International Journal of Science, Technology, Engineering and Mathematics
Volume 4 Issue 3 September 2024
DOI: https://doi.org/10.53378/ijstem.353104

Internship management system with passwordless authentication for university stakeholders

[1]St. Joseph M. Lumbog & [2]Maricel M. Gaspar

Abstract

Conventional account credentials that include a password are becoming obsolete due to their limitations and susceptibility to cyber threats. This demands using alternative authentication methods that eliminate the risks of breaches and phishing. This paper discusses the integration of passwordless authentication into an electronic document management system (EDMS). The authentication method used in the system utilizes a Time-Based One-Time Password (TOTP), which operates security keys in the form of one-time passwords (OTP) that are sent to the users via email, short message service (SMS), or mobile application. The TOTP algorithm is used in the system, allowing time value as a moving factor. The Rapid Application Development (RAD) model was used in the system development and ISO 25010 was used in the evaluation. The sample size of the respondents for the acceptance testing was determined using Krejcie and Morgan's formula. The research sample involves 10 information technology experts, one on-the-job training (OJT) coordinator, three OJT advisers, and 244 OJT students. Based on the results, the system was rated outstanding (system evaluation=4.66; acceptance evaluation=4.34), implying that the system met its requirements and that passwordless authentication was proven to increase the security of the developed system. This outcome serves as the basis for integrating passwordless authentication into various systems.

Keywords: *passwordless authentication, one-time password (OTP), time-based one-time password (TOTP), possession factor, rapid application development (RAD)*

Article History:

***Received**: July 30, 2024*
***Revised**: September 9, 2024*
***Accepted**: September 10, 2024*
***Published online**: September 14, 2024*

Suggested Citation:
Lumbog, S.J.M. & Gaspar, M.M. (2024). Internship management system with passwordless authentication for university stakeholders. *International Journal of Science, Technology, Engineering and Mathematics*, 4(3), 126-153. https://doi.org/10.53378/ijstem.353104

About the authors:
[1]Corresponding author. Instructor I, Cavite State University. Email: josephlumbog@gmail.com

[2]First Asia Institute of Technology and Humanities. Email: mlmalabanan@firstasia.edu.ph

1. Introduction

Developments in technology bring innovative ICT solutions, such as electronic document management systems (EDMS), that enhance performance and productivity in managing and processing documents (Andriansyah & Elmi, 2020). This benefits offices that process, analyze, save, and disseminate volumes of documents regularly (Justina et al., 2022). In the case of an internship program, this can be a practical tool that can help coordinators, trainees, and training supervisors efficiently and easily handle on-the-job training-related documents. Although the use of this technology in its bare form is already a huge improvement, there are still aspects that can be improved and technologies that can be integrated with it. For instance, in terms of security, unauthorized access to the system and its data exposes its users to threats, such as stolen identities and authentication credentials. Concerning this, passwordless authentication can be incorporated into the system. Since this type of authentication is not susceptible to the limitations, vulnerabilities, threats, and risks that come with password-based authentication, it can make the process and the documents more secure (Ukwandu & Bennett, 2023; Prasad, 2024; Oduguwa & Arabo, 2024; Parmar et al., 2022).

This study focuses on developing the Cavite State University Internship Management System (CIMS) by integrating passwordless authentication into electronic document management systems. Aside from the typical document management functions, such as conventional text-based file generation, printing, and distribution, the system is capable of eliciting, processing, analyzing, saving, and disseminating information. In addition, the system enables its users to retrieve, audit, set up, secure, share, download, and upload files. This aims to improve the overall experience of the institution's internship program stakeholders. The EDMS makes the management, storage, and retrieval of documents easier for the university's front-line staff, whereas the use of First Identifier Online 2 (FIDO2) to remove the use of preset passwords protects the system from server breaches and phishing.

More than just software, this system supports the Sustainable Development Goals (SGD) of the university, such as quality education, decent work and economic growth, industry, innovation and infrastructure, and partnerships. A platform that allows Cavite State University (CvSU) students to easily connect with the university internship program in a variety of fields that can reach not just Cavite but the entire Philippines. The CIMS expedites the procedure and makes it user-friendly and available to all interns. After matching, it

becomes a vibrant center for cooperation and communication, encouraging quicker submission, tracking of progress, and convenient access to on-the-job training (OJT) advisers and coordinators.

2. Literature review

2.1. Document Management System

A document management system is a vital standardized management process that includes the reception, collection, organization, control, maintenance, and storage of documents that can be used in other processes that may require it in the future (Firdaus & Jumaryadi, 2020). In addition, it involves planning and management theories implemented in multiple tasks at the same time. A common denominator of these tasks is the publication or production of reports that require verification of registered accounts (Afrizal et al., 2021). Further, a document management system can significantly enhance and improve several of the institution's operational features. The system offers a thorough and effective method for managing, exchanging, protecting, and adhering to documents (Zabukovšek et al., 2023). It makes handling document-related tasks easier for the college's front-line staff and enables quicker document management, storage, and retrieval (Angala et al., 2023). As industry 5.0 continues to dominate the process, the surge in document processing reaches a record high. Document management procedures have entered the digital era due to the information technology industry's present quick advancements. Since information is essential to decision-making, it is imperative to access this organizational asset as soon as possible with accuracy (Abacı & Medeni, 2022). The demand for document processing requires innovative, efficient ways of managing documentation that will address problems that may arise, such as inefficient time management, overconsumption of energy, insufficient storage, and most threateningly, loss of documentation (Firdaus & Jumaryadi, 2020).

An electronic document management system (EDMS) is an innovative ICT solution that enhances productivity and performance in terms of processing a document (Malekani, 2023; Jones, 2012; Gani et al., 2024; Rathnayaka et al., 2024). This technology offers more than just distribution, printing, and conventional text-based file generation. This sophisticated knowledge and computer-based tool is capable of disseminating, saving, analyzing, processing, and eliciting information in a fast and comprehensible manner, which is beneficial to policymakers and users (Justina et al., 2022). In addition, this innovation can

also be integrated with other technologies, such as cloud-based computing or architecture; this enables the EDMS to retrieve, audit, set up security, share, download, and upload files with the use of its multiple modes (Han et al., 2021). According to Gonçalves et al. (2020), since a document management system handles a huge amount of confidential information, security is one of the most challenging parts of the development process. There is a lot of security compliance to consider, including company policy, state law, and general security measures. If security measures are well-established, they can provide tight control over personal data to give data subjects more security and confidence and guarantee that the personal information they give to a firm or institution is utilized for the reasons for which they provided consent. Included in the long list of advantages of EDMS are system integration, privacy, performance, cooperation, budgetary support, and management support. These benefits make the use of EDMS a key factor in implementing document repositories and developing the capabilities of a firm as well as its workforce (Justina et al., 2022).

In education, the transition from the traditional method of managing documents to the use of advanced EDMS enables schools to minimize costs and enhance stakeholders' file security. With the help of EDMS, educational institutions are provided with a way to share, synchronize, manipulate, manage, access, and store documents that are efficient and easy. Another feature, which is authentication, can be integrated into the system to ensure that only authorized individuals can get access to the system and the inside documents. In addition, when it comes to archiving documents, they can be saved in portable document format (PDF) before moving into the repository to save space, prevent data loss, and ensure data integrity (Justina et al., 2022). In a study conducted by Tkachenko and Денисова (2022), the researchers claimed that an information system for the electronic document management of a university resulted in a decrease in classification errors, which is crucial for a university employee because it will free up time to work on more innovative projects rather than manually classifying documents. Indeed, in relation to managing documents, accuracy and clarity of information are major factors. These are very crucial to making the results of human activities precise and fast. According to Hernandez and Hernandez (2022), other impacts of ICT infrastructure include positive relationships with its stakeholders, increased technology transfer, and an improved hiring process. However, the effort in the technological shift towards the adaptation and implementation of ICT infrastructure should not solely come to the management of the university but also to its stakeholders.

2.2. Passwordless Authentication

The acceptance and utilization of mobile devices, as well as the applications and systems that come with them, by people around the world, demand the use of authentication. This is usually an identifier, or username, and a password, specific to every account for each application and system that is used by the user. This method is supposed to ensure security, so only the owner has the authority to use the account and access its information (Yoshimura et al., 2019). With the surge in the number of users of mobile applications or software, attacks on systems are becoming more frequent. This implies that security should be the top priority to ensure that the information of the users is safe from malicious access. To access a resource, there is normally a three-stage process that will happen before it is executed. First is identification; this is the process where the user should input a unique identifier for his or her account. It can be a number, an email address, or a username. The second is authentication; this is the process where the user needs to prove his or her identity by providing some kind of password. Lastly, authorization: when the data encoded by the user is correct, the system will grant access (Matiushin & Korkhov, 2021). Although this method has been used for a very long time, this type of authentication has been bombarded with various issues. For instance, during the pandemic, the cases of fraudulent violations significantly increased. The attacks primarily target personal information to gain access to bank credentials (Chebotareva & Chebotarev, 2021). One way to solve this problem is by entirely removing the use of passwords. This method is called Fast Identity Online 2 (FIDO2), passwordless authentication (Kunke et al., 2021).

Passwordless authentication is a method where the user is identified without the use of preset login credentials, particularly passwords. In this authentication method, public-key cryptosystems, possessions, knowledge, and application of attributes are the focus of research and development. In particular, Email Magic Links, Inherent Factors, Possession Factors, and Knowledge Factors are used for unique client identification. (Ukwandu & Bennett, 2023). The most common classifications of authentication methods are: first, knowledge factor, which assumes the user has secret information that can be used for initializing access, such as pin codes or passwords. Second, the possession factor assumes the user has unique hardware or devices, such as electronic keys or mobile phones. Lastly, the inherent factor relies on the biometric features of the user, such as face and fingerprint details (Matiushin & Korkhov, 2021).

Currently, one of the most promising passwordless authentication methods is the FIDO2 standard. It is an authentication method developed by the joint efforts of the FIDO alliance, which has around 260 member companies around the world, including VISA, Amazon, Microsoft, Facebook, Google, and the World Wide Web Consortium (W3C). It is now widely supported and accepted by various service providers and is adopted by multiple browser software (Lyastani et al., 2020). In a study conducted by Furuberg and Øseth (2023), the participants acknowledged their understanding of the vulnerabilities related to passwords in general as a technique for authentication. In particular, they made it clear that passwords can be broken and admitted that there were comparatively simple ways to accomplish this. Due to these problems, the FIDO2 authentication method has huge potential for the future of computer-based systems. It follows the development track of Universal 2nd Factor (U2F) authentication, which allows websites to use security keys, which are standardized ways of utilizing hardware for authentication. FIDO2 is considered the "password killer" since it supports both single-factor (passwordless) and second-factor (hardware) authentication. In addition to its features, it provides account credentials that cannot be subjected to server breachers, re-played, or phished. Further, it supports a wide range of authenticator devices, such as security keys from Feitian or Yubico. Also, since it is an open-web authentication standard, it can support any browser, like Windows and Android. Thus, it provides end-users with a consistent experience, regardless of the platform or website (Lyastani et al., 2020). According to Ukwandu and Bennett (2023), FIDO2 provides users with enhanced security and overall experience with its advantages, such as a simplified registration process, heightened protection against cyber-attacks, basic utilization, and disregarding the need to remember preset passwords. In addition, FIDO2 is not susceptible to the limitations, vulnerabilities, threats, and risks that come with the use of password-based authentication.

2.3. Time-Based One-Time Password Algorithm (TOTP)

The HMAC-Based One-Time Password Algorithm (HOTP) is the basis for the development of the Time-Based One-Time Password Algorithm. The HOTP, grounded on the Hashed Message Authentication Code (HMAC), has various network applications, including websites that are transaction-oriented, login systems for Wi-Fi connections, and access to a Virtual Private Network (VPN). The algorithm was developed by the combined efforts of Open Authentication (OATH) members, who aim to provide an open-source

algorithm to the computing community. The developers believe that by sharing the algorithm with the community, it will promote the system and widen the utilization of two-factor authentication on the internet (M'Raihi et al., 2005).

The Time-Based One-Time Password Algorithm (TOTP) supports moving factors that are time-based. The HOTP is an event-based algorithm that has an event counter as a moving factor, whereas the TOTP is a time-based algorithm that has a time value as a moving factor. It provides an expiring OTP value that increases the security of a system. Similar to HOTP, it has various applications, especially in network systems (Rydell et al., 2011). The foundation of the HOTP, HMAC development with the hash function of SHA-1, is also the basis of the enhanced security of the TOTP. In terms of security considerations, the algorithm's dynamic truncation outputs for various inputs are standardized, independent, distributed strings. Based on the requirements section of the TOTP, every key should be selected at random. This can be done by utilizing a generator seeded with a random value that can produce a cryptographically pseudorandom key. In addition, to enable interoperability on various implementations, the length of the key should be the same with the HMAC output. In relation to validation and time-step size, several factors, including the network latency and transmission delay window, are being considered. The previous and receiving timestamps are scrutinized to identify what particular time step it would fall during validation. Further, to lessen the risks of attacks, for a particular network delay, only one-time step is allowed.

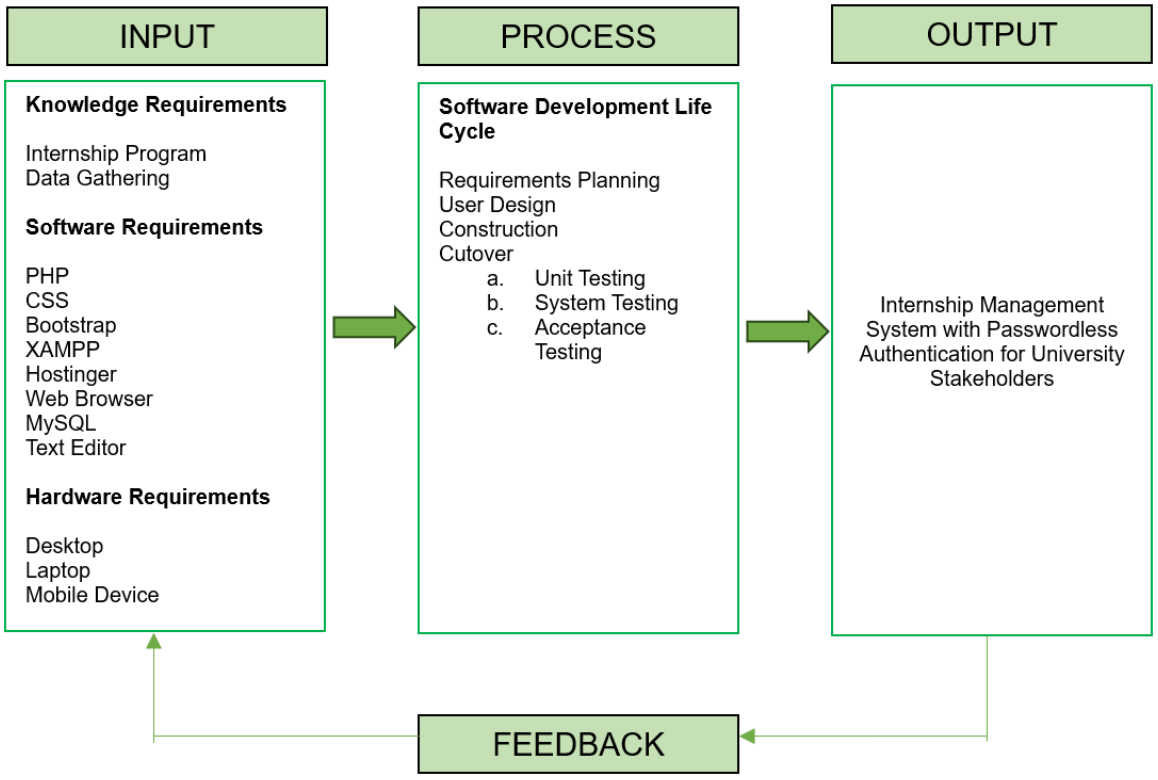
2.4. Theoretical framework

To illustrate the study's premise, a conceptual framework is shown in figure. 1. The input section of the diagram presents the variables used in the conceptualization of the system and study. It involves the internship program's basic requirements and its needs. These were identified by conducting data gathering in the form of interviews and questionnaires. These became the bases of the integration of technology to address the gaps in the program. In addition to the concepts, the software requirements that helped in the development and integration of technology into the internship program are also presented in the diagram. The process section shows the software development life cycle of the system. The data gathered was used in the requirements planning to identify the modules to be developed. The modules' functions, process flow, and users were pointed out in the user

design phase, and the development proceeded in the construction phase. The cutover phase focused on the testing and evaluation of the system. The problems and deviations with regard to the overall requirements of the system that were detected in the tests were immediately addressed by calibrating the modules and its units. After the system was developed, it underwent acceptance testing. Adjustments with the system, down to the units of the modules, were made based on the feedback taken from the test.

Figure 1

Conceptual framework of the study



3. Methodology

3.1. Research design

In conducting the study, a descriptive design was implemented. Its usefulness derives from the idea that observation, analysis, and description may be used to solve issues and improve procedures. Rosa and Galang (2023) used the same design in developing a web-based system for curriculum management at Bulacan State University, effectively describing the processes involved in curriculum development. In terms of software development, Rapid

Application Development was implemented. It is especially useful for projects with changing needs and user-centered goals. It enables to close the gap between concepts and reality and provides useful goods that satisfy the demands of the clients in a world that is changing quickly.

3.2. Algorithm

The Time-Based One-Time Password Algorithm (TOTP) supports moving factors that are time-based. The HOTP is an event-based algorithm that has an event counter as a moving factor, whereas the TOTP is a time-based algorithm that has a time value as a moving factor. It provides an expiring OTP value that increases the security of a system. Similar to HOTP, it has various applications, especially in network systems. The foundation of the HOTP, HMAC development with the hash function of SHA-1, is also the basis of the enhanced security of the TOTP. In terms of security considerations, the algorithm's dynamic truncation outputs for various inputs are standardized, independent, distributed strings. Based on the requirements section of the TOTP, every key should be selected at random. This can be done by utilizing a generator seeded with a random value that can produce a cryptographically pseudorandom key. In addition, to enable interoperability on various implementations, the length of the key should be the same with the HMAC output. In relation to validation and time-step size, several factors, including the network latency and transmission delay window, are being considered. The previous and receiving timestamps are scrutinized to identify what particular time step it would fall during validation. Further, to lessen the risks of attacks, for a particular network delay, only one-time step is allowed.

3.3. Subject of the study

The researcher conducted surveys and evaluations with information technology (IT) experts, OJT advisers and OJT students. In addition, the researcher met with the designated Management Information System (MIS) officer and the OJT coordinator to gather the necessary information for the study. Further, the researcher was granted access to the database of the registrar by the MIS officer of the campus. The certification grants read-only access to OJT-related information. There are 258 target respondents to evaluate the Cavite State University Internship Management System (CIMS) and its acceptance. The respondents are composed of 10 IT experts with at least two years of experience, one OJT coordinator,

three OJT advisers, among them from different programs on campus, and 244 OJT students. The IT experts evaluated the system testing based on ISO 25010, while the rest of the respondents evaluated the acceptance testing of the system. The sample size for the acceptance testing was determined using Krejcie and Morgan's (1970) formula.

All the respondents came from the City of Carmona and Cavite State University—Carmona Campus. Table 1 shows the profile of the IT experts that evaluated the system testing, and table 2 shows the profile of respondents that evaluated the acceptance of the system with frequency and percentage.

Table 1
Respondents profile of IT experts for system testing

Respondent Number	Profession	Company
1	Packaged App Development Analyst.	Accenture Inc.
2	Junior Software Developer	Uplink Integrated Solutions Inc.
3	Senior Programmer Analyst	Uplink Integrated Solutions Inc.
4	Senior Software Engineer	Accenture Inc.
5	Senior IT Manager	Educar Shared Services Inc.
6	MIS Officer	Cavite State University – Carmona
7	Web Developer	Customistation Inc.
8	System Engineer	Adonai Software & Digital Technologies Corp.
9	Software Engineer	Philippine Army
10	Software Engineer	Philippine Army

Table 2
Frequency of the respondents for the acceptance testing

Participants	Frequency	Percentage
OJT Adviser/ Coordinator	4	1.61
BSBM MM 4	33	13.31
BSBM HRM 4	25	10.08
BSIT 4	47	18.95
BSIndT 4	10	4.03
BSHM 4	30	12.10
BSHM 2	99	39.92
TOTAL	**248**	**100**

3.4. Requirements planning

The conceptualization of the study was conducted before proceeding to the development phase of the system. Initial data gathering happened to collect the requirements of the study and plan the steps needed accordingly. A follow-up interview happened between

the researcher and the client via Google Meet. An extensive and very informative meeting happened, different goals were targeted, and a timeline for the development was started. Nearly an hour of fruitful conversation was recorded in the interview sheet, and all necessary initial information for this research was obtained. In this phase, the inputs, processes, and outputs were identified. This helped in the conceptualization and guided the identification of the required modules to be developed. The parameters for each process and module were also identified based on the data taken from the interview. In general, the planning aimed to automate the manual OJT-related processes and improve any existing system used by the internship program.

The following requirements were identified: first, create a module that will allow the students to upload and download forms, such as recommendation letters, waivers, ledgers, etc.; second, construct a module that will allow the students to view training status and calendar of activities and enable the students to monitor the status of their reports; third, create a module that will allow the OJT adviser and coordinator to approve, view, accept, and generate forms and reports; and fourth, construct a module that will enable the system administrator to manage, setup, and backup system contents. Most importantly, integrate passwordless authentication into the system.

3.5 User design

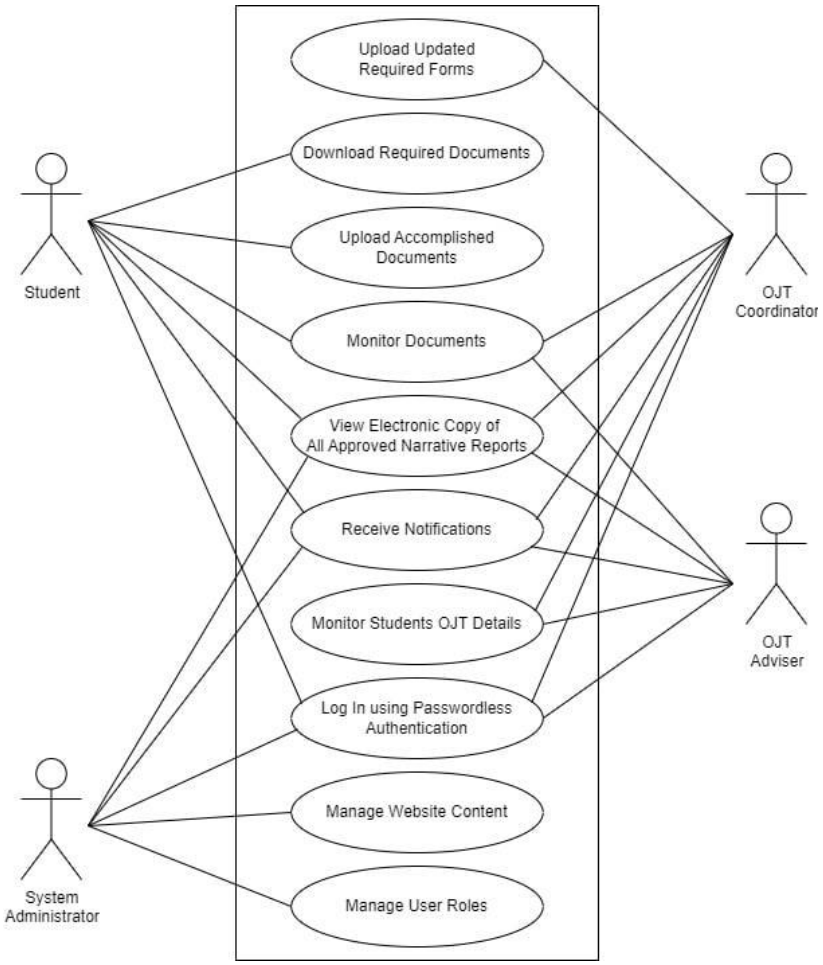
This phase incorporates all the requirements that were identified during the requirements planning phase. All the modules and their parameters were considered in order to create an efficient system. This is necessary to avoid redundancy in processes and waste of resources. A use case diagram (Figure 2) was created in this phase to help better visualize the modules and the features they will provide to the user.

The diagram shows the modules that are included in the system, such as the OJT coordinator module, OJT adviser module, student module, and system administrator module. Each module enables the user to access various features of the system. The upload required forms feature allows the OJT coordinator to upload necessary document templates for the trainees and OJT adviser. This includes the student waiver, training plan, evaluation forms, etc. The download document function allows the trainee to download the document templates uploaded by the OJT coordinator. These templates will automatically incorporate the personal information of the students into the documents and forms. The upload accomplished

document feature enables the trainee to upload necessary training documents, such as a registration form, a copy of the recommendation letter, an accomplished student waiver, a notarized memorandum of agreement, a training plan, journals, a certificate of completion, and a narrative report. The function of document monitoring is threefold: first, for the trainee, it allows them to monitor the pending and accomplished documents; second, for the OJT advisers, it enables them to monitor the document requests of the students as well as their accomplished forms; and third, for the OJT coordinator, the function allows the coordinator to monitor the status of all of the trainees and their progress. The narrative collection feature serves as a repository of all finished narrative reports of previous trainees. This acts as a library where the trainees can browse for references while doing their own narratives.

Figure 2

Use case diagram of the study

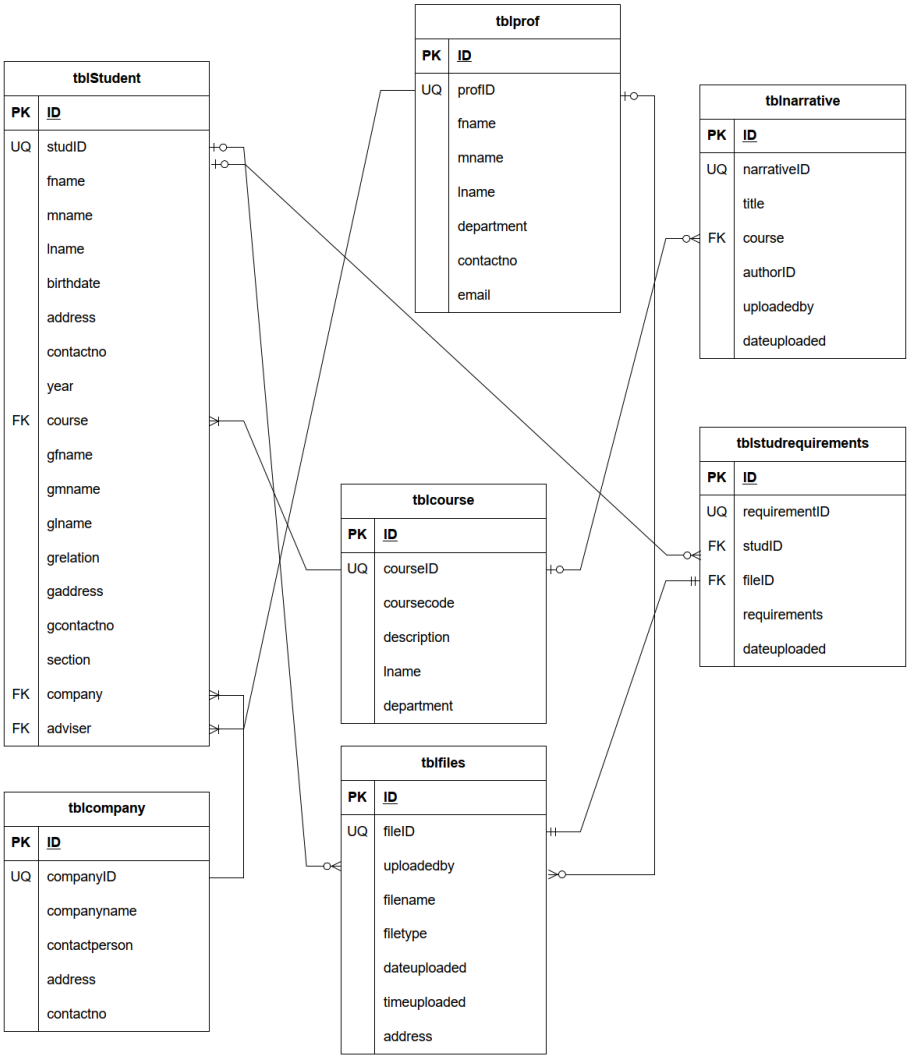


The notification function will notify all the users involved in the system. The trainees will be notified for their pending and approved documents, the OJT adviser will be notified

for the requests and accomplishments of the trainees, the OJT coordinator will be notified for the status of the trainees, especially those that have important discrepancies, and the system administrator will be notified if the semester is going to end and if there are critical updates needed.

Figure 3

Entity relationship diagram of the study



The student monitoring feature enables the OJT adviser to monitor the status of the documents and the progress of the trainees. The passwordless authentication log-in function allows all users to receive credentials on their mobile device that can be used for logging into the system. The content management feature enables the system administrator to edit system

information, such as mission, vision, address, quality policies, and core values. The user management function allows the system administrator to assign authorities to the user, such as OJT advisers and OJT coordinators.

In addition to the activity diagrams, an entity relationship diagram (ERD) was constructed to present the relationship between the instances of the entities in the tables of the database, as well as the internal controls of the system. The diagram as shown in figure 3 contains connectors that tell the type of association of the instances of the entities. The symbol, ⟜ or "zero or one", means that a single instance of an entity is associated with zero instance of another entity. The connector, ⫤ or "one or many", signifies that a single instance of an entity is associated with many instances of another entity. The symbol, ⟜ or "zero or many" implies that many instances of an entity is associated with zero instance of another entity. Lastly, the connector, ⫫ or "one (and only one), means that a single instance of an entity is exclusive associated with a single instance of another entity.

3.6. Construction

This phase involves the actual construction of the system. Inputs from the clients were considered in developing the system. In addition, the working models from the previous phases and the necessary requirements were used as guides in coding and developing the system. Further, the client's continued feedback and suggestions were gathered and incorporated, which helped in meeting their expectations.

The software used are: PHP, as the main programming language; CSS, used in designing the system; XAMPP, used for the local web server of the system; Visual Studio Code, the text editor used in coding; Hostinger, used in the hosting and domain services; MS Word, used for the documentation of the study and development; MS PowerPoint, used in creating the presentation; and Canva, used to edit the images used in the system. On the other hand, computers, such as the desktop and laptop, were used in coding and testing the system. These were also used in simulating the processes that are involved in the system. The mobile device was used for the mobile application notification process, especially for passwordless authentication. It was used to simulate the reception of the one-time password that is used to login to the system. The mobile device was also used to simulate the reception of notifications for updates in OJT-related forms and documents.

The construction phase underwent system evaluation. This is to ensure that the system is free from syntax and logic errors. Test and debug processes were conducted, and when errors appeared in the system, its structure and program were corrected to guarantee the reliability and quality of the system.

3.7. Cutover

This phase is implemented after the construction phase, where the system was developed. A full-scale test was conducted in this phase to ensure that all the modules and their features met the required specifications and standards. The upload required forms feature was tested to see if it allowed the OJT coordinator to upload the necessary document templates. It was also tested to see if it enabled the OJT coordinator to edit and set the deadlines for the training documents. The download-required document feature was tested to see if it allowed the trainees to download the documents uploaded by the OJT coordinator. In addition, if the downloaded document automatically incorporated the details of the trainees into the file. The upload accomplished document feature was tested to see if it enabled the trainees to upload their training forms and reports. The document monitoring function was tested to see if its three-fold monitoring function was met. In particular, if it allows the trainees to monitor their pending and submitted documents and reports; if it enables the OJT advisers to monitor the documents and reports of the trainees; and if it allows the OJT coordinator to monitor the trainees across different programs. The narrative repository feature was tested to see if it could successfully store accomplished narratives and if it could be browsed by other users. The notification function was tested to see if it successfully notified the users of each important process. The student monitoring feature was tested to see if it enabled the trainees to browse their profiles and monitor their progress. The passwordless authentication log-in system was tested to see if it successfully sent one-time passwords to the users based on its protocol. The content management function was tested to see if it allows the system administrator to edit the system contents, such as mission, vision, address, quality policies, and core values. Lastly, the user management function was tested to see if it enables the system administrator to assign authorities to the users, such as being an OJT adviser and OJT coordinator.

Upon the completion of the testing and after the system passed the software evaluation, it was deployed at Cavite State University – Carmona Campus.

3.8. Evaluation

The software was evaluated based on various criteria, such as portability, maintainability, security, reliability, usability, compatibility, performance efficiency, and functionality stability. These factors are based on ISO 25010 and are especially used for system and software quality requirements and evaluation. Functional suitability concerns whether a software product meets functional requirements. It deals with the appropriateness, correctness, and completeness of the software. Performance efficiency concerns whether a software product can effectively make use of the given resources. It involves the capacity, resource utilization, and time behavior of the system. Compatibility concerns whether a software product can consistently perform its functions while exchanging information and sharing resources with other products. It includes the interoperability and co-existence of the software. Usability concerns whether users can effectively and efficiently use a software product to complete tasks. It deals with the operability, learnability, and recognizability of the system. Reliability concerns whether a software product can perform desired functions after being scheduled to work. It involves the recoverability, fault tolerance, availability, and maturity of the software. Security concerns whether a software product can protect its data and only allow authorized users to access the data. It includes the authenticity, accountability, non-repudiation, integrity, and confidentiality of the system. Maintainability concerns whether a software product can be easily modified, repaired, and updated by maintainers. It deals with the testability, modifiability, analyzability, reusability, and modularity of the software. Lastly, portability concerns whether a software product can be easily used in different environments. It involves the replaceability, installability, and adaptability of the software.

3.9. Unit testing

In this phase, the system was tested down to its units, or the smallest parts. The testing was guided by the procedures, and remarks were noted during the testing. The units that failed the testing were corrected and re-evaluated until they passed the testing. This ensures that the smallest components of the modules and their features meet the standard requirements for their operation. The tested modules were the OJT coordinator, OJT adviser, student, and system administrator modules. The tested features were the upload required form, download document, upload document, document monitoring, narrative repository,

notification, student monitoring, passwordless authentication log-in, content management, and user management functions.

3.10. System testing

The system testing was evaluated by 10 IT experts with at least two years of experience in software and system development. The evaluation tool used was adapted from ISO 25010 Product Quality, which is especially used for software development. The purposeful sampling technique was used in selecting the respondents in this testing. After discussing the nature of the study, the functionalities of the system were demonstrated to the respondents. The respondents were also given ample time to utilize and try the system. The respondents' queries regarding the system and its functions were answered and clarified by the researcher. The evaluation with the use of the tool proceeded after the demonstration and utilization of the system's functions.

3.11. Acceptance testing

The acceptance testing of the system was evaluated by one OJT coordinator, three OJT advisers, among them from different programs on campus, and 244 OJT students. The sample size of the respondents for the acceptance testing was determined using Krejcie and Morgan's (1970) formula. The evaluation tool used was adapted from ISO 25010 Quality in Use, which is especially used for the assessment of product acceptance. The formula below was used in identifying the sample size of the respondents.

3.12. Data analysis

The Likert's scale, with a range of 1 to 5, was used in measuring the attitudes and opinions of the respondents. This scale is widely used in the evaluation process of many studies involving projects and software development. On the scale, 5 is outstanding, 4 is very satisfactory, 3 is satisfactory, 2 is unsatisfactory, and 1 is poor. The mean of every criterion was computed, and it served as their weighted mean, whereas the Andale (2014) formula was used in calculating the overall weighted mean of the criteria. Further, in interpreting the computed mean, the mean interpretation table from Bicol University (n.d.) was used.

4. Findings and Discussion

4.1. Internship management procedures

The system digitalizes the processes involved in the internship program, including the profiling of trainees, the request, approval, and release of documents, monitoring of in-service requirements, and generation of reports and summaries, making the document processing remote and mostly paperless.

The system administrator assigns the user type and authorization to the users, including the internship coordinator, advisers, and trainees. The administrator gives the internship coordinator the most authorization of the system's content. If any change in designation happens, new authorization will be given and the old will be removed. The internship coordinator can view the list of advisers and their handled trainees in the students tab. This list is normally updated after enrollment. Once the semester starts and there are announcements to be made, the coordinator can publish contents in the system using the announcement tab. Moreover, the coordinator can upload document templates in the format and narrative tabs, such as registration form, curriculum vitae, recommendation letter, memorandum of agreement, waiver, training plan, journal, certificate of completion, and narrative report. Also, the coordinator can view the profile, status, and requirements of the students and proceed with downloading if needed to. Furthermore, the system enables the coordinator to generate reports, including a summary of advisers, trainees, requirements, and progress of the internship program.

The advisers can access the list of trainees in the student tab. Similar to the coordinator, the advisers can view the profile, status, and requirements of the students. The summary of the student requirements and status is presented in the system as a table. Moreover, the advisers can message and notify to communicate instructions with the trainees. Also, the advisers can monitor, approve, and upload the requested documents of the students in the requirements tab. The documents, such as recommendation letters and memoranda of agreement, can be generated automatically when the students complete the document templates in the system. The completion of the requirements happens before the deployment of the trainees to avoid problems. When the training is in progress, the advisers can monitor the progress and journals of the trainees using the system. Similar to the coordinator, the advisers can also generate reports and summaries.

The trainees are given the authorization to access the system after enrolling in the internship program. The system enables the trainees to view their profile, status, and requirements in the profile tab. If the trainees need to request a particular document, it can be done in the requirements tab. The request can be monitored remotely and in real-time using the system. The instructions of the advisers through messages in the system can be seen in the notification tab, whereas announcements made by the coordinator can be viewed in the announcement tab. In addition to these, the trainees can view and read completed narrative reports in the narrative tab.

The access of the system and its modules, units, and data is secured by the passwordless authentication method implemented. The system is exclusive to the users with registered email and mobile number. This enables the system to send one-time passwords to users trying to access the system. This enhances the security of the system and avoids risks such as data breaches and phishing.

Passwordless authentication login. The starting point of the system is the landing page shown in figure 4. The page contains the name of the university and the system. It also has buttons that direct to the home, mission and vision, information about the system, and a login system. The login button directs the user to the text field dedicated to selecting the method of receiving the verification code, such as SMS or email. After inputting the mobile number or email, the login button should be clicked for confirmation. The verification code will be sent, and the user has 5 minutes to input the code for validation (figure 5). When the code is entered into the input box, the proceed button should be clicked to continue the process. In case of a delay or problem, the button named resend authentication code can be clicked for a new code.

OJT coordinator module. The OJT coordinator module as shown in figure 6 enables the user to upload document and form templates to the system. In the format tab of the module, a dropdown can be clicked to select the type of document to be uploaded. It includes the registration form, curriculum vitae, recommendation letter, MOA, student waiver, OJT training plan, daily journal, certificate of completion, and narrative report. Once the type is selected, the choose file button can be clicked to browse for the files on the computer to be uploaded to the system. The module also includes tabs, such as requirements, students, monitoring, and narrative.

Figure 4

CIMS Landing Page

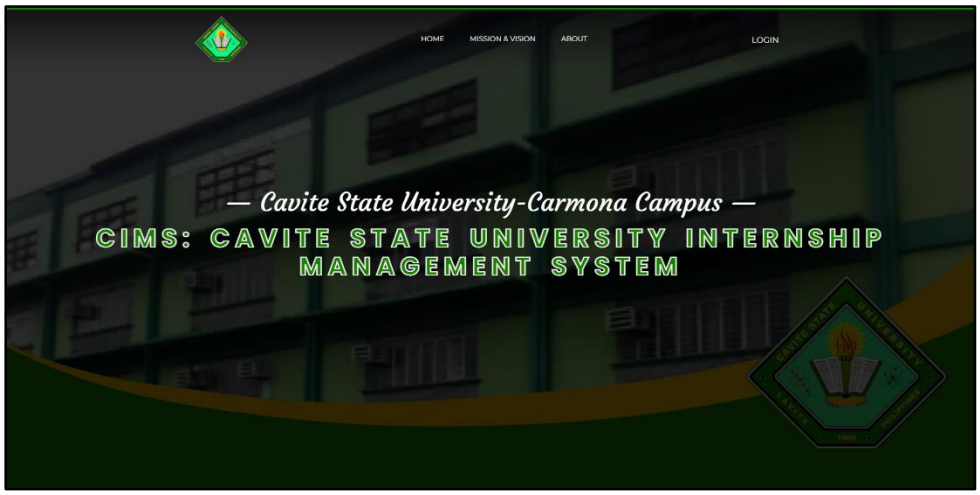


Figure 5

Verification Code Input

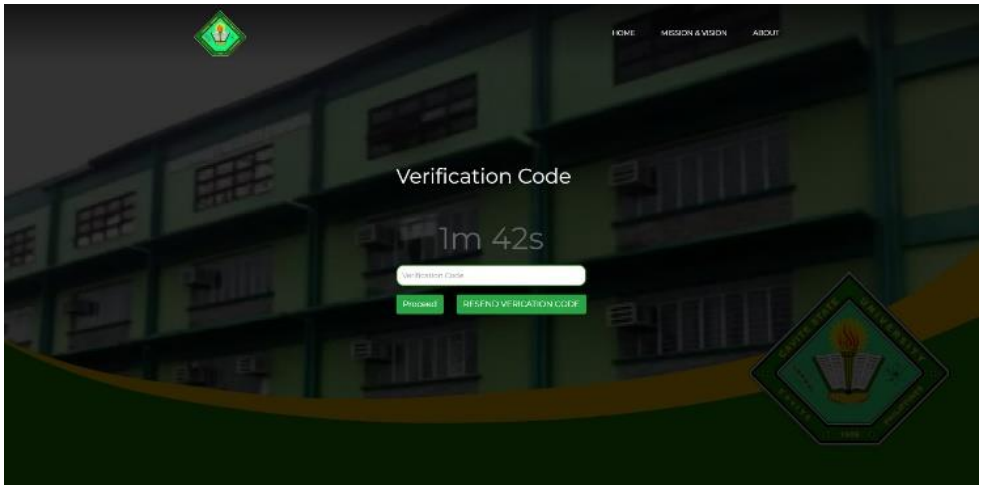
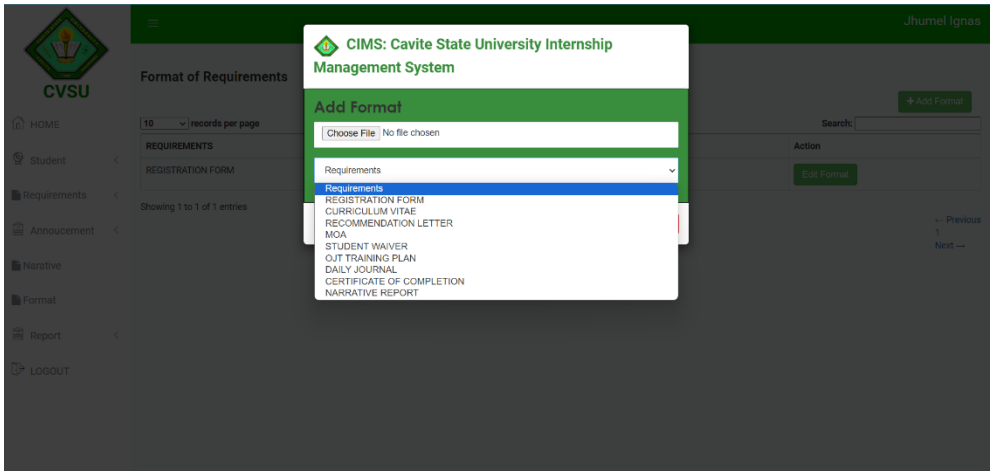


Figure 6

Uploading of Document Format



OJT adviser module. The OJT adviser module contains access buttons for home, students, requirements, registrations, requests, status, and settings. A search bar is also provided for easy access. In the case of a request for a recommendation letter or memorandum of agreement by a student, a table that contains the student's name and number of requests can be viewed as illustrated in figure 7. On the right side of the items, a button can be clicked to proceed with an action.

Figure 7

Recommendation Letter Requests

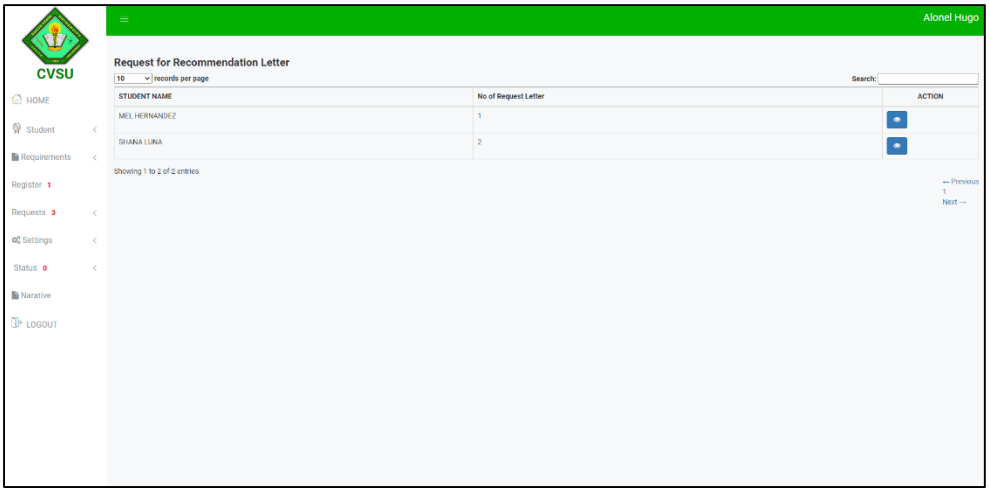
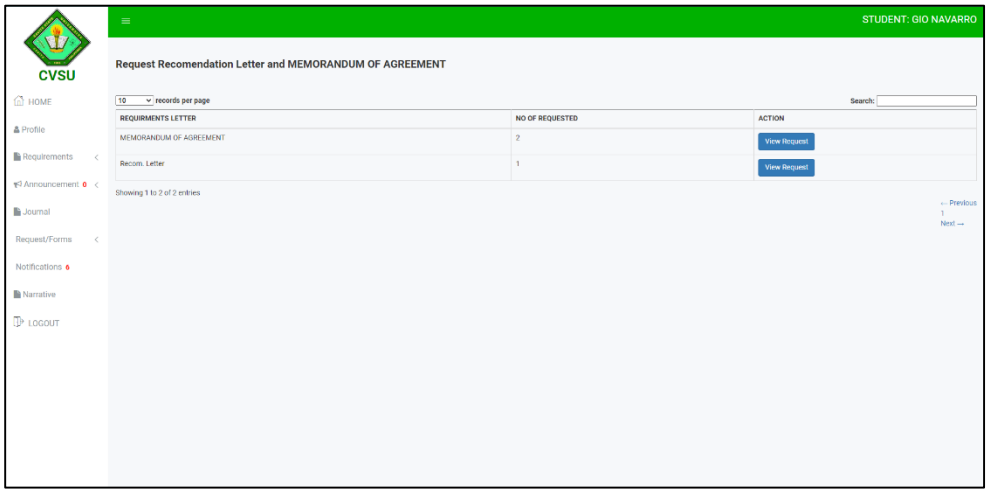


Figure 8

Student Requests for Recommendation Letter and MOA

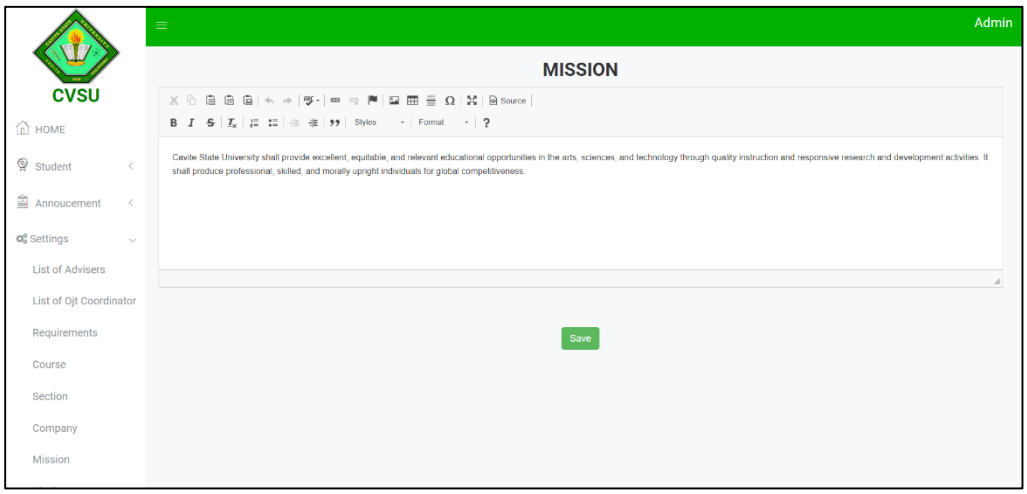


Student module. The student module contains access buttons for home, profile, requirements, announcements, journals, requests and forms, notifications, and narrative. Requests for a recommendation letter and memorandum agreement can be viewed and accessed in a table provided by this module as illustrated in figure 8. The table contains the

names and numbers of requests for the requirements. A search bar is provided for increased accessibility, and a view request button can be clicked to view the status of the request.

System administrator module. The system administrator module enables the user to edit and update information in the system, including the mission (Fig. 9), vision, and quality policy of the university. The module contains access tabs, such as home, announcements, list of advisers, and list of coordinators. Further, the module contains a text box and basic text editing tools to serve its function. After editing, the system administrator must click the save button to finish the process.

Figure 9
Content Management (University Mission)



4.2. System evaluation results

The summarized result of the unit testing is presented in table 3. All of the modules of the system got successful remarks during the first test. The features of the modules based on the requirements were all met. Similarly, in the test for platform compatibility, the system ran through different environments successfully without any errors. The system was tested on Google Chrome, Mozilla Firefox, Microsoft Edge, and Opera. However, in the test for the passwordless authentication method in terms of security, minor problems were encountered due to the delays in latency. After two tests, the issue was addressed by calibrating the time counter to compensate for the gap and delay.

Table 3

Unit testing result summary

Criteria	Units	No. Of Tests
Module	OJT Coordinator	1
	OJT Adviser	1
	Student	1
Security	System Administrator	1
	Passwordless Authentication	2
Platform	Google Chrome	1
	Mozilla Firefox	1
	Microsoft Edge	1
	Opera	1

Table 4

Overall system testing results

Item	Frequency					Average per Indicator	Average per Criterion	Standard Deviation
	5	4	3	2	1			
1	10	0	0	0	0	5.00		0.00
2	9	1	0	0	0	4.90	4.83	0.32
3	6	4	0	0	0	4.60		0.52
4	4	6	0	0	0	4.40		0.52
5	3	7	0	0	0	4.30	4.40	0.48
6	5	5	0	0	0	4.50		0.53
7	5	5	0	0	0	4.50		0.53
8	6	4	0	0	0	4.60	4.57	0.52
9	6	4	0	0	0	4.60		0.52
10	4	4	2	0	0	4.20		0.79
11	3	6	1	0	0	4.20	4.43	0.63
12	3	7	0	0	0	4.30		0.48
13	10	0	0	0	0	5.00		0.00
14	9	1	0	0	0	4.90		0.32
15	2	8	0	0	0	4.20	4.50	0.42
16	4	6	0	0	0	4.40		0.52
17	10	0	0	0	0	5.00		0.00
18	10	0	0	0	0	5.00	4.97	0.00
19	9	1	0	0	0	4.90		0.32
20	8	2	0	0	0	4.80		0.42
21	10	0	0	0	0	5.00	4.70	0.00
22	5	3	2	0	0	4.30		0.82
23	10	0	0	0	0	5.00		0.00
24	8	2	0	0	0	4.80	4.90	0.42
25	9	1	0	0	0	4.90		0.32
Overall							**4.66**	**0.38**

Legend: 1.00-1.80 – Poor, 1.81-2.60 – Fair, 2.61-3.40 – Satisfactory, 3.41-4.20 – Very Satisfactory, 4.21-5.00 - Outstanding

The system passed both the system (table 4) and the acceptance testing (table 5) based on the instruments adopted from ISO 25010. The criteria used were functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability. The system got an average mean score of 4.66 in the system evaluation, whereas it got 4.34 in the acceptance evaluation. Both results got an adjectival rating of outstanding. This implies that the system successfully passed the evaluation and is ready for utilization.

Table 5
Acceptance testing results

Item	Frequency					Average per Indicator	Average per Criterion	Standard Deviation
	5	4	3	2	1			
1	220	28	0	0	0	4.89	4.91	0.32
2	232	16	0	0	0	4.94		0.25
3	30	178	40	0	0	3.96	3.92	0.53
4	8	203	37	0	0	3.88		0.41
5	187	54	7	0	0	4.73	4.33	0.51
6	3	226	19	0	0	3.94		0.29
7	2	163	83	0	0	3.67	3.83	0.49
8	12	159	77	0	0	3.74		0.54
9	17	231	0	0	0	4.07	4.45	0.25
10	202	46	0	0	0	4.81		0.39
11	56	159	33	0	0	4.09		0.59
12	243	5	0	0	0	4.98	4.98	0.14
13	245	3	0	0	0	4.99		0.11
14	15	231	2	0	0	4.05	3.88	0.26
15	6	161	81	0	0	3.70		0.51
16	218	30	0	0	0	4.88	4.43	0.33
17	0	241	7	0	0	3.97		0.17
Overall							**4.31**	**0.36**

Legend: 1.00-1.80 – Poor, 1.81-2.60 – Fair, 2.61-3.40 – Satisfactory, 3.41-4.20 – Very Satisfactory, 4.21-5.00 - Outstanding

5. Conclusion

The study concludes the successful development of the CIMS and integration of the passwordless authentication technology, and the acceptance of the entire system. The system provides a web-based platform for the internship coordinator, advisers, and trainees to process necessary documents efficiently, remotely, and real-time. The modules enable the users to view, upload, download, request, approve, release, and monitor documents just by navigating the system. Also, the system serves a safe repository of the internship documents, such as trainees' profiles and reports. In addition, the CIMS becomes a medium for

communication through its messages, notifications, and announcements features. Further, the system enables fast generation of reports and summaries. Moreover, the use of the passwordless authentication method eliminates the use of preset passwords and protects the system from the vulnerabilities that come with traditional passwords, such as server breaches, phishing, and hacking. This secures the data of the stakeholders in the developed internship document management system. Given the results of the study, it was recommended to provide an additional method for passwordless authentication dedicated to iOS users to enhance accessibility.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Funding
This work was not supported by any funding.

ORCID
St. Joseph M. Lumbog – https://orcid.org/0009-0002-0740-7797
Maricel M. Gaspar - https://orcid.org/0000-0001-8486-6490

References

Abacı, K., & Medeni, I. T. (2022). Efficiency of electronic document management systems: A case study. *Sci. Educ. Innov. Context Mod. Probl*, *5*, 75-86.

Afrizal, W., Lubis, M., & Musnansyah, A. (2021). Design approach in Document Management System: the development of EZDESK Dashboard. *MATEC Web of Conferences*, *348*, 01006. https://doi.org/10.1051/matecconf/202134801006

Andriansyah, R. & Elmi, F. (2020). Analysis of the effect of electronic document management system, organizational commitment and work satisfaction on employee performance. *International Journal of Innovative Science and Research Technology*, 5(8), 944-952.

Angala, D., Casugay, B. C., Estillore, H. M., Lebantino, J., Marcha, S., & Villanueva, G. J. (2023). Development and implementation of Document Management System for

Ilocos sur Polytechnic State College, Tagudin Campus. *E-Dawa an International Multidisciplinary Research Journal, 3*(Special Issue). https://doi.org/10.56901/hpcb6748

Chebotareva, A. A., & Chebotarev, V. E. (2021). Hardware, biometric and passwordless authentication: vulnerability and cybercrime issues. *IOP Conference Series. Materials Science and Engineering, 1069*(1), 012038. https://doi.org/10.1088/1757-899x/1069/1/012038

Firdaus, D., & Jumaryadi, Y. (2020). Implementation of Document Management System using Levenshtein Distance Algorithm. *International Journal of Computer Applications, 176*(16), 18–24. https://doi.org/10.5120/ijca2020920091

Furuberg, I. L., & Øseth, M. (2023). *From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication (Master's thesis, NTNU).*

Gani, D.H.A., Abd Kadir, I.K., Rahman, A.A., & Yunus, A.M. (2024). Electronic document management system in electronic government environment. In A.K. Othman, M.K.B.A. Rahman, S. Noranee, N.A.R. Demong, & A. Mat (Eds.), *Industry-Academia Linkages for Business Sustainability*, vol 133. European Proceedings of Social and Behavioural Sciences (pp. 585-597). European Publisher. https://doi.org/10.15405/epsbs.2024.05.48

Gonçalves E., Teixeira P., and Silva J.P. (2020). Development of GDPR-Compliant Software: Document Management System for HR Department. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain,* 1-6. https://doi.org/10.23919/CISTI49556.2020.9140922

Hernandez, R., & Hernandez, R. L. (2022). Delivery, support, and influence of ICT infrastructure towards digital empowerment: A proposed stakeholders' collaborative framework. *International Journal of Open-Access, Interdisciplinary & New Educational Discoveries,* 1(2), 48-59.

Jones, S. (2012). eGovernment Document Management System: A case analysis of risk and reward. *International Journal of Information Management*, 32(4), 396-400. https://doi.org/10.1016/j.ijinfomgt.2012.04.002

Justina, I. A., Oyekan, E. A., & Orogbemi, O. M. (2022). A secured cloud-based electronic document management system. *International Journal of Innovative Research and Development, 11(12),* 38-45. https://doi.org/10.24940/ijird/2022/v11/i12/dec22010

Kunke, J., Wiefling, S., Ullmann, M., & Lo Iacono, L. (2021). Evaluation of account recovery strategies with FIDO2-based passwordless authentication. *arXiv (Cornell University).* https://doi.org/10.48550/arxiv.2105.12477

Lyastani, S. G., Schilling, M., Neumayr, M., Backes, M., Bugiel, S. (2020). Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication. *IEEE Symposium on Security and Privacy.* https://doi.org/10.1109/sp40000.2020.00047

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *HOTP: an HMAC-Based One-Time password Algorithm.* https://doi.org/10.17487/rfc4226

Malekani, A.W. (2023). Examining the efficacy of electronic document management system and employees' perceptions of its usefulness at Sokoine University of Agriculture. *University of Dar es Salaam Library Journal,* 18(1), 112-133. https://dx.doi.org/10.4314/udslj.v18i1.8

Matiushin, I., & Korkhov, V. (2021). Passwordless authentication using magic link technology. *9th International Conference Distributed Computing and Grid Technologies in Science and Education.* https://doi.org/10.54546/mlit.2021.89.13.001

Oduguwa, T., & Arabo, A. (2024). Passwordless authentication using a combination of cryptography, steganography, and biometrics. *Journal of Cybersecurity and Privacy*, 4(2), 278-297. https://doi.org/10.3390/jcp4020014

Parmar, V.H.A., Sanghvi, R., Patel, H. & Pandya, A.S. (2022). A comprehensive study on passwordless authentication. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS),* 1266-1275. https://doi.org/10.1109/ICSCDS53736.2022.9760934

Prasad, A. (2024). A comparative study of passwordless authentication. *TechRxiv.* https://doi.org/10.36227/techrxiv.171560547.71979752/v1

Rathnayaka, L.S.D., Malsha Nadeetharu, B.K. & Kulatunga, U. (2024). Applicability of electronic document management system (EDMS) for the cost management of mega construction projects in Sri Lanka. *Journal of Financial Management of Property and Construction*, 29(2), 314-330. https://doi.org/10.1108/JFMPC-01-2023-0005

Rosa, A. P. M. D., & Galang, G. M. (2023). Development of a curriculum management system for a state university in the Philippines. *International Journal of Emerging Technologies in Learning (iJET)*, 18(18), 222–233. https://doi.org/10.3991/ijet.v18i18.39377

Rydell, J., Pei, M., & Machani, S. (2011). *TOTP: Time-based one-time password algorithm.* https://doi.org/10.17487/rfc6238

Shakil, A. F., Zaidi, S. A., & Rafiullah, S. (2023). Exploring the need of internship program for productive learning among students at college level in Pakistan. *Voyage Journal of Educational Studies, 3*(2), 1–16. https://doi.org/10.58622/vjes.v3i2.43

Tkachenko, A. L., & Денисова, Л. А. (2022). Designing an information system for the electronic document management of a university: automatic classification of documents. *Journal of Physics: Conference Series, 2182*(1), 012035. https://doi.org/10.1088/1742-6596/2182/1/012035

Ukwandu, E., & Bennett, A. (2023). *Exploring the views of end-users on passwordless authentication methods.* https://doi.org/10.2139/ssrn.4616393

Yoshimura, Y., Suga, Y., Omori, Y., Yamashita, T., & Shibata, A. (2019). Privilege sharing and transfer based on passwordless authentication. *NTT Technical Review, 17*(6), 37–40. https://doi.org/10.53829/ntr201906fa11

Zabukovšek S.S., Jordan, S., Bobek, S. (2023). Managing document management systems' life cycle in relation to an organization's maturity for digital transformation. *Sustainability*, 15(21), 15212. https://doi.org/10.3390/su152115212