**IMPLEMENTING SECURE HASH ALGORITHM-256 (SHA-256) FOR**

**A QR IDENTIFICATION SYSTEM WITH SMS NOTIFICATION**

Undergraduate Thesis

Submitted to the Faculty of the

College of Engineering and Information Technology

Cavite State University

Indang, Cavite

In Partial Fulfillment

of the requirements for the degree

Bachelor of Science in Computer Science

**JULIUS N. ABUCEJO**

**KEVIN ALLI AQUINO**

**PATRICK B. BONGALOS**

**LAWRENCE NEIL C. LIMBOC**

January 2023

**IMPLEMENTING SECURE HASH ALGORITHM-256 (SHA-256) FOR**

**A QR IDENTIFICATION SYSTEM WITH SMS NOTIFICATION**

**Julius N. Abucejo**

**Kevin Alli Aquino**

**Patrick B. Bongalos**

**Lawrence Neil C. Limboc**

|  |
| --- |
| An undergraduate thesis proposal submitted to the faculty of the Department of Information Technology. College of Engineering and Information Technology, Cavite State University, Indang Cavite in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science with Contribution No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Prepared under the supervision of Ms. Ria Clarisse M. Sy. |

**INTRODUCTION**

**Project Context**

The system for identification in most universities and campuses of manual checking of identification cards is prone to fault and less secure. Incidents of extreme violence in schools are rare, yet the horrific nature of attacks and abductions in what should be safe environments draws immediate and intense reactions from students, parents, the public, politicians, and the press. According to Mostafavi (2020), one-third of parents may not send their children to school because of safety concerns. The primary reason for this is the safety concern for the transmission of COVID-19.

There are several automated attendance systems, including biometric and radio frequency identification (RFID) technologies. However, the particular system that is mentioned needs a piece of equipment that is neither inexpensive nor low maintenance. The price range for a biometric system is between 7,500 and 67,500 pesos (Office Warehouse, n.d.). The price range for RFID scanners is between 2,600 and 78,00 pesos (BigGo Philippines, n.d.). On the other hand, the QR code is an efficient and secure alternative for these devices available on the market. The QR code is a type of barcode that stores information as a series of pixels in a square-shaped grid. It is read in two directions: top to bottom and right to left. This allows it to store significantly more data compared to standard barcodes that can only be read in one direction, from top to bottom.

As easily accessible information comes in handy with the use of QR codes, it is also prone to exposing sensitive information such as birthdays, emails, addresses, and contact numbers. With 5 million people claiming to have been victims of identity theft, a growing number of Filipinos are suspicious of frauds and scams as a result of the rise in digital banking within the country. Many student identity cards include volatile information that is simple to obtain. Most universities unintentionally disclose this information to the public, resulting in cyber threats.

To avoid such, hashing the QR codes make the data more private and secure. The hashing algorithm is a much more secure way of encrypting data. It consists of numeric and string combinations output with a fixed length that represents the original data. Using the algorithm will prevent the disclosure of confidential information and prevent hacking.

One of the most secure hashing algorithms available is SHA-256. The United States government mandates that its agencies use SHA-256 to secure specific sensitive data. In this regard, the proponents aim to develop a QR identification system implementing SHA-256 with SMS alert notification to prevent the disclosure of sensitive information and assist security personnel of a school, college, or university by providing additional security measures.

**Purpose and Description**

The QR Identification System aims to address issues in security and efficient identification processes. Automating the identification at the entrances of a school, college, or university can help lessen, if not completely prevent intruders and outsiders from entering the premises and also make the process faster and more convenient.

The system was of great significance in educational institutions, specifically at Cavite State University, in providing additional and faster security services to the people. The system will benefit both the educational institutions and the people in terms of their safety. In addition, the success of the study will be beneficial in the following:

**Students.** By automating the process of identification through the generation of unique QR codes, it will take much less of their time to undergo the process compared to the manual and traditional ways. This will also help them feel safer about their personal data knowing that it undergoes the process of hashing, and at the same time provide them safer campus environment knowing that anyone they meet must go through identification procedures. The system will also serve as an assurance of their safety by sending remote messages to their immediate contacts and relatives during the identification process.

**Parents.** Through SMS notifications provided by the system, it gives parents a way to monitor the status of their children. It will ease their concerns to know that students arrived safely and showed up to class by allowing them to trace the precise time and date that their children enter and exit the school. Additionally, the method will allay concerns of parents about their children not attending their classes.

**Educational Institutions.** The system will serve as a platform and medium for them to be able to manage the records of their students, particularly the data about their attendance. This will give them meaningful insights about different factors including the quality of education an academic institution provides.

**Security Personnel.** By implementing the system and automating the process of identification through the scanning of QR Codes that is significantly faster, they will be able to cut down on the time and workload associated with manual operations and the screening students that enters the facility.

**Future Researchers.** The study will aid future academics in determining the benefits and drawbacks of putting the system in place in terms of security. The system will also be used by them as a foundation and for a related investigation.

**Objectives of the Study**

Generally, the study aims to develop a QR identification system with SMS notification that implements SHA-256, which provides an additional layer of safeguarding for educational institutions. Specifically, it aims to:

1. Create an account management module for authenticating the users;
2. Build a record management module for managing students and attendance records;
3. Develop a notification module for message alerts notification and system notifications;
4. Create a QR module for generation of QR Codes and automation of attendance and identification; and
5. Implement a secure hashing algorithm-256 (SHA-256) to the student information.
6. Assess the proposed system through software evaluation based on ISO standards, unit testing, integration testing, and system testing

**Scope and Limitations of the Study**

The proposed system is a web application that will use a secure hashing algorithm of 256 bits (SHA-256) and will require the integration of Logicowl OJ-MP6200 barcode and QR Code scanner. It will be comparable to an automated attendance system. The system will be written in React JS, and its backend will be handled by an Express server for the MySQL database. The system will have several users and participants, namely: the students who have access to the system through the QR scanner attached to the system, the parents which primarily acts as the recipient of SMS notifications and the system administrator who has full control of the main functions of the system. This system will consist of four modules, namely: account management, record management, notification, and QR modules.

**Account Management Module.** This feature determines whether unauthorized users are accessing the key objectives of the system, this module acts as the primary security of the system. It requires admin users to enter the username and password of their accounts and the system will evaluate these credentials for matched accounts in the database to gain access to the system features. Upon successful authentication, the user will be directed to the dashboard of the system. Only the administrator can manage and access the system features by logging in with their authorized credentials.

**Record Management Module.** The management of both the records of students and their attendance records is under the purview of this feature. The authorized user can add, alter, view, and delete student and attendance records in this module, among other changes to the records within the system. Among the records that will be gathered from students include but are not limited to student number, name, address, contact number of both the student and their parents, course, and year level. This module is also where the implementation of Secure Hashing Algorithm-256 (SHA-256) happens. Before student information are stored in a database, certain unique details undergo the hashing process which will serve as their unique key. This unique key is later used in the QR module for the generation of QR Codes. For the proper recording of attendance, it is suggested that the system will be implemented and placed at both the entrances and exits of the institution. The add capability of this module is incorporated with the QR module, for each QR scan it accomplishes, it invokes the addition of a student attendance record automatically.

**Notification Module.** This feature is responsible for handling system notifications displaying information about the result of a system process like “Success”, “Network Error”, “Invalid Credentials”, “Invalid Requests” and “No records found” notifications. This module also handles sending message notifications to the immediate contacts of students which will be triggered by the QR module upon the process of scanning. Sending of SMS alerts will be implemented using an SMS API. However, sending SMS notifications is limited to 10 messages per day for each student.

**QR Module.** This feature is responsible for the generation and reading of the QR codes of students. Unique QR Codes are generated for each student based on the hash value of student information that undergoes the SHA-256 process, which will serve as their identification. On the other hand, scanning of the generated QR Codes will be done through the use of QR scanner, an external device that can be plugged into the computer. During the process, the system will decrypt the data stored in QR Codes and will find the matched record in the database. On successful operations, this will invoke the system to display information of students on the computer screen. Additionally, this module is in charge of invoking the SMS module to deliver notifications to parents and generating attendance records for the fetched students data during the process of QR scanning.

The study also specifies limitations and the system requirements for effective use. The system is human-operated and thus needs an operator. The system does not always keep track of SMS notifications that are unsuccessfully delivered due to difficulties mostly with internet connection. Issues and problems that are not related to attendance tracking, monitoring, SMS notifications, and QR identification systems will not be dealt with in this study.

This proposed system can be used in any academic institution. However, for the sole purpose of testing the system, the proponents will involve the security personnel and students of Cavite State University – Don Severino delas Alas Campus.

**Definition of Terms**

The following are the technical definitions of terms used within the study:

**Algorithm** isa detailed process that outlines a series of steps that must be followed in a certain order in order to obtain the desired outcome.

**Application Programming Interface (API)** are pieces of code that allow the software to communicate by sending requests and receiving responses

**Attendance Management** is the processuse to record, track, and monitor the attendance history of students that enter the campus.

**Cyber security** is the technique of preventing harmful assaults on computers, servers, mobile devices, electronic systems, networks, and data.

**Database** is a softwareuse to store information of students, QR Codes data, hash values, and credentials of accounts within the system in the form of tables, rows and columns

**Hacking** is the process offinding and then using a computer system or network vulnerabilities to obtain unauthorized access to data of someone or some organization.

**Hash Values**  arethe output data or result of performing a hashing process

**Hashing** is the process ofchanging one value into another based on a given key or string of characters. A shorter, fixed-length value or key that serves as a representation of the original string is normally used to decrypt the processed data

**Microchip** is a set of electronic circuits on a small, flat piece of silicon.

**Middleware** aresoftwares that act as a bridge between an operating system or database and applications, especially on a network.

**Phishing** is a social engineering approach that is frequently used to steal user information, such as login information.

**QR Code** is short term for quick response, QR codes are scannable bar codes made up of white and black squares that store data. The system generates QR Codes that students can use to identify themselves.

**QR Scanner** is a device use to read QR Codes. The system can read and validate the identity of an individual by scanning the QR codes attached to their IDs.

**Routing** isthe process of selecting a path for traffic in a network or between or across multiple networks.

**Secure Hashing Algorithm-256 (SHA-256)** is a cryptographic hash algorithm uses by the system that takes raw data as an input and produces an irreversible and unique output value (hash) that is 256 bits

**SMS Notification** are text messages sent to parents or contacts of students upon the process of successful scanning notifying them about the status of their children.

**Uniform Resource Locator (URL)** is a reference to a resource on the Internet.

**REVIEW OF RELATED LITERATURE**

This chapter contains related literature and studies that address different concepts and ideas that are relevant to the study. The researchers used the information gathered from this related literature and studies to familiarize themselves with the subject and use it as a guide in developing their project.

**Technical Background**

**ReactJS.** According to Deshpande (2022), ReactJS is a UI development library based on JavaScript. It was founded in 2011 by Jordan Walke, a software engineer at Facebook, and first appeared in May 2013. React is influenced by tools like XHP, a simple HTML component framework for PHP, and is now one of the most commonly used front-end libraries for web development. Among the reasons for its popularity include easier creation of dynamic applications, improved performance, reusable components, unidirectional data flow, easy-to-learn, multi-platform development, and dedicated tools for debugging. React utilizes the JavaScript structure called virtual DOM, a lightweight and faster version of real DOM which results in faster program performance.

The proponents have found that React will be the most suitable tool for the development of the system by allowing the developers to break down system modules into several React components. This makes the development divided into multiple smaller tasks easier to achieve compare to one but more complex system.

**ExpressJS.** A Node JS web application framework ExpressJS offers a variety of features for creating both web and mobile applications according to Sharma (2022). It can be use to create single-page, multi-page and hybrid applications. Node JS, on the other hand, is a fast JavaScript runtime environment use to develop server-side applications that were built on top of V8 JavaScript engine of Google that enables it to run and execute JavaScript code outside of web browsers. Express JS is designed to create web APIs, perform and handle web serving and requests, and makes Node JS easier to use. Among the really helpful features of Express includes routing, middleware, and dynamic rendering.

The researchers decided to use Express due to its flexibility, ability to be integrated into different type of applications, and Node JS modules that will be essential to the development of the system like a **crypto** module that provides cryptographic functions mainly use to perform different hashing algorithms and **express-session** module use to manage and create session middleware. It is also a great choice since the system is built mostly base on JavaScript for both front-end and back-end components, it lessens the need to study multiple and complex programming languages.

**MySQL.** Based on Richard B. (2022), MySQL is an open-source relational database management system (RDBMS) that uses a client-server architecture. A relational database management system (RDBMS) is software or service to build and manage databases. What makes MySQL popular are its characteristics such as flexibility-developers can modify source codes to meet their needs, and high performance - it is supported by a variety of cluster servers and thus can assist developers fast, secure - password encryption and host-based verification are both supported by MySQL, and industry-standard - since industries have been using MySQL for years, there are many opportunities for skilled developers.

**Logicowl OJ-MP6200.** It is an external bar code and QR code scanner. This scanner features CCD optical image scanning technology that has been independently researched and developed, capable of identifying screen code as well as incomplete and fuzzy code. Easy installation and USB cable of 2 meters with scanner dimensions of 78 x 75 x 141 mm. It automatically scans QR Codes within the non-blind area recognition without the need to aim and has an auto power off feature when not in use.

**Related Literature**

**Attendance Management System.** According to GreatSchool (2022), the first steps in creating successful schools is encouraging students and making sure they consistently attend school. Furthermore, students who consistently attend school have a higher chance of academic success. In a 2008 study by the Rodel Community Scholars at Arizona State University, dropout trends were associated with poor attendance starting in kindergarten and followed by kids from kindergarten through high school. As such the traditional tracking of attendance is inefficient and costs the loss of classroom time.

In accordance to SEAtS Software (2022), recent years show that there have been significant changes in the way that student attendance is managed and tracked in schools. As more classes have moved to a hybrid or digital model, the methods of tracking attendance have also evolved. Previously, attendance was often tracked using paper-based systems, which were prone to errors and required a lot of manual data entry. This was not only time-consuming, but also led to an increase in mistakes and inefficiencies. Additionally, these systems often produced reports and alerts that were too late to be useful in improving student retention or outcomes. As a result, there has been a shift towards more modern and efficient methods of attendance tracking that can help to improve student success.

**Importance of Attendance System.** In line with Classter (2019), regular attendance benefits the academic performance of the students as well as their personal and emotional growth, enhancing their sense of belonging to their classmates and communities. Managing school attendance with a cloud-based, digital system can make a difference for educational institutions in the modern day when everything takes place on the internet. Having such a system enables educators to have a clear picture of student and classroom attendance rates wherever they are. Additionally, as the technology automatically logs the presence of the students by scanning radio frequency identification (RFID) cards or even smartphones, attendance tracking can become more effective. By doing this, teachers may stop doing this tedious, repetitive task and spend more time doing what really matters: instructing students.

Moreover, parents will benefit as well. By employing an attendance management system, it is possible to keep track of the precise arrival time of students and immediately notify parents when a student is absent. Furthermore, teachers can track student attendance in their classes, note absence reasons, and send SMS and email notifications to parents about absences of their children. If done manually, the process of tracking attendance would be chaotic. In order to keep track of the daily attendance of the students at school, administrators, teachers, and parents can use digital management software to easily access the system and monitor the attendance records.

As to why management of student attendance is important according to the National Center for Education Statistics (2009), missed school days can negatively impact the learning of students. In recent years, there has been a focus on the relationship between student attendance and academic performance, leading to a demand for consistent attendance data reporting from educational organizations. This allows for comparisons to be made across different schools and districts. A report from the United Kingdom Department for Education in 2011 found that a significant number of students in primary, secondary, and special schools in the UK were missing a significant portion of their lessons. Over 1.1 million students missed 20% of their lessons in the year covered by the report, while over 430,000 students missed 15% or more of their lessons each year. These high absentee rates can have negative impacts on the future outcomes of students. According to data from the DfE, students who frequently miss school tend to perform poorly on assessments and exams, leading to an increased risk of leaving school with few or no qualifications. These students may also face increased risks of unemployment, homelessness, and mental health issues, which can be related to criminal behavior.

**Drawbacks of Manual Attendance Management Systems.** While manual attendance management system comes with its advantages. It also comes with some disadvantages and drawbacks. According to Khan (2022), manual and traditional attendance systems can be used in manipulation of data or the act of altering data in order to achieve a desired outcome. This can occur when data is manually recorded and entered by individuals. One possible reason for this is to maintain profitability,this type of manipulation can result in a situation known as "time theft". Manually tracking of attendance can also lead to an increased risk of human error, as people may make mistakes when recording their attendance This can have serious consequences for compliance, pay, and other important factors. Manual attendance reporting can take a lot of time and have a bad effect on how productive and efficient people are. It can entail handling spreadsheets and fixing time entry errors, both of which can consume a lot of time. Lastly, since more modern technology is available that can increase accuracy and streamline the process, it is generally accepted that using manual procedures for recording attendance is ineffective and out-of-date. These out-of-date techniques can significantly affect business operations and can be expensive to maintain.

**Automated Attendance Management System.** As described by BasuMallick (2022), an attendance management system is any tool that aids in keeping track of time spent at work by the employee. The interesting fact that this does not have have to be a digital tool; some of the traditional types of attendance tracking include paper registers, time clocks, and Excel-based spreadsheets. An automated attendance management system is a software tool that is used to record and track attendance of students in a classroom setting. It allows teachers to easily and automatically record class attendance and provides insight into overall attendance trends and patterns. The system helps teachers save time by eliminating the need for manual attendance tracking, allowing them to focus on other tasks such as providing quality education to students. Overall, the attendance management system helps to improve the efficiency and accuracy of attendance tracking in a school or educational setting.

There are several benefits to using a student attendance management system in a school or educational setting. According to Kandra (2019) an automated attendance management system can help improve attendance by incentivizing rather than penalizing students. It can also provide valuable data and insights on attendance trends. This can help schools improve attendance and learn more about their students. This system can generate various reports quickly and easily, helping schools efficiently track and manage class attendance. It can also provide parents with updates on attendance of their children. This can be done through monthly or weekly reports, or through a system that allows parents to check the attendance details themselves. Automated attendance management system can also save a significant amount of time for teachers and schools. Automating this process can reduce this time to just one hour, freeing up significant time that can be used to improve student outcomes. It can also eliminate human error in attendance tracking, resulting in accurate and reliable data. This can help with administrative decision-making. Lastly, it can provide a central location for managing various aspects of attendance, including records for students, parents, and teachers, as well as leave records, punctuality records, and admission records.

**Technologies used in Automated Attendance Management Systems.** There are several technologies that are commonly used in automated attendance systems according to Zimyo Marketing Team (2020). Among these technologies are Biometric logins that use matched fingerprint scanning to mark attendance, however they can be bypassed by someone who knows how to do it. RFID (Radio Frequency Identification) tags are installed in personal identification cards and communicate with card readers to mark and automate attendance. However, these tags can be cloned and are expensive to replace. Bluetooth attendance systems use a mobile app and Bluetooth connectivity to mark attendance using unique Media Access Control (MAC) addresses. Barcode scanning uses unique barcodes on employee identification cards to mark attendance, while GPS technology tracks the location of company-issued devices to ensure that an employee is not being dishonest about their location. Facial recognition is a more expensive option that is commonly used for security purposes, but can also be used for attendance tracking.

**Core Features of an Attendance Management System.** Bellana (2021) stated that a top-notch attendance management system, regardless of the hardware utilized must have the following necessary features. Among these features are clock in and clock out tracker that properly documents, record the time, location of entry, and identity or code used to identify the user ID. This will also be beneficial if the system allows for customization to fit the specific needs of the organization. Leave or absence management systems that will update the current records accordingly must be integrated into the attendance management system as well. Comprehensive attendance reports are also important for large organizations, it serves as historical data and reference material. An attendance management system that provides these reports demonstrates its effectiveness and efficiency in handling and processing large amounts of data. And lastly, calendar integration is a key feature of an attendance management system because it allows the system to synchronize with an existing schedule of organzations, making it easier to track attendance. Without this feature, organizations would need to manually input events, which can be time-consuming and negate the benefits of having an automated system.

**Secure Hash Algorithm.** According to Landman et al. ( n.d.), secure hash algorithms (or SHA) are a family of cryptographic operations that aims to protect data. It is a revised version of MD5 used for hashing data and certificates. It applies a hash function, an algorithm made up of bitwise operations, modular additions, and compression functions, to alter the data. These algorithms are one-way functions by design, making it nearly impossible to convert them back to the original data once they have been transformed into the corresponding hash values. The National Institute of Standards and Technology (NIST), the standard body of the government of the United States, created Secure Hash Algorithm 1, or SHA-1, in 1993. It accepts input and generates a 160-bit hash value as an output. Cryptographers changed the SHA-1 algorithm to construct SHA-2, which consists of not one but two hash functions called SHA-256 and SHA-512, employing 32- and 64-bit words, respectively. This change was made since SHA-1 vulnerabilities were introduced.

Conforming with Code Signing Store (2022), the secure hash algorithm-256 (SHA-256) is the most secure hashing algorithm .It is substantially more secure than other prevalent hashing algorithms because it employs a 256-bit key. Technology pioneers mostly employ SHA-256 because, unlike some other well-liked hashing algorithms, it has not been "broken" and has no known security flaws. Unlike earlier hashing techniques, even a small change to the source data completely changes the hash result. As regards why much network industry implores the use of the SHA-256 that it takes a lot of computing power in order to decode its message.

**Secure Hash Algorithm-256 (SHA-256) for encryption.** According to Veness (2019), a cryptographic hash, also known as a "digest," is a type of signature for a text or data file. The SHA-256 algorithm generates a nearly unique 256-bit signature, or "hash," for a given text. SHA-256 is a cryptographic hash function that is widely used for data security. It is a successor to SHA-1 and is considered to be one of the strongest hash functions available. A hash function is a mathematical algorithm that takes in data as input and produces a fixed-size output, known as a hash or digest. The output is designed to be unique for each input, so that even small changes to the input data will result in a significantly different output. One of the key benefits of SHA-256 is that it is resistant to collision attacks, which are a type of attack that seeks to find two different inputs that produce the same hash output. This makes it well-suited for use in applications where data integrity is critical, such as digital signatures and file verification. In addition to its security properties, SHA-256 is also relatively easy to implement and has a relatively low computational cost. It is defined in the NIST standard FIPS 180-4 and includes a number of test vectors to verify the accuracy of its implementation. Overall, SHA-256 is a widely used and trusted cryptographic hash function that is an important tool in the field of data security.

It is used in some of the most secure networks throughout the world, and no one has yet been able to break it. As stated in Jena (2022) secure hash algorithm-256 (SHA-256) is an enhanced version of the older hashing algorithms SHA-1 and MD5 from 1991, which are extremely vulnerable to planned collisions known as collision attacks, which attempt to generate two distinct inputs with the same hash value. In fact, a simple computer and a program like HashClash can produce collisions in a matter of seconds. When Google announced the first official SHA-1 collision in 2017, this theoretical vulnerability became extremely real. The Chrome team announced that they would gradually phase out using SHA-1.

**QR Codes.** According to Hayes (2021), QR Codes are the following generation of traditional one-dimensional barcodes. The Internal Organization for Standardization (ISO) then approves QR codes in the year 2000. Despite their increased capability, QR codes have become more popular for handling online and digital payments, communicating site URLs, and associating advertisers with marketing techniques than for information exchange.

According to Gregersen (2022), a Quick Response Code or QR Code is a sort of barcode composed of black-and-white printed squares that represent numbers from 0 to 9 and letters from A to Z or non-Latin characters, used to encode data and read by computer systems. Denso Wave, a subsidiary of Toyota Corporation, invented QR Codes in 1994. They were initially employed to track vehicle parts during assembly. The three corners of QR Codes include the finder pattern, a series of black and white squares that defines the orientation of the codes. There are also two more patterns that pertain to the alignment pattern - small square containers for other small squares - and the timing pattern - a row and column of alternating black and white squares that link the bigger squares of finder pattern and determine the locations of the codes.

**QR Codes Benefits.** The greatest advantage of a QR code is its simplicity. The user only needs to launch a QR reader app on their mobile device, the point at the code, and scan to access encoded information such as websites, email addresses, and retail floor maps displaying product locations, among others. (Wara & Dugga, 2016)

Numerous technologies have been developed for the creation of QR codes for papers and report cards. Author Mamtha Shetty is interested in the use of QR codes to hide encrypted private data. The TTJSA technique may decode encrypted data extracted from embedded QR codes using a smartphone running Android, iOS, or any other new-generation mobile operating system. They used three types of algorithms to encrypt and decrypt any data or information contained in the present work information. After examining all three algorithms using a variety of picture formats, they conclude that the Vernam method is more suitable for encrypting images and data. In comparison, the NJJSAA technique has a greater PSNR value and a lower MSE value for encrypting any type of data, hence, it is not often used. (Goyal et. al., 2016).

Data may be recorded more efficiently with QR Scanning than with pen and paper. It is simpler to track information online than to transcribe paper data into an electronic device. As attendance is always recorded in the database, the collection of data for studies requiring attendance information will be simplified. A significant advantage of QR codes is that they limit the number of surfaces that must be touched. In a time when everyone is concerned about germs and viruses, QR codes decrease the necessity for direct touch.

**Implementing QR Scanning with Secure Hash Algorithm.** Encrypting, signing, and controlling access to the information contained in QR codes may all be accomplished through the use of cryptographic techniques. The utilization of data encryption offers both confidentiality and access control for the encoded information. As a result, only authorized users will be able to decode the data that has been encrypted. In addition, digital signatures may accomplish authentication, integrity, and non-repudiation all at the same time. Recent research has also looked into the usage of Visual Secret Sharing methods for QR Codes as a means of providing extra security procedures, such as for online transactions. The selection of an appropriate algorithm, key length, and structure are all topics that are covered in various research; nonetheless, the size of the overhead is the most important aspect of barcode usability (Wahsheh & Luccio, 2020).

The Madiff Net reader program is able to scan and generate QR codes that are secured by a password. The content of these codes is encrypted using a shared key between the generator and the barcode reader. The creator does not disclose the algorithm that was utilized, although the length of the keys is specified as 6 bytes, and the ciphertext is a string represented in base 64. QR Droid Private offers services in the areas of scanning and the production of QR codes. This application allows for the shortening of URLs, the sharing of QR codes, and the encryption of content. The Data Encryption Standard (DES), which has a key size of 56 bits and may be cracked, is the insecure encryption technique that is used by QR Droid Private. It makes use of a keyword structure, in which the ciphertext is encoded using the base 64 numerical system. A security program known as Crypto Message, which enables an encryption service for encrypting text messages within QR codes, is known as Crypto Message. The free version of this program allows for the production of QR codes, but in order to decode them, the user will need to upgrade to the premium version. It utilizes the Cipher Block Chaining (CBC), Electronic Codebook (ECB), Counter (CTR), and Output Feedback (OFB) modes, which are all part of the Advanced Encryption Standard (AES). It encodes ciphertexts as strings in hexadecimal or base 64, depending on the size of the key, which might be 128, 192, or 256 bits. The developers assert that they are able to enable message encryption as well as other security measures. Only authorized users who are in possession of the key (password) are able to decode and access the contents of the QR codes that are password protected, thereby achieving confidentiality and access control. However, encrypting the contents is not the best way to protect people who scan the QR code since even encrypted data may include harmful URLs or offline attacks. This is because encryption does not prevent dangerous URLs from being included in the data. The use of public-key cryptography, which Digital Signature uses to verify the identity of the user, can be beneficial to the security of the user.

These three applications are the best examples of integrating QR codes with secure hash algorithms. It addresses the benefits and drawbacks of each of these technologies.

**SMS Alert Notification.** According to the Oxford Dictionary, SMS stands for Short Message Service and refers to a type of text message that can be sent between mobile phones. It is characterized by having a limited number of characters. Based upon Labs Mobile (n.d), SMS, or Short Message Service, was invented in 1985 by Finnish engineer Matti Makkonen as part of the development of GSM technology. It was not until 1992 that the first SMS message was sent, by Neil Papworth of the Sema Group to Richard Jarvis of Vodafone. Despite its age, SMS has remained popular and is now used in a variety of networks, including 4G and 5G. It has proven to be an enduring communication method that is widely used in modern processes and communication.

In the decade 2010, tens of thousands of SMS messages were sent per second. Those who connect via text messages send and receive 41.5 texts on average per day, according to a Pew Research Center survey. That suggests that millions of text messages are still sent and received every day, despite the rise of social media and Internet-based messaging services. Studies have repeatedly proven that text messages are the preferred method of contact with clients. This is probably due to the reduced length of SMS messages. Customers trust SMS more, according to research by the Cellular Telecommunications Industry Association; 93% of consumers said SMS was a more dependable form of communication. Users experience this because they receive less spam via SMS than spam emails. According to the survey, spam rates for SMS texts are 2.8%, significantly lower than the 53% rates for emails.

According to Salked (2022), the secret to safely managing emergency situations is a swift and effective communication. An emergency text alert system can assist people in rapid communication with as many individuals as possible.It is a software that enables people to simultaneously send mass SMS texts to huge numbers of individuals. The effective flow of information can lead to lowers rates of hazard.

**SMS API Integration.** An SMS API is a tool that allows developers to connect to an SMS gateway and easily send and receive messages. This is useful when a manual SMS system, such as email to SMS or web SMS, becomes inadequate for a business communication needs. According to Mike (2021), the ability to receive real-time reports of the messages sent by the user is a significant benefit of integrating SMS API. Integration of SMS API enables quick and safe message delivery. The flexibility and effectiveness that API offers are exceptional. The system can be integrated with other systems in the network of the user. In this manner, the user is not required to access this system in order to send SMSes.

**Related Studies**

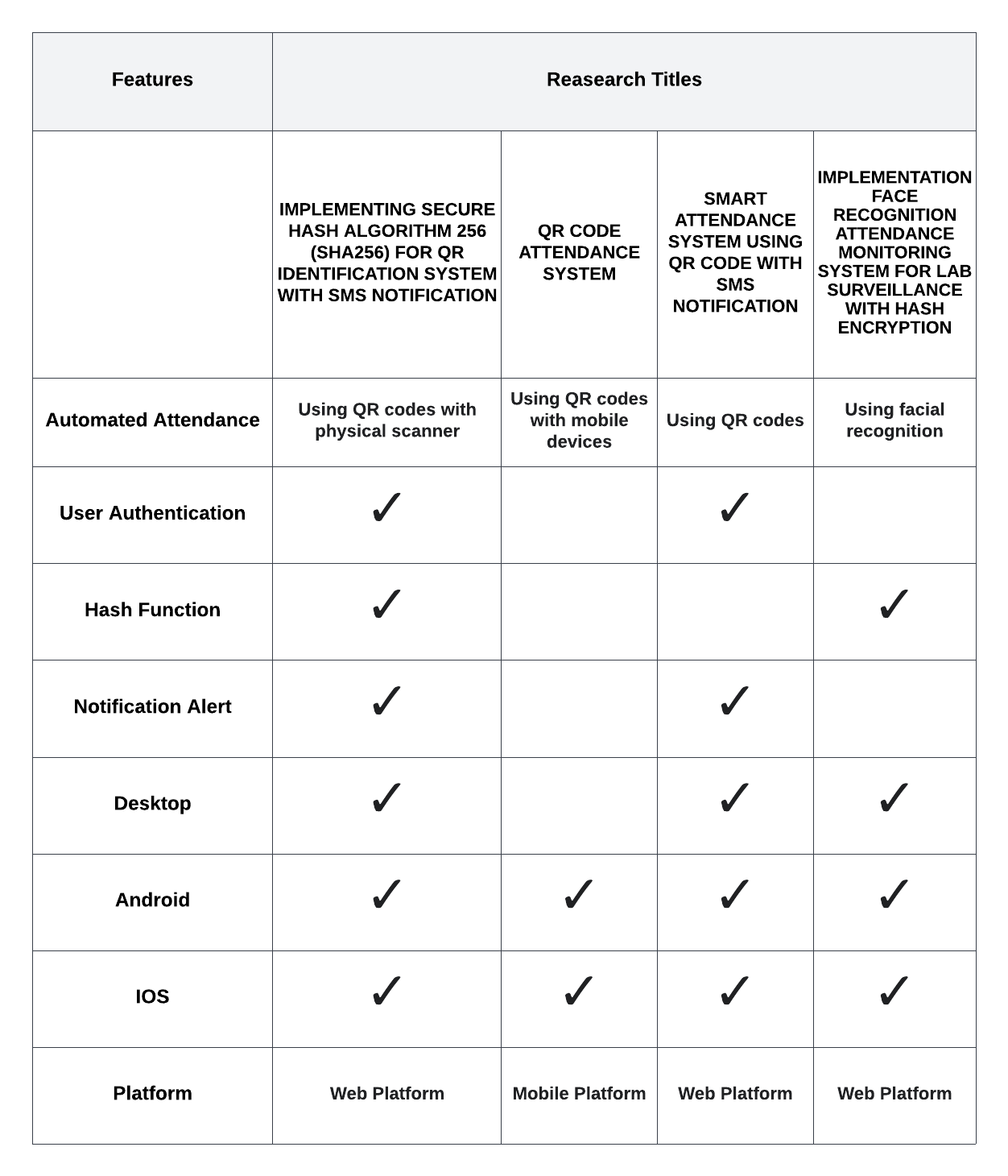
**QR Code Attendance System (Zailani, 2020).** A portable attendance system that can replace the current method of keeping track of attendance was the focus of this project (Zailani, 2020)**.** This research aims to develop a smartphone-based identification system that makes use of QR codes and shows their effectiveness. The system of this study was created utilizing Android Studio, XAMPP, Java SE Development Kit (JDK), and PHP to connect to a MySQL database.The QR code reader and generator are the main components of the system. For the purpose of storing attendance data, it used Google Sheets. The system for this study is developed for the Electrical Engineering Department of the Politeknik Ibrahim Sultan in Pasir Gudang, Malaysia. Unfortunately, this system can only be used with mobile devices and needs an internet connection to function. This study and the proponents study both share the use of QR code technologies for integrating in the attendance management system.

**Smart Attendance System Using QR Code with SMS Notification (Mohammed, 2020).** Thisstudy was focused on the development of a student attendance system that utilizes and demonstrates the capability and effectiveness of QR Codes. The study aimed to replace manual attendance management which was a slow and inefficient way to do things (Mohhamed 2020). The study also emphasized the significance of having weekly message notifications to the parents about the attendance of students to make sure that they know when their children are in class and to keep kids from skipping school. The system is a web based application that is developed and implemented on a computer device that runs on Windows operating system. It uses PHP, MySQL, and Apache. MySQL is where most of the data is stored, while PHP was chosen as the programming language. Regarding the attendance record, the professors need to log into the system and choose the program (diploma or bachelor), course code, class, and semester. Then, the students need to scan the QR code that the professors have set up before the class starts. Unfortunately, this study was limited by the absence of devices built for the system.This study and the proponents study both made use of the QR codes technology in automating attendance as well as the web platform where it is developed. This study also contain a SMS notification feature of which is comparable to the notification module of the proposed system. As this study shares similarities to the proponents system it serves as its primary reference.

**Implementation Face Recognition Attendance Monitoring System for Lab Surveillance with Hash Encryption (Hamami et al., 2020).** This study focused on the implementation of face recognition as a biometric method for smart attendance in a laboratory environment. The system employs a deep learning algorithm and uses FaceNet model capturing faces of employees and maps points to face images determining distances that correspond to measure of face similarity real-time through CCTVs and will be matched with database records to check and verify identity (Hamami, et. al., 2020). Captured data is streamed into a dedicated server and presents real-time data into android mobile devices.The study also implements and highlights the importance of hash encryption from the transmission of data through web, android devices with API to ensure that it can only be accessed by authorized users**.** This study and the proponents study both contain a hashing technique in securing data information. This study aids the proposed study by providing insights of hashing algorithms for data protection in an identification system.

Table 1 shows the comparison of the proposed system to its related studies. This presents how the systems differ from one another in terms of their features and technology used.

Table 1. Comparison of the study to the related studies.



**Synthesis**

The related studies cited in the section helped the proponents with the development of the proposed system. Below are each remarks that each related studies showed similarities:

The studies “QR Code Attendance System” and "Smart Attendance System USing QR Code with SMS Notification" made use of QR codes as a technology incorporated with the attendance system. These studies act as references and assist in the development of the proposed system in terms of technology used. These served as the primary references of the study in the integration of QR Codes in the process of identification and attendance management in a mobile and web platform respectively. The idea of these studies is to utilize the potential capability of QR Codes in fast data transactions . These studies have both the QR generator and QR reader function comparable to the QR module of the proposed system.

The study entitled "Smart Attendance System Using QR Code with SMS Notification" at the same time provides the proponents a basis for the importance and significance of integration of SMS alert notifications in an identification system to be able to use it in a more efficient and useful way.

The study "Implementation Face Recognition Attendance Monitoring System for Lab Surveillance with Hash Encryption" helped the proponents in terms of implementing a security measure in the process of human identification. This study and proposed system both share the goal of providing its users a way to ensure that the data they provided are safe and secured.

The system made sure to secure the student data information, which is not included in any attendance system using the specified QR codes, making this study stronger than the prior study.

The strength of this study is that the system utilize QR Codes and scanning in much more efficient and effective way. For instance, it eliminates the needs of users to use gadgets for scanning by allowing the system to do the process for them. The system only requires its users their unique QR codes which is also regenerative in case of lost and damage. As this system is in a fixed position the time it will took to identify the students will be lessened. A single unit of the proposed system can also cover and handle the entire student population of the institution. The system also implements security hashing algorithm in a way that will secure student data even outside of the system process in case of attempted scanning by other devices.

**METHODOLOGY**

The research design that will be applied in the creation of the proposed approach has been described by the researchers in this chapter. This comprises analyzing the specifications needed to build the system and formulating a sequence of events for the researchers to follow during the design and development of the suggested system.

**Design and Methodology**

**Conceptual Framework.** The researchers conceptualize the QR identification system using the input-process-output (IPO) paradigm model. All the requirements for building the system are listed in the input section and are divided into three main categories: knowledge requirements, software requirements, and hardware requirements. Details containing specific specifications are listed beneath these categories. The process part, which is the next stage in the software development life cycle, is then presented (SLDC). The procedure is separated into seven sections that each work on an iterative system component. enabling the system to advance through several stages of creation. This step ensures that the system fulfills the criteria of the end-users and contains many visually appealing outputs. In the output section is the creation of the said system. Effects for specific system participants are included in a bulleted list of the impact of QR identification system. The impact of the system will be used for feedback and evaluation of the system. This will enable the system to improve based on the feedback.

Figure 1 below shows the input-process-output model diagram for the development of the proposed system. It presents the necessary requirements, processes and results of the completion of the system.

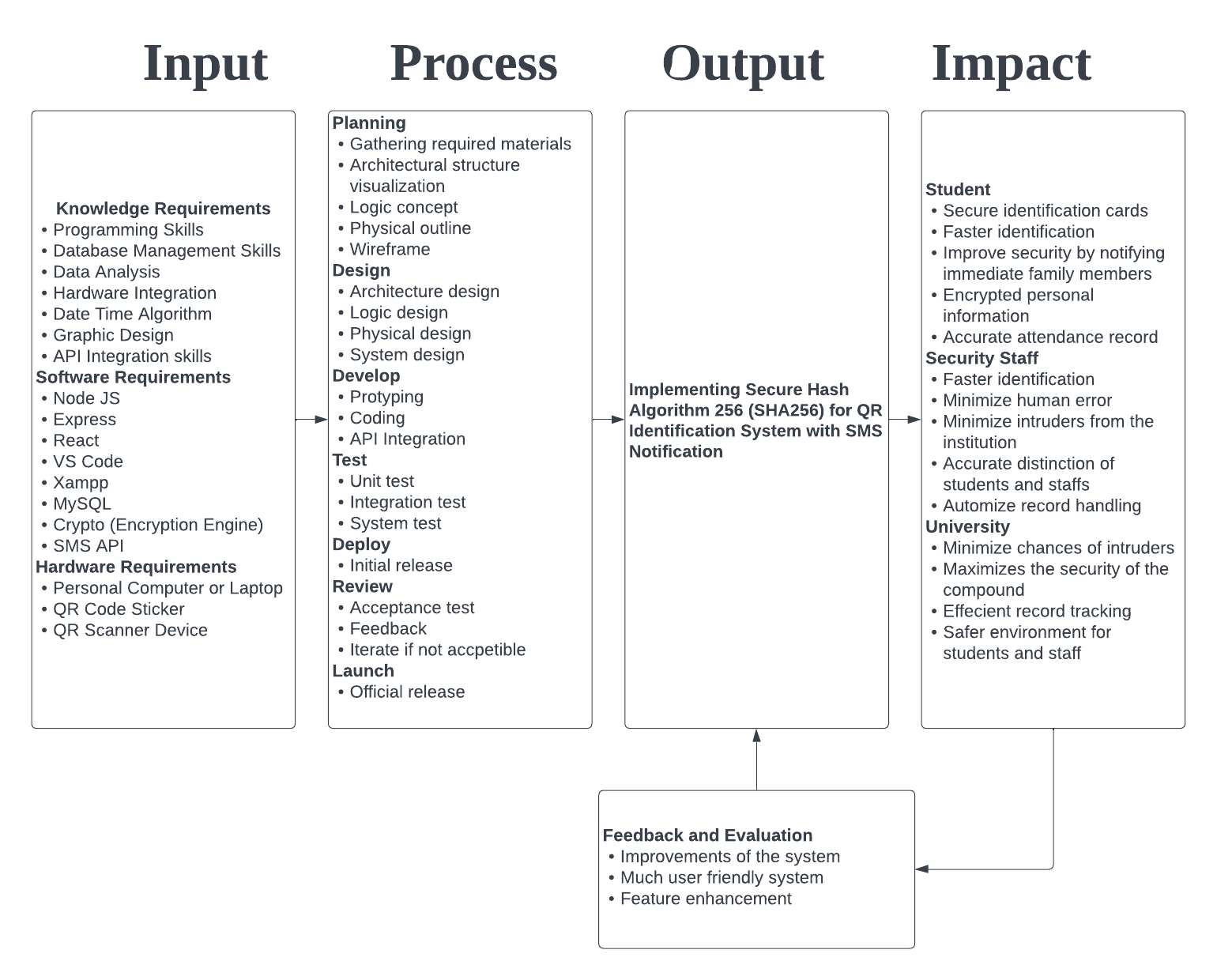
****

Figure 1. Conceptual framework for the “Implementing Secure Hash Algorithm-256 (SHA-256) for QR Identification System with SMS Notification”

**System Architecture.** This section presents the architectural framework of the system. The conceptual model that the researchers have developed represents how each module is interconnected with the others. The modules were created to match the overall functionality and key features of the system. The following duties are accomplished by the four modules, which consist of account management module, record management module, notification module, and QR module.

The administrator will first access the **account management module**, which is in charge of user authentication. Upon successful account authentication, the system dashboard will be presented to the user which enables and gives total system control and access to other different modules.

The **record management module**, this module is divided into two major system processes namely the student record management which is in charge of managing data records of students. The administrator has the capability to add, change, delete, and view student data. The other process is attendance record management which handles and is in charge of managing the attendance records of the students, including add, update, delete, and viewing of records. This module also relies on the QR Code scanning process under the QR module to add attendance records automatically.

The next module will be the **notification module**, this module is responsible for sending message notifications to the family of students during the identification process, as shown in Figure 2. This module also handles the system notifications by invoking alerts that will display details, status and result of certain system processes. And lastly, the **QR module** is the key module of the system. This module handles the QR Code generation processes. This module performs SHA-256 implementation on certain student information before it generates corresponding QR Codes to ensure that the data of students are protected and secured when scanned by other scanning devices outside the system. This module is also mostly where the attendance system is automated. This module utilizes a QR scanner, which is a hardware component of the system. Every time a QR code is read, it adds records to the attendance of students as well as triggers the SMS module, notifying the family of students.

Figure 2 shows the system architecture for the proposed system, which defines the overall organization of the system, relationships between different system components and the levels of access of different users.

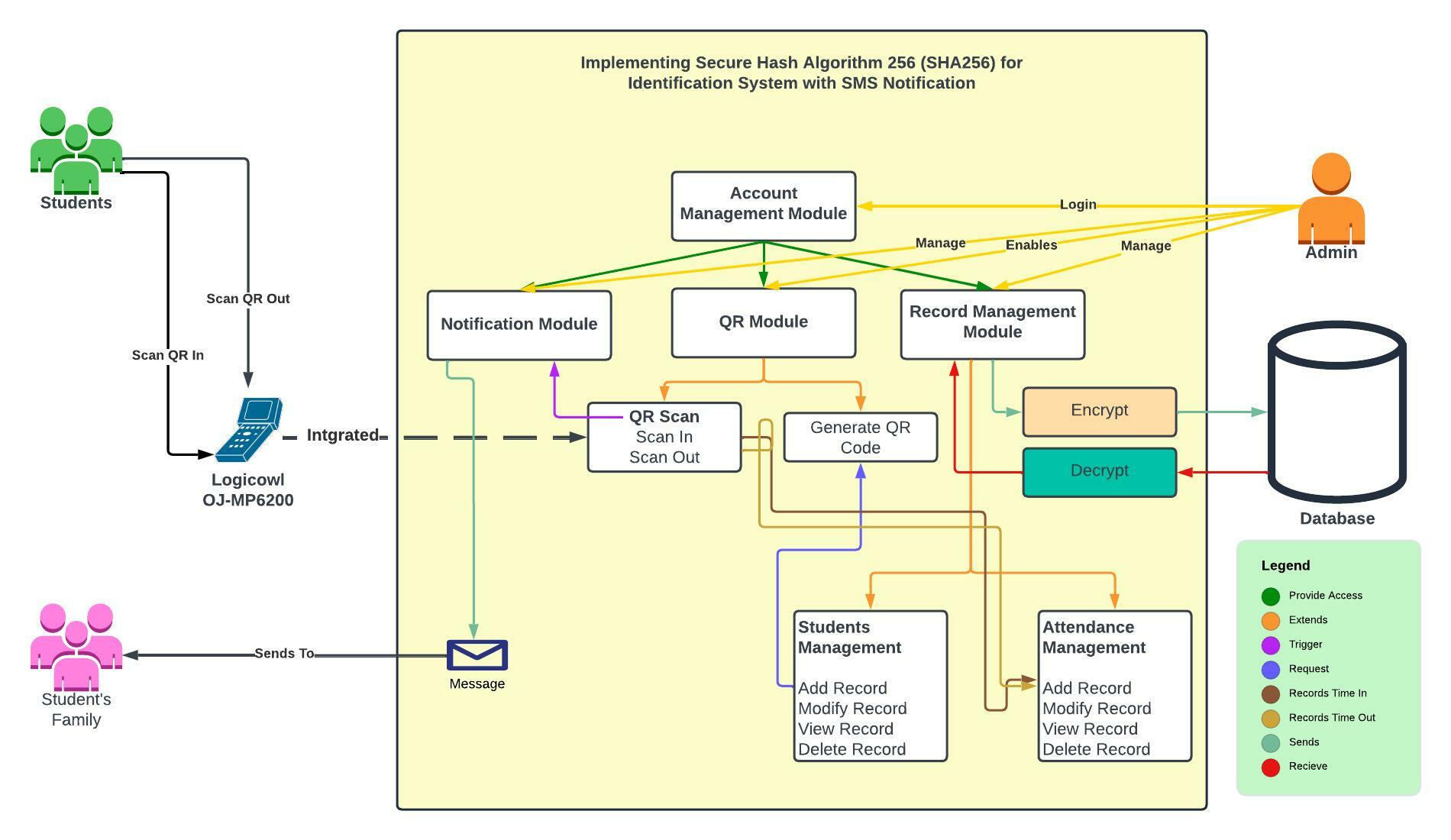


Figure 2. System Architecture for the “Implementing Secure Hash Algorithm-256 (SHA-256) for a QR Identification System with SMS Notification”

**Development and Testing**

The proponents follow the concept of Agile Method as the Software Development Life Cycle in developing the proposed system due to its iterative nature, which allows the developers to create a system with a much more user-friendly end result. These reduce the overall risk of mistakes and failures. This approach is broken down into seven steps: planning, designing, developing, testing, deploying, reviewing, and launch. Following a review of the end users who helped the system mature, this process can circle back to the design phase. The procedure is then carried out once more until the system is prepared for public release and is well-received by end users. The researchers, in particular, employ the Kanban Agile approach. With this method, tasks are classified as pending, ongoing, and completed. This enables the developers to monitor the tasks that have been completed and those that still need to be done.

**Development.** In developing the system, the proponents mainly use ReactJS which is a JavaScript library developed by Facebook that utilizes the concept of reusable components for building the front-end design and interface of the system. The researchers also use Visual Studio Code as an IDE where actual coding and debugging take place. This also helps the developers to integrate different external modules and dependencies needed in the system with its built-in terminal through Node package manager (npm).

In addition, the proponents use XAMPP, a software that provides Apache Web Server and MySQL Database, which will be used to connect and store the actual data during the development process.

**Testing.** The system will undergo different testing procedures and methods before its release and deployment for implementation to evaluate its performance and functionality. The system will undergo the following tests: unit testing and integration testing. Unit testing is the first level of testing which evaluates and tests the individual components or modules of the system ensuring its functionalities. This test helps the developers validate each system component and make sure that it performs as expected. Integration Testing on the other hand tests the overall performance of the system as well as how different system modules functions together including the flow of data from one unit to another. The system will also be tested by selected students from the DIT department of Cavite State University-Main Campus. The system will also be evaluated and ensure to comply with ISO/IEC 9126 standards, an international standard to assess software quality. This will ensure that the functionality, reliability, and efficiency of the system work and perform correctly and is able to fulfill its purpose and objectives.

**Data Analysis Plan**. The researchers used to mean computing the result of the evaluation. The mean is use to solve for the average value of all results from the collected data. It will provide significance to the system in terms of its functionality and efficiency. Below shows the formula to solve for the mean.

Mean Formula;

Where;

= mean

= sum of all scores

= total number of participants

Moreover, the standard deviation is also use to evaluate the data. It measures how the data are spread-out and each score lies from the mean. The formula use to obtain the standard deviation is

Where;

= sample standard deviation

= individual value of dataset

= sample means

= total number of observations

= sum of for all data points

**REFERENCES**

Bah, S. M. & Ming, F. (2020, March). *An improved face recognition algorithm and its application in attendance management system*. https://www.sciencedirect.com/science/article/pii/S2590005619300141?fbclid=IwAR2W4zBT2GeGoquGPuj8-9oSKVlkHcrayg6C0tJOnqrIeGS3vzCcNP0PTYM

BasuMallick, C. (2022, March 15). *10 Key Features of Attendance Management Systems*. Spiceworks. https://www.spiceworks.com/hr/workforce-management/articles/features-of-attendance-management-systems/

Bellana, C. (2021, July 13). *Attendance Management System: Everything You Need to Know – GoSchooler*. Go Schooler. https://goschooler.com/attendance-management-system/

*BigGo Philippines | Check - Compare Products, Price, Promotion*. (n.d.). Ph.biggo.com. https://ph.biggo.com/

B., R. (2018, December 14). *What is MySQL: MySQL Explained for Beginners*. Hostinger Tutorials. https://www.hostinger.com/tutorials/what-is-mysql

Code Signing Store. (2022). *What Is the Most Secure Hashing Algorithm?* Code Signing Store. https://codesigningstore.com/what-is-the-most-secure-hashing-algorithm

Classter. (2019, May 20). *How a Student Attendance System Can Improve the Educational Experience for K12 Schools*. Classter. https://www.classter.com/student-attendance-system-k12-schools/

Deshpande, C. (2022, November 25). *What is ReactJS: Introduction To React and Its Features*. Simplilearn.com. https://www.simplilearn.com/tutorials/reactjs-tutorial/what-is-reactjs

Goyal, S., Yadav, S., & Mathuria, M. (September 2016). *Exploring concept of QR code and its benefits in digital education system.* https://www.researchgate.net/publication/309775446\_Exploring\_concept\_of\_QR\_code\_and\_its\_benefits\_in\_digital\_education\_system

GreatSchools Stuffs (Ed.). (2022, November 17). *Why attendance matters*. Parenting. https://www.greatschools.org/gk/articles/school-attendance-issues/

Gregersen, E. (February, 2022). *Quick response code.* https://www.britannica.com/technology/QR-Code

Hamami, F., Dahlan, I. A., Prakosa, S. W., & Somantri K. F. (2020). *Implementation face recognition attendance monitoring system for lab surveillance with hash encryption.*  https://iopscience.iop.org/article/10.1088/1742-6596/1641/1/012084

Haque, S. & Dybowski, R. (April 2014). *Advanced QR code based identity card: A new era for generating student id card in developing countries.* https://www.researchgate.net/publication/266672526\_Advanced\_QR\_Code\_Based\_Identity\_Card\_A\_New\_Era\_for\_Generating\_Student\_ID\_Card\_in\_Developing\_Countries

Hayes, A. (2021, March 29). *Quick Response (QR) Code Definition*. Investopedia. https://www.investopedia.com/terms/q/quick-response-qr-code.asp

Hossain, M. S., Zhou, X., & Rahman, M. F. (2018). Examining the impact of QR codes on purchase intention and customer satisfaction on the basis of perceived flow. *International Journal of Engineering Business Management*, *10*, 184797901881232. https://doi.org/10.1177/1847979018812323

Imperva. (2019). *What is phishing | Attack techniques & scam examples | Imperva*. Imperva. https://www.imperva.com/learn/application-security/phishing-attack-scam/

Jena, B. K. (2022, November 11). *What Is SHA-256 Algorithm: How it Works & Applications | Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

Kandra, M. (2022, July 19). *Advantages of Automated Attendance Management System*. Kandra.pro. https://kandra.pro/info/advantages-of-automated-attendance-management-system/

Kaspersky. (2019). *What is Cyber Security?* Kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Khan, S. (2022, July 4). *Manual Attendance System: An Unbiased Knowledgebase*. Hrone.cloud. https://hrone.cloud/manual-attendance-system/

LabsMobile. (n.d.). *History and benefits of SMS Messaging - LabsMobile*. Www.labsmobile.com. https://www.labsmobile.com/en/sms-messages

Macaria, C. (2021, June 2). *Session Management in Node.js using ExpressJS and Express Session*. Engineering Education (EngEd) Program | Section. https://www.section.io/engineering-education/session-management-in-nodejs-using-expressjs-and-express-session/

Maramis, G. D. P. & Rompas, P. T. D. (2018). *Radio frequency identification based employee attendance management system* https://iopscience.iop.org/article/10.1088/1757-899X/306/1/012045/

Mike. (2021, June 29). *The Advantages Of SMS API Integration To Your Client Management System*. SHOUTS. https://mikeshouts.com/the-advantages-of-sms-api-integration-to-your-client-management-system/

Mohammed, F. N. B. A. K. (2020). *Smart attendance system using qr code with sms notification.* https://myfik.unisza.edu.my/www/fyp/fyp19sem1/report/46392.pdf

Mostafavi, B. (2020, January 26). *1/3 of Parents in 3 States May Not Send Children to School Because of COVID-19*. University of Michigan. https://labblog.uofmhealth.org/rounds/13-of-parents-3-states-may-not-send-children-to-school-because-of-covid-19

National Center for Education Statistics. (2009, February). *Every School Day Counts: The Forum Guide to Collecting and Using Attendance Data*. Nces.ed.gov. https://nces.ed.gov/pubs2009/attendancedata/chapter1a.asp#

*Office Warehouse Online Store - School and Office Supplies - Office Furniture - Technology Items (Philippines) | Office Warehouse, Inc.* (n.d.). Www.officewarehouse.com.ph. https://www.officewarehouse.com.ph/

Okta. (n.d.). *Hashing Algorithm Overview: Types, Methodologies & Usage | Okta*. https://www.okta.com/identity-101/hashing-algorithms/

Quilala, R., Sison, A. M., & Medina, R. (December 2018). *QR code integrity verification based on modified SHA-1 algorithm.* https://www.researchgate.net/publication/337135594\_QR\_Code\_Integrity\_Verification\_Based\_on\_Modified\_SHA-1\_Algorithm

Royandoyan, R. (2022, April 26). *Filipino kids are the second most vulnerable to online threats globally — study*. Philstar.com. https://www.philstar.com/business/2022/04/26/2176906/filipino-kids-are-second-most-vulnerable-online-threats-globally-study

Rubio, P. (2022, August 25). *5 million Filipinos are victims of identity theft: data analytics firm*. Ph.news.yahoo.com. https://ph.news.yahoo.com/data-analytics-firm-finds-5-million-filipinos-identity-theft-victims-091946956.html

SEAtS Software. (2022, September 5). *A Guide to Student Attendance Management*. SEAtS Software. https://www.seatssoftware.com/2022/09/05/a-guide-to-student-attendance-management/

Sharma, A. (2022, November 18). *What Is Express JS In Node JS | Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/nodejs-tutorial/what-is-express-js

Sophia (2019, June 28). *Essay on Technology: 3 Selected Essays on Technology*. The Wisdom Post. https://www.thewisdompost.com/essay/technology-essay/3387

Uzun, V. & Bilgin, S. (August 2016). *Evaluation and implementation of QR Code identity tag system for healthcare in Turkey.* https://www.semanticscholar.org/paper/Evaluation-and-implementation-of-QR-Code-Identity-Uzun-Bilgin/04d663af36aa75da3a788d850983e01bd24f24de

Veness, C. (2019). *SHA-256 Cryptographic Hash Algorithm implemented in JavaScript | Movable Type Scripts*. Movable-Type.co.uk. https://www.movable-type.co.uk/scripts/sha256.html

Wahsheh, H. A. M., & Luccio, F. (2020). Security and Privacy of QR Code Applications: A Comprehensive Study, General Guidelines and Solutions. *Inf.* https://www.semanticscholar.org/paper/Security-and-Privacy-of-QR-Code-Application

Wara, A. A., & Dugga, S. (2014). *Enhancing User Experience using Mobile QR-Code Application*. https://www.semanticscholar.org/paper/Enhancing-User-Experience-using-Mobile-QR-Code-Wara-Dugga/02d584e6b276130e896ce6013981b2f861e231b9

Yoshida, H. & Biryukov, A. (2016). *Analysis of SHA-256 variant.* https://link.springer.com/content/pdf/10.1007/11693383\_17.pdf

Zailani, F. (2020, December). *(PDF) QR Code Attendance System*. ResearchGate. https://www.researchgate.net/publication/346705138\_QR\_Code\_Attendance\_System

Zimyo Marketing Team. (2020, August 7). *Technologies used in the Attendance management | Zimyo HRMS*. Zimyo. https://www.zimyo.com/insights/technologies-used-in-the-attendance-management/