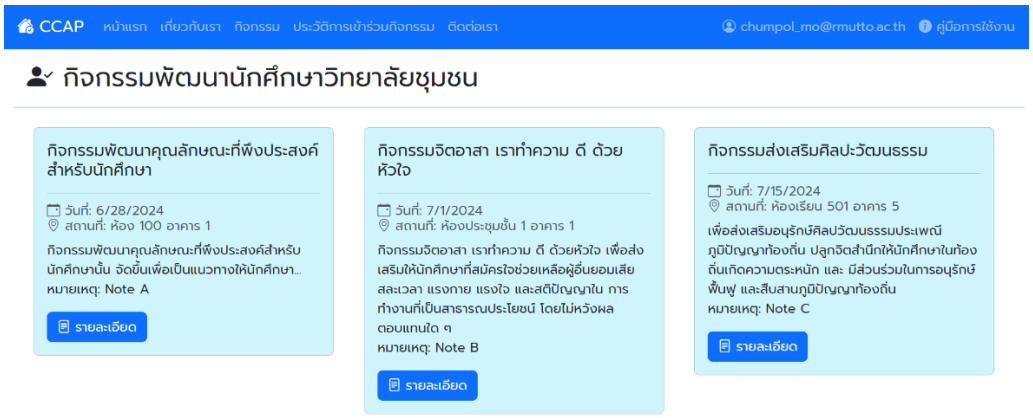

Figure 12 Display the page of an activity list.

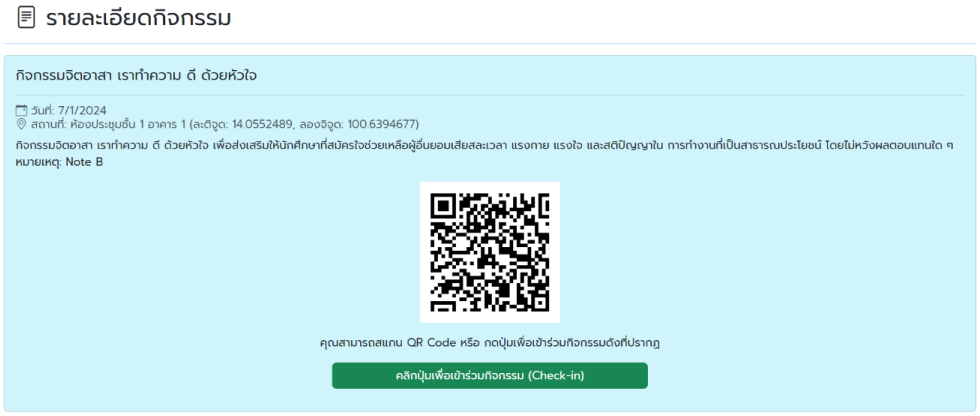

Figure 13 Display the page of an activity description.

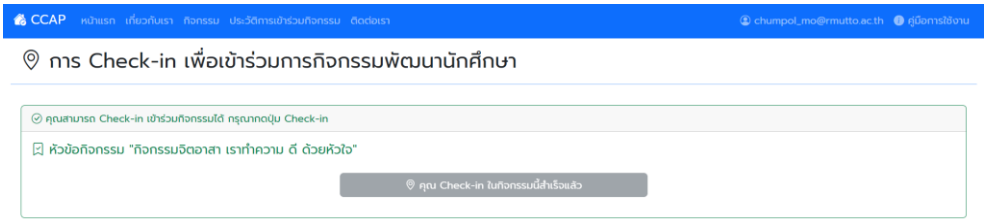

Figure 14 Display the page of the activity check-in.

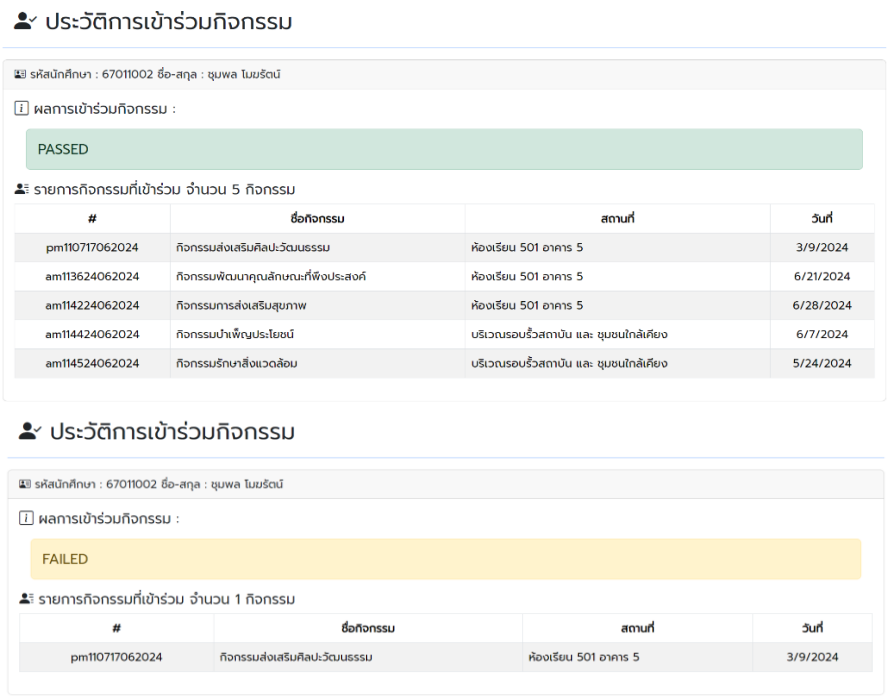

Figure 15 Page displaying the individual's activity history.

When users wish to view activity details, they can click the “Details” button to access the information. They can also participate in activities until the application disables this button, as illustrated in Figure 13.

As shown in Figure 13, when users scan the QR code or press the button to join the activity, the system verifies the event location and checks the distance of the user from the activity venue, ensuring it is within the range specified by the institution. Once the check-in process for participating in the activity is successfully completed, the system displays the registration confirmation for the activity, as illustrated in Figure 14.

Additionally, users can review their activity participation history. If they have met the institution's participation requirements, the application will display a “PASSED” status, along with a list of completed activities. If participation requirements are not yet fulfilled, the application will display a “FAILED” status, as illustrated in Figure 15 (A) - (B).

3.1.2 Evaluation of user authentication using OAuth 2.0

The evaluation of the system's performance was conducted using a questionnaire, which employed a 5-point Likert scale to assess user satisfaction with each function of the system. This included authentication, activity information retrieval, location verification, and participation recording. The reliability of the data was evaluated using the mean ($\overline{X}$) and standard deviation (SD) values.

The evaluation of user authentication using OAuth 2.0 focuses on three key aspects: Security, User Experience, and Compliance. This assessment is carried out using a prototype application built with OAuth 2.0 on the Google platform, executed over the HTTPS protocol. The process includes testing functionalities such as sign-in/sign-up, check-in, distance verification (The process of verifying the distance between the user's check-in coordinates for activity participation and the coordinates of the activity venue), sign-out, and token expiration. Additionally, secure storage mechanisms, such as local storage and cookies, are utilized to ensure a safe and reliable environment for managing tokens.

In order to evaluate the efficacy of the OAuth 2.0 user authentication process, the development team conducted a performance assessment involving 250 transactions (5 transactions per test user). The response times for each user were recorded and are presented in Table 1.

Table 1 Evaluation of OAuth2.0-based user application authentication.

No.	Test Case	Response time (Seconds)	$\bar{X}$	SD	Remark
1	Sign In / Sign Up	5-10	6.06	2.96	Total time being typing passwords to every user.
2	Check-in	1-5	2.90	1.36	
3	Distance Verification	5-20	8.66	2.62	Depending on the device and cycle (the slowest with the first).
4	Sign Out	1	2.70	0.98	
Total			**4.06**	**1.58**	

Table 2 Evaluation of the registration for student activities.

Test Case	The average registration time (Minutes)	$\bar{X}$	SD	Remark
Activity 1	3	2.70	0.79	First time registration using WIFI
Activity 2	1	1.10	0.30	Second registration using WIFI
Activity 3	1	1.00	0.00	Third registration using WIFI
Activity 4	2	1.60	0.49	Fourth registration using Cellular
Activity 5	2	1.32	0.47	Fifth registration using Cellular
Total		**1.54**	**0.41**	

A test involving 50 students was conducted to assess the registration process with 5 different test cases per student. Participants were asked to record the time taken for each step. The results showed that the "Verify Distance" step took the longest, followed by "Sign in/Sign up." The "Check-in" process required a moderate amount of time, while "Sign out" was almost instantaneous. Edited the performance was deemed acceptable by the users, as detailed in Table 2.

From Table 2, the testing was divided into two scenarios: Activities 1-3 were conducted within the college premises using the college's internet network, while Activities 4-5 were tested by students using mobile network provider. It was found that Activity 1, which required users to register for the first time via the venue's WIFI network, took the longest registration time. However, when the users were asked to register two more times in the same environment, the time taken was significantly less than the first time. For the fourth and fifth registration attempts, users were asked to change locations to outer areas and use the internet network from a service provider, resulting in a slight increase in registration time.

3.1.3 Evaluation of system usability

The system usability evaluation by users was conducted on various aspects, including the graphic user interface, usability, security, reliability, and utilization, respectively. The assessment employs a Likert scale as a measurement tool, consisting of five levels. The questionnaire covers five key areas: graphic user interface, usability, security, availability, and utilization. The response options are as follows: Level 5 indicates "very high satisfied", Level 4 represents "highly satisfied", Level 3 corresponds to "satisfied", Level 2 signifies "dissatisfied", and Level 1 denotes "strongly dissatisfied". These levels allow for a structured evaluation of user satisfaction across the specified areas, with the evaluation being carried out

Table 3 Evaluation of users' uses of the system.

No.	Title	$\bar{X}$	SD	Results
1	Graphic User Interface	4.20	0.70	High
2	Usability	4.80	0.49	Very High
3	Security	4.92	0.27	Very High
4	Reliability	4.70	0.51	Very High
5	Utilization	5.00	0.00	Very High
Total		**4.72**	**0.39**	**Very High**

by 50 users, all of whom were students, as detailed in Table 3.

From Table 3, the overall system usability evaluation by users yielded an average score of 4.72 ($\bar{X}$=4.72, SD=0.39), which falls into the "very high" category. Specifically, the aspects of usability, application security, application reliability, and application utility received average scores of 4.80 (SD=0.49), 4.92 (SD=0.27), 4.70 (SD=0.51), and 5.00 (SD=0.0), respectively, all of which are rated "very high". On the other hand, the graphic user interface received an average score of 4.20, which is rated as "high". The evaluation results indicated that users were highly satisfied with the system, and they were able to access it without any issues to their operations.

From the evaluation of system performance in various aspects, an extensive authentication and authorization framework leveraging OAuth 2.0 was proposed (Chen *et al.*, 2022). In this approach, the researcher categorized it into the assessment of user authentication using OAuth 2.0 and found that the relatively short time for "Sign in/Sign up" could be attributed to users having saved their passwords on their smartphones. Additional time was sometimes spent on device-specific authentication methods like fingerprints, PINs, or patterns. Smartphone specifications were found to influence the "Distance Verification" step, especially for first-time users in a new location. However, most aspects were within the acceptable level for users. Regarding the evaluation of student activity registration, the test results revealed that during the initial use, students were unfamiliar with the system, including the activation of the location verification program during the first attempt. This required them to study and carefully consider each step involved in the system's operations. However, in subsequent tests, students demonstrated increased familiarity with the system, leading to a noticeable reduction in the time required to complete the tasks. Furthermore, in cases where the system was accessed via mobile network providers, the performance was influenced by the characteristics of the smartphone and the signal strength of the network provider in the specific area. This is consistent with the fact that testing to determine the system's response time depends on several factors, such as internet speed, network traffic conditions, or the hardware and software of the API system and database. As a result, the test results demonstrated a trend in response speed during simultaneous user logins (Puntumnunt and Sompong, 2024). However, the results generally fell within an acceptable range for user satisfaction. Since the operation of the previous system relied solely on manual signatures on documents, it facilitated the recording of activity participation. However, in cases where access to an unstable internet network occurs, it may affect system functionality, as the system retrieves real-time data for recording. The current version of the system does not support storing data in backup memory (cache). Therefore, if the event location cannot access the internet or has poor signal quality, it will impact the system's performance. The final aspect, focused on evaluating system usability, showed that based on the test results, users were satisfied with the usability and security, but there may still be some dissatisfaction with the user interface (UI) compared to other aspects. The evaluation of the system's usability assessed students' understanding of how to use the system and their awareness of the importance of email, which serves as the primary account for student authentication. It also created a

new experience for students in using the application to record, verify, and track their participation in activities, as well as to receive various updates and notifications.

When comparing the operations between the existing system and the developed system, it was found that the previous process was conducted using a document-based approach, managed by personnel involved in each activity. The outcomes of this process affected operations related to data collection, data verification, and retrieving information about activity participation. The developed time attendance web application took the form of a responsive web, accessible on both computer and portable devices (Sittijuk and Sanchana, 2024). This approach proved inconvenient for both practitioners and users. Therefore, the researcher designed and developed an information system to support usage across multiple devices, integrating data verification for identity authentication through existing user account systems. By utilizing OAuth services, the system streamlines user authentication, removing the need for physical identification cards or manual input of personal information for officer verification. This highlights the system's readiness for development and its potential to integrate seamlessly with other organizational systems. The ultimate goal is to enhance operational efficiency for officers, students, and other stakeholders in these activities in the future.

4. Conclusion

The design and development of the information system are aimed at supporting usage across devices and telecommunications networks that are accessible to users. Currently, these networks cover most areas of the country, and the majority of students at community colleges are located outside urban areas. Although the characteristics of communication devices and internet-connected networks may vary, they do not impede the system's operation. In addition, referencing identity verification through existing user accounts (e.g., Google accounts) can utilize OAuth services to authenticate individuals. This eliminates the need for physical identification cards and the manual entry of personal credentials by users. It allows for the shared use of user accounts and reduces the necessity of creating and maintaining separate user accounts for each system. However, this approach also ensures the security of password data, protecting personal information and reducing the risk of password leaks or guessing within the system.

The test results indicate that both the mobile network infrastructure and the characteristics of smartphones most commonly used by students, particularly the integration of authentication systems through OAuth services, demonstrate readiness for the development of an information system. This allows users to access and utilize the system via applications across various platforms, ensuring that access is seamless and without issues in usage. This study assumes that user accounts and passwords are unique to each individual (without any processes for delegation of login credentials). The overall evaluation results show that users are highly satisfied and expect the developed system to be compatible and interoperable with other systems within the organization. For example, the integration of the application with the student registration system can assist students in effectively planning their participation in activities that align with the prescribed curriculum. This integration also serves as a direct communication channel to inform students about upcoming events and participation requirements through various devices. Additionally, the system can incorporate functionality for attaching photos or videos as tangible evidence of student involvement in activities. This feature can enhance accountability and provide comprehensive data management support for users.

5. Acknowledgments

The study and research in this article were successfully completed thanks to the support from the Department of Information Technology, Faculty of Business Administration and Information Technology, Rajamangala University of Technology Tawan-ok, Chakrabongse Bhuvanarth Campus. The researcher is sincerely grateful for this support.

6. References

Amazon Web Services. 2024. **What is Multi-Factor Authentication (MFA)?.** What is Multi-Factor Authentication (MFA) - An explanation of MFA -AWS. Available Source: https://aws.amazon.com/th/what-is/mfa/, May 24, 2024. (in Thai)

Chen, J., Hoppen, M., Böken, D., Reitz, J., Schluse, M., and Roßmann, J. 2022. Identity, Authentication and Authorization in Forestry 4.0 Using OAuth 2.0, pp. 1-6. *In* **2022 3rd International Informatics and Software Engineering Conference (IISEC).** Ankara, Turkey.

Google. 2024a. **Developer documentation for Firebase.** Firebase Documentation. Available Source: https://firebase.google.com/docs, June 7, 2024.

Google. 2025. **OAuth 2.0 Policies.** OAuth 2.0 Policies | Authorization. Available Source: https://developers.google.com/identity/protocols/oauth2/policies, January 21, 2025.

Google. 2024b. **Using OAuth 2.0 to Access Google APIs.** Using OAuth 2.0 to Access Google APIs | Authorization. Available Source: https://developers.google.com/identity/protocols/oauth2, May 24, 2024.

Hardt, D. 2012. **RF 6749 - The OAuth 2.0 Authorization Framework.** Available Source: https://datatracker.ietf.org/doc/html/rfc6749, November 20, 2024.

Kantipudi, R., Mallavarapu, A.S.K., Rajagopal, S.M., and Kagolanu, M. 2024. A Comprehensive Analysis on using Multifactor Authentication System for Three Level Security, pp. 498-503. *In* **2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT).** Bengaluru, India.

Karim, N.A., Khashan, O.A., Kanaker, H., Abdulraheem, W.K., Alshinwan, M. and Al-Banna, A.K. 2023. Online Banking User Authentication Methods: A Systematic Literature Review. **IEEE Access** 12: 741-757.

Sommerville, L. 2016. **Software Engineering Tenth Edition.** Pearson Education Limited, England.

Meta Platforms, Inc. 2024. **React.** Available Source: https://react.dev/, June 7, 2024.

Microsoft (Thailand) Co., Ltd. 2024. **What is Two-Factor Authentication?.** What is Two-Factor Authentication? | Microsoft Security. Available Source: https://www.microsoft.com/th-th/security/business/security-101/what-is-two-factor-authentication-2fa, June 5, 2024. (in Thai)

Office of the Higher Education Commission, Ministry of Education. 2003. **Regulations of the Management of Lower-Degree Higher Education in the Community College Act B.E. 2546 (2003).** Thai Government Gazette vol. 120, Part 103 A. (dated October 15, 2003). (in Thai)

OpenJS Foundation. 2024. **Introduction to Node.js.** Node.js – Introduction to Node.js. Available Source: https://nodejs.org/en/learn/getting-started/introduction-to-nodejs, June 7, 2024.

Polpong, J., Puengson, S., Tantisattayanon, N. and Pornpongtechavanich, P. 2024. Enhancing Password Storage Through the Integration of Cryptarithmetic Techniques and Hash Functions. **ECTI Transactions on Computer and Information Technology (ECTI-CIT)** 18(2): 147-157.

Puntumnunt, V. and Sompong, C. 2024. Two-factor Authentication for Web Application. **Journal of Science, Engineering and Technology Loei Rajabhat University** 4(1): 1-13. (in Thai)

Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M. and Egelman, S. 2020. Empirical Measurement of Systemic 2FA Usability, pp. 127-143. *In* **29th USENIX Security Symposium (USENIX Security 20).** USENIX Association.

Sainui, J., Jankaew, N. and U-seng. H. 2021. A prototype of seminar registration system using face authentication. **Journal of Applied Information Technology** 7(2): 40-50. (in Thai)

Sharif, A., Carbone, R., Sciarretta, G. and Ranise, S. 2022. Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients. **Journal of Information Security and Applications** 65: 103097.

Singh, J. and Chaudhary, N.K. 2022. OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities. **Journal of Information Security and Applications** 65: 103091.

Sittijuk, P. and Sanchana, W. 2024. Development and Acceptance of Time Attendance Web Application Using Identity Verification with Picture and Location of Personnel in Private Universities. **Rajamangala University of Technology Srivijaya Research Journal** 16(3): 689-702. (in Thai)

The Bureau of Registration Administration. 2024. **The digital identity verification and authentication system of the ThaID application.** The Department of Provincial Administration's Digital ID System in the ThaID Application - The Bureau of Registration Administration. Available Source: https://www.bora.dopa.go.th/app-thaid/, May 24, 2024. (in Thai)