**Web-based Paperless Clearance Management**

**System with DSA (Digital Signature Algorithm) Encryption**

**in Concepcion Holy Cross College Inc.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**A Thesis Presented to**

**The Faculty of the College of Computer Studies**

**Concepcion Holy Cross College Inc.**

**Concepcion, Tarlac**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**In Partial Fulfillment**

**of the Requirements for the Degree**

**Bachelor of Science in Computer Science**

**by:**

**Nicole G. Ballesteros**

**Jerald E. Cutchon**

**Arvin P. Gomez**

**2023**

# Table of Contents

[**1** **INTRODUCTION\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_1**](#_heading=h.2et92p0)

[**1.1** **Project Context\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_3**](#_heading=h.tyjcwt)

[**1.2** **Purpose and Descriptions\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_6**](#_heading=h.3dy6vkm)

[**1.3** **Objectives\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_7**](#_heading=h.1t3h5sf)

[**1.4** **Scope and Delimitations\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_9**](#_heading=h.4d34og8)

[**Algorithm Matrix\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_10**](#_heading=h.4d34og8)

[**REFERENCES\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_13**](#_heading=h.26in1rg)

# INTRODUCTION

Adapting to new technology is an essential part of life in the modern world. With the rapid pace of technological advancement, individuals, businesses, and society must adapt to new and emerging technologies to stay competitive and keep up with the times. New technology improves efficiency and productivity, which leads to new and better ways of doing things and keeps us competitive in today's fast-paced business environment.

Even though new technology sounds promising, cyber-attacks are still a significant concern in today's digital world, and encryption plays a crucial role in protecting against these threats. Without encryption, sensitive information transmitted and stored digitally is vulnerable to being accessed by unauthorized parties, which can lead to data breaches and other security incidents [1]

Since technology has developed, many schools are enhancing their administrative functions by automating nearly all manual procedures, including the clearance system. [2] A student clearance is a process that many schools and universities require their students to complete before they can graduate or move on to the next academic level. This process typically involves completing several administrative tasks and submitting various documents, such as transcripts and proof of completion of required courses.

The purpose of a student clearance is to ensure that all students have fulfilled their program's academic and administrative requirements and are eligible to move on to the next phase of their education. This process is often time-consuming and confusing, especially for students unfamiliar with the requirements.

A student ready to leave an institution must go through a clearance procedure to determine if they will be allowed to sign off or not. The person would receive a clearance if permission were granted. [3]. Some universities still implement the traditional way of signing clearance: the student needs to visit the office, receive the clearance form and fill out related fields. The student is also required to hand over their ID for verification and obtain approval from different offices such as the Library Office for checking of borrowed and unreturned books, the Office of Student Affairs Office for violations or disciplinary actions that should be cleared by the students, Cashier Office for unpaid balance or tuition fees, and the Registrar Office for requirements that should be submitted such as personal documents and transfer credentials. [4]

Thus, the researchers conducted a study entitled Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College. It is a paperless clearance system that encrypts e-signatures into digital signatures. An e-signature is a type of electronic signature that can be used to sign documents electronically. It typically involves a person writing or drawing their signature using a computer mouse or touchpad, and then inserting the image into a document.

A digital signature, on the other hand, is a type of electronic signature that uses cryptography to verify the authenticity of the signature and the document. Digital signatures use a complex mathematical algorithm to create a unique code that is attached to the document, which can be used to verify the document's authenticity. Unlike e-signatures, digital signatures are considered to be a more secure and legally binding way to sign documents electronically. [5]

The objective of digital signatures is to authenticate and verify documents and data. This is necessary to avoid tampering and digital modification or forgery during the transmission of official documents. [6] To avoid this forgery, the researchers will use DSA Algorithm Encryption. Digital Signatures Algorithm is a FIPS (Federal Information Processing Standard) for digital signatures. It was proposed in 1991 and globally standardized in 1994 by the National Institute of Standards and Technology (NIST). It functions on the framework of modular exponentiation and discrete logarithmic problems, which are difficult to compute as a force-brute system.[6] Digital Signatures Algorithm uses a key that is 2048 bits long, DSA is robust, works intensely fast, is free from patents, and requires little storage space. While compared with specific other signature verification algorithms, DSA is relatively superior. Generating the key is quick. The DSA cycle requires minimum space. 'Patent-free' indicates that it costs nothing globally and thus lies within reach of everybody. [7]

## Project Context

The lack of a clearance form can cause a number of problems for schools and students. It can make it difficult for schools or any organization to collect important information about students, keep track of their progress, and maintain accurate records. It is important for schools to have a clearance form to ensure that they can provide the best possible support and resources for their students [8].

As of now, Concepcion Holy Cross College Inc. does not have a clearance for students. And they are currently implementing a clearance system. However, this clearance they are implementing is still a traditional manual procedure. These must be signed in paper copy and brought to the various departments for approval, which when properly completed, indicate that the student has satisfied all criteria and is not owed to any of the departments or units that the student was affiliated with inside the college. The document must be delivered in a hard copy to designated offices, personally, making this method time-consuming.

The traditional clearance process faces several obstacles such as time wastage due to long queues of students; students traveling long distances and bouncing because administrators are not in the office; a lack of cooperation between students and administrators when cross-checking records; and bureaucracy regarding which unit clears first [8].

Therefore, we realized the need to develop an online clearance system that serves as a more reliable, effective, and easier means of undertaking students’ clearance. With an online clearance system, students of Concepcion Holy Cross College are able to undertake clearance without having to visit the physical location of all offices, reduce delay and stress, and know the clearance procedures and requirements.

Using the Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption, the clearance management will be automated, and all of the processes will be handled through the system, which will result in paperless improvement. With this, the institute's information will be accurate and help prevent data loss.

This system also has encrypted signatures, a type of digital signature that uses encryption to secure the signature and verify the signer's identity. This ensures that only the signer can create a valid signature and makes it difficult for someone to forge the signature or alter the signed document in any way. If the decrypted signature matches the signed document, it can be proved that the signature is valid and that the signer is who they claim to be. This provides a secure and verifiable way to sign digital documents.

One of the main reasons why encryption is necessary to protect against cyber-attacks is that it makes it much more difficult for attackers to access sensitive information. Encryption uses complex mathematical algorithms to scramble data into a code that can only be decrypted by someone with the correct key. This means that even if an attacker is able to intercept the encrypted data, they will not be able to read it or use it without the key.

Fraud and reliability are the common risks of e-signatures where there’s still a high risk of signatory forging and fraud for organizations as technology can be compromised or hacked, this can put sensitive information at risk and make it difficult for users to trust electronic signature solutions.

The researchers come up with an encryption solution because it helps to protect sensitive information and prevent unauthorized access. When electronic signatures are encrypted, the information they contain is scrambled and can only be decrypted by someone with the appropriate key. This helps to prevent hackers or other unauthorized individuals from accessing the information contained in the electronic signature. Encryption can also help to ensure the authenticity and integrity of electronic signatures. By using encryption, it is possible to verify that an electronic signature has not been altered or tampered with, which helps to maintain the integrity of the signed document or transaction. Overall, encryption can help to make electronic signatures a more reliable and trustworthy option for completing signing documents.

## Purpose and Description

The purpose of this study is to develop a Web-based Paperless Clearance System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College. This research is intended for students who wish to leave the college or request a personal record. An encryption will be used to protect e-signatures of the assigned staff per department to avoid tampering, forgery and digital modification.

This system will be beneficial to:

**To the Registrar.** He/she will immediately view the students’ clearance progress, as well as see if the student is cleared to other departments.

**To the Office of Student Affairs** **(OSA).** This research can help the department to check any pending student account that needs approval and change clearance status.  
 **To the Library.** This research helps the department to view any pending student account that needs approval and change clearance status.

**To the Student.** This researchwill be also beneficial to them in terms of monitoring clearance progress as well as their violations.

**To the Researcher.** The researcher would acquire new knowledge, abilities, and research-planning techniques.

**To the Future Researchers.** This research will be beneficial to future researchers as their guide while gathering data regarding the Clearance Management System.

## Objectives

The general objective of this research is to design and develop a paperless clearance management system that will help graduating students get their clearances quickly. This will also help students that are currently enrolled monitor their clearance progress.

This research aims to achieve the following:

1. To design and develop a Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College Inc. associated with the following features:
   1. Admin
      1. Add Office of Student Affairs (OSA) staff Account
         1. View OSA staff Information
         2. Manage OSA staff Information
            1. Add Information
            2. Edit Information
            3. Delete Information
      2. Add Library Staff Account
         1. View Library staff Information
         2. Manage Library staff Information
            1. Add Information
            2. Edit Information
            3. Delete Information
      3. Add Registrar Staff Account
         1. View Registrar staff Information
         2. Manage Registrar staff Information
            1. Add Information
            2. Edit Information
            3. Delete Information
      4. Add Cashier Staff Account
         1. View Cashier staff Information
         2. Manage Cashier staff Information
            1. Add Information
            2. Edit Information
            3. Delete Information
      5. Add Student Account
         1. View Student Information
         2. Manage Student Information
            1. Add Information
            2. Edit Information
            3. Delete Information
   2. Registrar
      1. View List of User Accounts
      2. Deploy Student Clearance
         1. Notify Departments for Clearance
      3. View Pending Student Clearance
         1. Approve Student Clearance
         2. Disapprove Student Clearance
         3. Update Student Clearance Status
   3. Office of Student Affairs (OSA)
      1. View Pending Student Clearance
         1. Approve Student Clearance
         2. Disapprove Student Clearance
         3. Update Student Clearance Status
   4. Library Staff
      1. View Pending Student Clearance
         1. Approve Student Clearance
         2. Disapprove Student Clearance
         3. Update Student Clearance Status
   5. Cashier Staff
      1. View Pending Student Clearance
         1. Approve Student Clearance
         2. Disapprove Student Clearance
         3. Update Student Clearance Status
   6. Student
      1. View Clearance Progress.
   7. DSA Algorithm Encryption
      1. Encryption of e-signatures

## Scope and Delimitation

The aim of this study is to develop a computer software system to improve manual clearance procedures. As well as for the students to easily monitor the clearance progress in Concepcion Holy Cross College. The Web-based Paperless Clearance Management System DSA (Digital Signature Algorithm) Encryption Concepcion Holy Cross College is inclusive for undergraduate and graduate students only. Also, this study will use dummy data to test or demo the system.

The system process will start with creating an account per department which will be done by the main admin or the registrar that plays two roles and can (add, edit, and delete) a department staff account. For the student counterpart, the registrar can (add, edit, and delete) a student account, deploy student clearance, and approve/disapprove student clearance. The approving officer per department are the library, Office of Student Affairs (OSA), and the cashier they can update, approve/disapprove a student clearance and can indicate a reason for disapproval. Lastly, the students can only view their clearance progress in real-time.

# RELATED LITERATURE

## Discussion of Model

The Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College is an online clearance system that the researchers propose for the CHCCI students and offices. It implements authentication for users and encryption of web content; and evaluates the functionality, reliability, usability, and portability of the system. This web application has the capability to guarantee the security of the data it stores.

### Foreign Literature

The literature entitled "Improving the Student Clearance Process through Technology: A Case Study" examined the student clearance process at a large university and identified several opportunities for improvement through the use of technology. The authors proposed the development of a centralized, online system that would allow students to complete the clearance process electronically, including submitting required documents, paying fees, and tracking their progress. The study found that this approach would reduce the time and effort required for students to complete the clearance process, as well as improve the efficiency and accuracy of the process for the university. [9]

This literature and the one we are studying look at the same objective. Utilizing a technological tool in order to achieve a more streamlined operation is one of our primary goals here at the school and to apply this in the student clearance process.

The literature entitled "The impact of a comprehensive student clearance process on student retention and graduation rates" examined the relationship between student clearance and student outcomes. The researchers found that students who completed the student clearance process were more likely to graduate and had higher retention rates compared to those who did not. [10]

This study points out that the students that completed the clearance process were more likely to graduate. Which was a feature in our study, where the clearance administrator can monitor the students that are more likely to graduate based on the clearance progress.

The study entitled. “Development of Online Clearance System for an Educational Institution” aims to create an online clearance management system to overcome the issue of manual processing. It will also reduce the amount of time and effort. With this, students can monitor their clearance whenever they are online. [11]

Both systems aim to address the issue of the manual process of taking and monitoring student clearance and improve the way of taking and monitoring clearance.

The major goal of this literature, "Predictors of Zero Tolerance Policy Violations Among High School and Middle School Students," was to find a set of characteristics that may help determine the situations that cause a student to break zero-tolerance rules. This literature investigated whether the qualification variable, zero-tolerance policy violation, can be predicted by a set of five risk factors: (i) grade level, (ii) retention, (iii) suspension, (iv) race, and (v) gender. [12]

This literature aims to know whether the following criteria have an effect when it comes to the student who violates the rules of the school. This will also can be used in the researcher’s literature when giving clearance to students.

### Local Literature

According to (Caroro, R. A., & Hernandez, A. A.), the research is about determining the level of green IT implementation at a university for the purpose of achieving environmental sustainability and a decrease in operational costs. In order to contribute to an ongoing effort to increase green IT stewardship and implementation. [13]

When it comes to migrating to paperless improvement, this body of literature aims to do the same thing that our study will undertake in order to fulfill its goals. Its goal is to reduce the amount of damage that is caused to the natural world by information technology operations by promoting environmentally responsible practices in all aspects of the industry.

According to Mark Kevin V. Rimando and Reynaldo R. Corpuz, schools' top concerns are about the use of paper-based forms and how they track their progress and location. This literature investigated the use of watermarking algorithms and QR code-based tracking systems. In addition, it discusses the structure, applications, security, and strategies for using QR codes. According to related research, existing watermarking techniques may be developed in terms of discreetness and durability in the future. [14]

This article is related to using the Real-Time tracking System. It is used to track all the violations that a student has disobeyed and to the general concern about the use of the manual process for tracking, what the researcher wants to do is to improve this process so that the user will not have difficulty using it.

### Foreign Study

According to Rochmawati, N. et al, Laboratory Clearance Form application using QR codes utilize the Bootstrap framework, which supports responsive web design. The framework enables access to the application through a mobile device. The final product is anticipated to be a design of the application to make it easier for students who will graduate to obtain their Laboratory Clearance Form in the Departments of Engineering faculty of UNESA. [15]

This study and the Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College serve the same purpose, goal to make an online clearance system. It also supports web responsive design, making the system more interactive.

According to Albert, M. B. G., the primary goal was to create an online clearance system that would replace manual forms in a reliable, efficient, effective, and transparent manner. As long as the devices they are using can access the internet, this system enables final-year students to check the status of their clearance forms online. [16]

Both studies have a clearance management system that allows ~~the~~ users to monitor the status of their clearance forms online. The use of the Clearance System will eliminate the manual process of taking clearance. Due to that, future users can save time, and prevent data loss.

Constructing a new system or changing an existing system in accordance with stakeholder requirements is the goal of system implementation. A student requests clearance, and an SMS message is delivered to the administrative staff handling the department's student clearances. [17]

This study aims to design and implement a Web-Based SMS-Notification Clearance System. The student will apply to the clearance system and receive an SMS text for confirmation. Both studies have clearance management systems that can help students in school to reduce the time and efforts that consume by manual processes.

### Local Study

The researchers developed an e-clearance system that automates and centralizes the clearance system. The system was designed to facilitate the fast processing of student clearance, allow users to access the system online, and save the cost that paper clearance entails. [18]

The study tells about paper-based forms that need to have a solid monitoring system to ensure that forms are stable and reliable. It is quite obvious that papers are a big part of business, office, and especially in schools. But somehow, once you keep those paper-based forms might be time-consuming. Just like the study " Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College" it helps the locale to go paperless to save time and easy access to records, especially student violations.

The study describes the use and predicted consequences of the Secured CCSPC Web-Based Student Clearance System. For students and designated offices, this system includes two-factor authentication. A Secure Socket Layer (SSL) for data transit, as well as a software firewall and anti-SQL Injection attack, were proposed and implemented in the clearance system. [19]

This research is related to the study because it encrypts data information the same way we do in the system. This is a good approach when it comes to the clearance system, to prevent unauthorized persons to steal important data.

### Table 1. Literature Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| **References** | **Description** | **Strength** | **Weakness** |
| Cadiz et al. (2017) [17] | The researchers developed an e-clearance system that automates and centralizes the clearance system. The system was designed to facilitate the fast processing of student clearance, allow users to access the system online, and save the cost that paper clearance entails. | The paperless clearance system eliminates those disadvantages of the  manual system. Hence, e-clearance offers academic constituent convenience in the processing of  student clearance. | It is not mobile responsive. Users can access it via mobile, but the user interface is difficult to understand.  It does not consist of violation management.  so students who violate can easily and quickly escape.  Since it lacks Basic Encryption, it's possible that data submissions could be manipulated by an anonymous user. |
| Daud et al. (2022) [18] | The study describes the Secured CCSPC Web-Based Student Clearance System's used and predicted effects. This system includes two-factor authentication for students and designated offices. In the clearance system, a Secure Socket Layer (SSL) for data transit, as well as a software firewall and anti-SQL Injection attack, were offered and implemented. | No need for account creation as it relies on the CCSPC Portal to get information by using a Web API | It does not include violation management, so students can easily bypass violations.  It is not responsive to mobile devices. Mobile users can access it, although the user experience is confusing. |
| Jonathan et al. (2019) [10] | This study proposes a system that overcomes the issues with manual processing while improving on the identified automated ones. The study adopts a case study approach of a complete manual system for leading institutions of learning in Southwest Nigeria, with the existing procedure being carried out. The new system will reduce the amount of time and effort wasted on students’ clearance as well as reduce costs incurred on paper by the institution. | The system encrypted the entire data. Which prevents hackers from accessing their important files. The only thing the hackers can see is jumbled nonsense (random characters, numbers, and symbols) that is meaningless to them. | It does not consist of violation management with this student who can easily leave violations. |
| Rochmawati et al. (2018) [14] | The researchers developed a system that creates a Laboratory Clearance Form. To create a license from this application, the student needs to request the license by accessing this web application and filling out the request form with their registration number. If it is successful, each subhead and head laboratory will receive notification from the system about students who request the license. If all of the subhead laboratories confirm, the head of the laboratory will receive a notification. After the head of the laboratory confirms, the student then can download the Laboratory Clearance Form. | It has a unique way of validating the users, by using QR Code technology. | The department does not have the ability to approve the student and cannot track their clearance progress.  It lacks Basic Encryption, which means that the information submitted can be corrupted by an anonymous user. |
| Albert et al. (2019) [15] | The Researchers' main objective was to develop a reliable, effective, efficient, and transparent Online Clearance System to eliminate the challenges stated. This system enables final-year students to monitor the progress/status of their clearance forms online as long as the technologies they are using can access the internet. | It covers a lot of functions, such as the student module and administrator module. The student module can monitor their clearance progress. And in the administrator module, they can monitor the overall student clearance progress with a bar chart | It also lacks Basic Encryption, which means that data submitted could be manipulated by someone with an anonymous user.  It is not responsive on mobile. Mobile users have access to it, but it is still challenging to understand the user interface.  The program does not consist of violation management with this student who could also easily avoid violations. |
| Tunde at el. (2021) [16] | The purpose of system implementation is  to create a new system or modify an existing  system in compliance with stakeholders’ requirements. The student applies for clearance, an SMS notification is sent to the admin personnel in charge of clearing students in the department. | The system sends a notification to students who might have issues in the department. The system automatically fetches the student’s number and sends an SMS notification. The same format applies to other units | The system does not have student information management. In case the student that applies for clearance made mistake, the system cannot revise it.  This does not consist of violation management from this student who could really easily ignore violations.  It does not work on mobile devices. Mobile phone users can use it. But even so, the user interface is difficult to comprehend.  Since it lacks Basic Encryption, it might be possible for anonymous users to manipulate provided data. |

1. Student Information Management (e.g., add, delete, edit, save, search, and update database).
2. Log In System
3. User Admin Module
4. Web Based
5. Mobile Responsive
6. Digital Signature

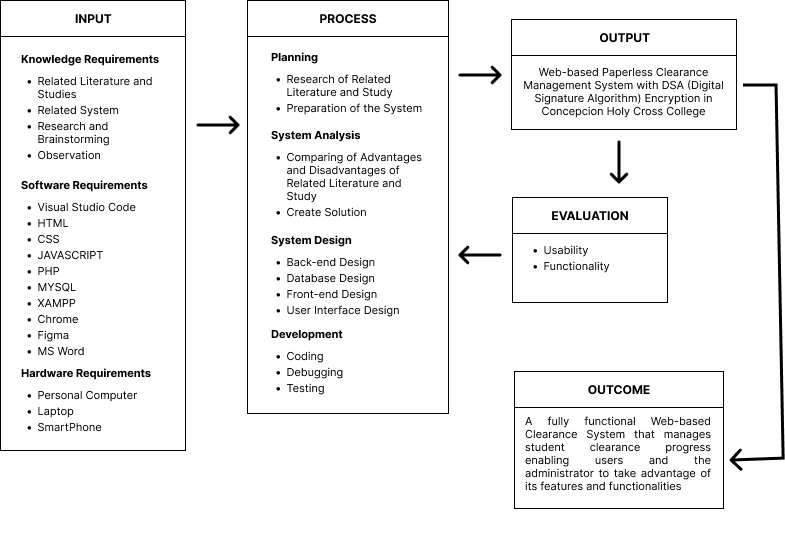
### Table 2. Functionality and Feature Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Software | 1 | 2 | 3 | 4 | 5 | 6 |
| Moving Towards Global Technological Advancement: Basis for the E-Clearance  Program Development | ✔ | ✔ | ✔ | ✔ | ✖ | ✖ |
| Secured Cotabato City State Polytechnic College Web-Based Student Clearance System | ✔ | ✖ | ✔ | ✔ | ✖ | ✖ |
| Development of Online Clearance System for an Educational Institution | ✔ | ✔ | ✔ | ✔ | ✔ | ✖ |
| A Responsive Web-Based QR Code for Laboratory Clearance Form | ✔ | ✔ | ✔ | ✔ | ✔ | ✖ |
| ONLINE CLEARANCE SYSTEM | ✔ | ✔ | ✔ | ✔ | ✖ | ✖ |
| Design and Implementation of a Web-Based Sms-Notification Clearance System: A Case Study of Federal Polytechnic,Ile – Oluji, Ondo State. | ✖ | ✔ | ✔ | ✔ | ✖ | ✖ |

*Synthesis*

In table 2, most of the studies that the researchers found about online clearance systems have some common features. They prominently display a basic function, but they differ in the more detailed feature they offer. The analysis of other systems, such as the clearance system, revealed that they lack digital signatures. The Researchers decided to design and develop a Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College.

## Conceptual Framework



**Figure 1. Conceptual Framework**

This conceptual framework demonstrates the researchers’ process for coming up with the following idea and developing a solution to the issue. There are three components to the input. Knowledge Requirements are where we obtain the underlying problems we are now attempting to solve, together with how we came up with the solution plan. Software requirements and hardware requirements are the tools and devices that we are going to use with regard to achieving our desired system. The overall process is getting the idea and putting it into action in order to solve the problem. Putting it into action means implementing it in the system from designing it up to development. To put it simply, the process is the preparation of the system. Output is the exact expected system that has been designed. And the outcome will be the benefits and main features of the system.

* 1. Algorithm Matrix

### Table 3. Algorithm Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm and Reference** | **Description** | **Strength** | **Weakness** |
| DSA (Digital Signature Algorithm) [20] | DSA, or Digital Signature Algorithm, is a cryptographic algorithm that is used to generate digital signatures. Digital signatures are a type of security measure that is used to authenticate the identity of the sender of a digital message or document. | It is a digital signature scheme that is based on the mathematical concept of the discrete logarithm. This allows it to provide a high level of security, as it is difficult for an attacker to forge a digital signature without the corresponding private key.  Another strength of DSA is that it is relatively fast and efficient, compared to other digital signature schemes | Limited to signature generation and not suitable for other tasks  Not as widely used and studied as RSA and ECC |
| RSA (Rivest-Shamir-Adleman) [21] | RSA is an algorithm for public-key cryptography. It is one of the first and most widely used algorithms for secure data transmission. RSA is named after its inventors, Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, who created it in 1977. RSA uses a combination of a public key and a private key to encrypt and decrypt messages. The public key is used to encrypt the message, while the private key is used to decrypt it. This allows people to securely communicate with each other even if they are not in the same location. RSA is commonly used in electronic commerce, including in the security of online credit card transactions. | It is a widely used and well-studied algorithm. This means that it has been thoroughly tested and is generally considered to be secure. Additionally, RSA is relatively fast and efficient, making it well-suited for use in applications that require secure communication over the internet or other networks. | It is relatively slow compared to other algorithms, such as ECC. This can make it less suitable for applications that require high performance or low latency.  Another, it is vulnerable to attack if the private key is compromised. This can happen if the private key is stolen, or if it is generated using a weak random number generator. In such cases, an attacker could use the private key to decrypt messages that were encrypted using the corresponding public key |
| ECC (Elliptic-curve cryptography) [22] | Elliptic-curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography to provide equivalent security. | The main strength of ECC is its efficiency. ECC can provide the same level of security as other, more established algorithms, but with shorter keys. This means that it requires less computational power to implement, which makes it well-suited for use in applications that have limited resources. | Requires more computational power to implement  Another potential weakness of ECC is that it is vulnerable to a type of attack known as the "random curve attack". This attack involves an attacker using a carefully chosen random curve to trick the system into accepting a forged signature as valid. |
| Twofish [23] | Twofish is the successor to Blowfish, and, like its predecessor, uses symmetric encryption, so only one 256-bit key is necessary. This technique is one of the fastest encryption algorithms and is ideal for both hardware and software environments. | It provides a high level of security, as it is extremely difficult for an attacker to determine the key using brute-force methods. Additionally, Twofish has been extensively analyzed and tested by cryptographers and has not been found to have any significant weaknesses. It is also relatively fast and efficient, making it well-suited for use in applications that require secure communication or data storage. | One potential weakness of Twofish is that it is vulnerable to a known-plaintext attack, in which an attacker has access to both the encrypted message and the corresponding plaintext message. In such cases, the attacker can use this information to determine the key and decrypt the message. |

*Synthesis*

It is generally considered that Digital Signature Algorithm (DSA) is a more secure choice for electronic signatures compared to other algorithms such as RSA, ECC, and Twofish. This is because DSA is a "pure" digital signature algorithm that was specifically designed for this purpose. This makes DSA more efficient and effective than algorithms that were not originally designed for electronic signatures. And DSA has been extensively tested and reviewed by the cryptography community and has been found to be a secure and reliable algorithm for digital signatures. These factors make DSA a good choice for creating secure and reliable digital signatures.

# TECHNICAL BACKGROUND

## Network Architecture

*Synthesis*

In order for the user to access the system, users can use any device that has a browser which was mentioned in the hardware requirements, but the most recommended device is a smartphone since it usually has a QR Code scanner. Once the link has been accessed through the browser, the browser then sends an HTTP request message to the server, asking it to send a copy of the website to the client. Then after the client inputs data, all other data sent between the client and the server is sent across your internet connection using TCP/IP.

## Software Development Requirement

**Table 3. Software Requirements**

|  |  |
| --- | --- |
| **SOFTWARE** | **DESCRIPTION** |
| **Windows 10** | Operating System on the Developer's Computer or Laptop |
| **Visual Studio Code** | It is a text or code editor that will be used for coding and modifying the system's programming codes. |
| **HTML** | The code that will be used to organize and display a web page's content |
| **CSS** | It will be used to design and layout web pages. |
| **JAVASCRIPT** | Will be used to construct highly responsive interfaces, in order to enhance the user experience and provide dynamic functionality |
| **PHP** | A programming language that will be used for the system back-end. |
| **SQL** | Is a query language that is required in order for MySQL to work. |
| **MYSQL** | To store and retrieve information from the database |
| **XAMPP** | Is a local host or server that will be used to test the website on computers and laptops before it is deployed to the main server. |
| **CHROME** | A browser to test and access the website |
| **FIGMA** | To design and layout the desired user-friendly interface (without code) |
| **MS Word** | Software that will be used to document the study |
| **DSA (Digital Signature Algorithm)** | The encryption algorithm that will be used in the electronic signature of this study. |

Visual Studio Code will be used to create and debug the web-based application. The front-end stacks will be HTML, CSS, and JavaScript. PHP will be utilized for the backend. The database for the program will be provided by the researcher using MySQL databases.

## Hardware Development

**Table 3. Software Requirements**

|  |  |
| --- | --- |
| **HARDWARE** | **SPECIFICATION** |
| **Personal Computer** | Operating System: Windows 10  Processor: AMD Ryzen 2600  GPU: Nvidia GT710  RAM: 8.00gb Memory |
| **Laptop** | Operating System: Windows 10  Processor: Intel Core i3-2370M  RAM: 4.00gb Memory |
| **Smart Phone** | Operating System: Android  Processor: Octa-core (2.0GHz, 1.8GHz)  RAM: 4 GB  Storage: 64 GB  Display: 6.53 inches |

This section demonstrates the hardware and devices that will be used to create the Web-based Paperless Clearance Management System with DSA (Digital Signature Algorithm) Encryption in Concepcion Holy Cross College. These are suitable computer hardware for running the application, and this type of specification will also be compatible with application testing. The application is compatible with Windows 7 and later versions of the operating system.

## Sources of Data

The data was acquired by the researchers through the reading of research, literature, and studies about the clearance system, violation management, and QR codes. The researchers acquired ideas and knowledge through literature and studies to help with the creation of new features and functionalities for the Clearance System. Additionally, the researchers would use these references to improve the system's implementation and design.

# REFERENCES

[1] Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128.

[2] Dr. Radhika K., “Use of Technology in School Governance and Administration”, 2019

[3] Umar F, “Online Clearance System”, 2021

[4] Isra J., Nov 20, 2022. [Online] “Clearance Procedure”. KOC University. Available: <https://registrar.ku.edu.tr/en/sss/what-is-clearance-procedure-why-and-how-to-do-it/?fbclid=IwAR15R4e4oJj-UaByCJrq5vRSEjWJJZk2ePaF-DHLO17xI0Hhyk-F37uKyBI>

[5] M. Hart."Digital Signature Algorithm (DSA) in Cryptography: How It Works and Advantages." simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm#what\_is\_the\_dsa\_algorithm (accessed Oct. 27, 2022).

[6] B. Jena."What's the Difference Between Electronic Signatures and Digital Signatures? Everything You Need to Know" globalsign.com. https://www.globalsign.com/en/blog/electronic-signatures-vs-digital-signatures (accessed May 10, 2022).

[7] U. Mitra."Digital Signature Algorithms (DSA) in Cryptography." tutorialspoint.com. https://www.tutorialspoint.com/digital-signature-algorithms-dsa-in-cryptography (accessed Dec. 07, 2022).

[8] Albert, M. B. G. (2019). ONLINE CLEARANCE SYSTEM (Doctoral dissertation, DEPARTMENT OF INFORMATION TECHNOLOGY SCHOOL OF COMPUTING AND INFORMATICS TECHNOLOGY A Report Submitted to the School of Computing and Informatics Technology for the Study Leading to a Project in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Information Technology of Makerere University. Supervisor Mr. Bitwire George Albert Department of Information Technology School of Computing and Informatics Technology, Makerere University).

[9] Walton, J., & Thompson, M. (2019). Improving the student clearance process through technology: A case study. Journal of Higher Education Management, 35(2), 39-52.

[10] Flores, M. K. (2018). The impact of student clearance on persistence and graduation at a public metropolitan university. Journal of Student Affairs Research and Practice, 53(2), 110-119.

[11] Jonathan, O., Misra, S., Makinde, F., Damasevicius, R., Maskeliunas, R., & Leon, M. (2019, November). Development of Online Clearance System for an Educational Institution. In International Conference on Applied Informatics (pp. 327-339). Springer, Cham.

[12] Roberson, A. J. (2019). Predictors of Zero Tolerance Policy Violations Among High School and Middle School Students.

[13] Caroro, R. A., & Hernandez, A. A. (2018). Migrating office processes to automation: An evaluation on green IT practices in a university in the Philippines. In 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM) (pp. 1-9). IEEE.

[14] Rimando, M. K. V., & Corpuz, R. R. (2022). A Real Time Tracking System for School Forms Using QR Codes with Watermarking Algorithm. Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN) ISSN: 2799-1172, 2(03), 24-33.

[15] Rochmawati, N., Anistyasari, Y., Suyatno, D. F., & Kurniawan, I. F. (2018, November). A Responsive Web-Based QR Code for Laboratory Clearance Form. In Journal of Physics: Conference Series (Vol. 1108, No. 1, p. 012048). IOP Publishing.

[16] Albert, M. B. G. (2019). ONLINE CLEARANCE SYSTEM (Doctoral dissertation, DEPARTMENT OF INFORMATION TECHNOLOGY SCHOOL OF COMPUTING AND INFORMATICS TECHNOLOGY A Report Submitted to the School of Computing and Informatics Technology for the Study Leading to a Project in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Information Technology of Makerere University. Supervisor Mr. Bitwire George Albert Department of Information Technology School of Computing and Informatics Technology, Makerere University).

[17] Tunde, F. J., AjinajaMichealOlalekan, O., & Victor, J. O. Design and Implementation of a Web-Based Sms-Notification Clearance System: A Case Study of Federal Polytechnic, Ile–Oluji, Ondo State.

[18] Cadiz III, L., Bondoc, C. N., & Estroga, J. (2017). Moving Towards Global Technological Advancement: Basis for the E-Clearance Program Development. International Journal of Computing Academic Research (IJCAR), 6(6), 171-179.

[19] Daud, G. S., & Maguid, M. A. (2022). Secured Cotabato City State Polytechnic College Web-Based Student Clearance System. Randwick International of Social Science Journal, 3(1), 61-66.

[20] Al-Absi, M. A., Abdullaev, A., Al-Absi, A. A., Sain, M., & Lee, H. J. (2020). Cryptography Survey of DSS and DSA. In Advances in Materials and Manufacturing Engineering (pp. 661-669). Springer, Singapore.

[21] Mahto, D., & Yadav, D. K. (2018). Performance Analysis of RSA and Elliptic Curve Cryptography. Int. J. Netw. Secur., 20(4), 625-635.

[22] Kim, J., Choo, H., & Lee, D. (2019). A Comparative Analysis on ECC (Elliptic Curve Cryptography) Operation Algorit hm for Data Protection in Video security System. Convergence Security Journal, 19(5), 37-45.

[23] Ghosh, A. (2020). Comparison of encryption algorithms: AES, Blowfish and Twofish for security of wireless networks. International Research Journal of Engineering Technology, 7, 4656-4658.