Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 6, No.4, October 2024, pp. 02404012-01 ~ 02404012-019
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v6i4.850

Integrating Cryptographic Security Features in Information System Barcodes for Self-Service Systems

Sucipto[1], Aidina Ristyawan[2], Dwi Harini[3], Wahid Ibnu Zaman[4], Muhammad Najibulloh Muzaki[5], Mohamed Naeem Antharathara Abdulnazar[6]

[1,2,3,5]Dept. Information System, Universitas Nusantara PGRI Kediri Indonesia

[4]Dept. Education, Universitas Nusantara PGRI Kediri Indonesia

[6]Dept. Computer Systems, ISMA University, Latvia

*sucipto@unpkediri.ac.id

Abstract. Integrating services in an information system is necessary to provide services that can optimize an information system. One of the systems in PKKMB activities that will be combined with information security features is the attendance system. This research uses the Liner Sequential Model (LSM) method to integrate the QR Code attendance system with security features. This research aims to integrate QR Codes by optimizing increased security by combining the Advanced Encryption Standard (AES) algorithm with base64 with a dynamic data model to complicate the QR Code manipulation process. Contribution This study makes optimization of the AES encryption model to improve data security on QR Code. Algorithm testing results include using a Character Error Rate (CER) of 0%, Avalanche Effect (AE) testing with a value of 53.05%, and response time (RT) testing of 10.26ms.

Keywords: QR Code, cryptography, AES Algorithm, attendance, integration, security,

(Received 2024-07-17, Accepted 2024-08-14, Available Online by 2024-09-20)

1. Introduction

Higher education is an educational institution that aims to educate young people at heart by providing learning models based on knowledge and skills that can be applied to community life and the environment [1], [2]. The essence of the task of universities is to prepare academic people who can become agents of social change. The vehicle to introduce the new environment is Introduction to Campus Life for New Students (PKKMB) [3], [4], [5]. PKKMB aims to introduce new students early to various aspects of university life, such as academic regulations, curriculum systems, how to study in college, student ethics, and student organizations.

The rapid development of technology enables human work to be completed quickly. The participation of technology makes data and information processing easier to do. Almost all fields require the involvement of technology in their management, especially in educational administration management. Some systems have been made, but data integration still needs to be improved so that information systems utilize data integration in running their business [6], [7]. It is undeniable that modern technology is considered much more practical than conventional technology. Data and information management in education administration must be appropriately managed. Also, managing primary educational data containing student identity is an essential factor in control so that business processes can run smoothly and optimally [8], [9], [10].

The development of the PKKMB Information System, the object of this research, has been carried out, but there still needs to be improvements in integrating other features into this system [10]. The necessary system development includes an attendance system. Service development must be done so that data effectiveness and security in PKKMB attendance data recap can run efficiently and precisely. Attendance development research to provide a high-security system. They avoided data duplication and fraud committed by students as well as security elements to facilitate the detection of the authenticity of certificate ownership information that is fast and accurate [11]. Research on the Application of QR Codes in Digital Attendance Signatures as a Guarantee of the Authenticity Produced. This research resulted in a practical attendance application using a QRcode to optimize filling attendance in educational institutions [12]. Other research: Implementation of QRcode in Portable Document Format and QR Code for Academic Activities. The research results in the form of Paperless can be done with the presence of digital documents that can be accessed independently (portable), easily, and across platforms [12].

Using attendance with barcode models provides innovation and ease of integration into information systems. Barcode features, in general, still have many gaps, as he got in some previous studies. In this study, additional security is needed to provide attendance data security so that barcode codes cannot be manipulated. The QR Code model is a barcode model that can store many data. QR Code is a two-dimensional matrix technology capable of storing various types of information in it. The information that a QR Code can accommodate reaches 7089 digit numbers and 4296 alphanumeric characters [13]. The QR Code model can accommodate a reasonably long encryption code [14], [15], [16]. Encryption secures information by making it unreadable without specialized knowledge of the type of encryption [17]. In addition, encryption is undoubtedly used in security; this technique is still needed in making special communications secure, especially in ensuring the integrity and authentication of a message to avoid a third person reading the message. Each encryption function has its weak and strong algorithm [18]. Encryption models can provide additional security to barcodes so that it will be difficult to manipulate the data in the barcode code [15]. The importance of implementing additional security by using modifications to the Advanced Encryption Standard (AES) algorithm is carried out by Hameed to reduce authorization problems in a system [19]. Another study was also conducted by Maazouz using AES to improve the security of encryption on images [20].

Based on the description of the PKKMB problem and several research references related to barcode technology, especially in the QR Code model and research on the cryptographic security of the AES algorithm. The purpose of this research is to integrate the QR Code by optimizing security improvement by combining the Advanced Encryption Standard (AES) algorithm with the Base64 algorithm in a dynamic data model so that it can complicate the QR Code manipulation process. This research contributes to introducing a combination scheme of cryptographic algorithms in the QR Code application to improve the security of the attendance system.

2. Methods

2.1. QR Code Technology

A QR Code is a 2D barcode developed by Denso Wave, a subsidiary of Toyota, in 1994 to track automobiles during the manufacturing process. Due to its ability to contain a significant amount of data and be easily scanned and processed by a QR Code reader, often a smartphone, its usage has moved from manufacturing to diverse areas such as retail, marketing, and digital payments [21]. QR Code technology is also used as a tool to make data tracking easier. One of the uses of QR Code technology in the field of digital transactions [22]. The use of digital transactions is carried out to make a code difficult to change [22]. QR Code technology can be used in data processing that is much larger than other barcode technologies. This utilization is used to help the Covid-19 application [23]. QR Code technology plays a very important role in various current technological needs, this is also a problem with the problem of data falsification [24]. QR Code research must be supported by adding security to the code to increase the authenticity of the data, and it is difficult to make changes to the data on the QR Code. The wrong way of supplying it with a two-layer structure can display two alternate messages when scanned from two different directions [25].

2.2. Cryptographic Security

One method of cryptography is encryption, which protects text by making it unreadable without a secret key [21]. Text encryption is essential to improve data security, especially in digital space transactions. It involves the process of converting the original readable data (plaintext) into an unreadable format (ciphertext) so that disinterested people cannot access it [18]. Data encryption's purpose is to maintain data confidentiality during storage, transmission, or processing. However, because the attackers are aware of the existence of ciphertext, they can exploit various weaknesses in the implementation of encryption algorithms, allowing them to decrypt or guess the associated primitive cryptography [18]. There have been several studies on these two algorithms. The research was conducted by Fahmi Anwar in 2019 under the title StegoCrypt Scheme using LSB-AES Base64. The results of this study, Combination of Least Significant Bit (LSB) - Advanced Encryption Standard (AES) - Base64, protect messages and various file formats embedded in digital images [26]. Another study was conducted by Ajeet Ram Pathak in 2019. This study's results address security demands with secure methods to provide security on all file formats using AES (Rijndael) and Base64 encoding, which will later be stored on MySQL database servers in the cloud [27]. Another study was conducted by Abolore Muhamin Logunleko in 2020 under the title An End-to-End Secured Email System using Base64 Algorithm. The developed system secures sensitive information sent via email by providing secure, fast, and strong encryption that makes mail very difficult for attackers to interpret upon incoming transmission, making it resistant to attack [28]. Another study presents a low-power VLSI architecture design for AES cryptographic applications that focuses on electrocardiogram signal transmission as the Advanced Encryption (AES) standard has added a new dimension to cryptography with the potential to protect healthcare devices and systems [29].

The discussion of QR Code literature and cryptography shows that the QR Code technique is still widely used in research because of its ease of use in terms of data storage which is larger than other barcode models. The use of QR Codes is not enough to overcome data security, there needs to be additional security through cryptographic algorithms. The use of the AES cryptographic algorithm needs to be improved from the basic model to prevent data exploitation. In this study, the application of QR Code with the application of a combination of AES algorithm with base64 with a dynamic data model complicates the QR Code manipulation process.

3. Methods

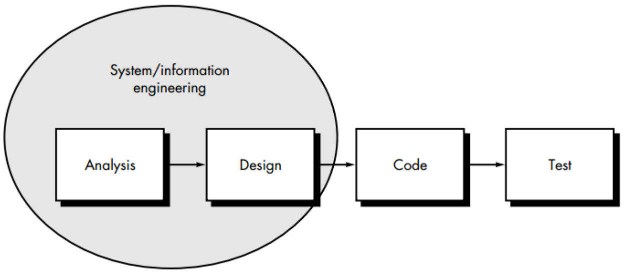


Figure 1. Linear Sequential Model

This study used the Linear Sequential Model (LSM) method. This method demonstrates a systematic, sequential approach to software development that begins at the system level and progresses through analysis, design, coding, and testing [30], [31]. The work on the LSM is carried out systematically, with each process going through certain stages to ensure that the first and last stages of the process required to develop this software have been completed [32]. Figure 1 illustrates a linear sequential model for software engineering. Being part of a business system, the work begins with establishing requirements for all system elements and allocating some of these requirements to software. Software systems must interact with other components, such as hardware, people, and databases. Systems engineering and analysis includes requirements collection at the system level with a small amount of top-level design and analysis. Information engineering consists of a group of requirements at the strategic business level and the business area level.

The advantage of LSM is the ability to capture linear relationships between variables in sequential data. As a result, LSM can be used to find system development values that are based on linear patterns. The software development process, prediction with AI models, and sequential hybrid exploration can be used by LSM [33], [34]. In this study, LSM was used to implement software development by integrating QR codes to improve security by combining Advanced Encryption Standard (AES) algorithms with base64 with dynamic data models, which allows these models to be used in various contexts. Therefore, understanding LSM and their applications in the case of system security in this research can optimize the information system security process.

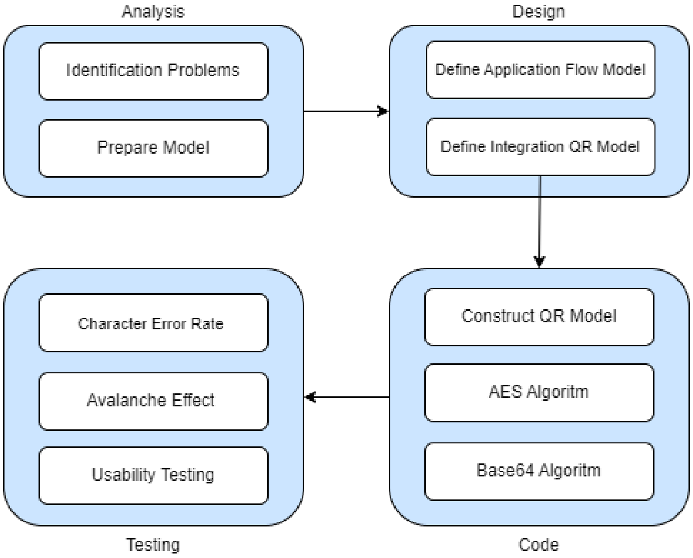


Figure 2. Flowchart Diagram Research

The following Figure 2 is the LSM process in detail:

Analysis. At this stage of the process, the gathering of requirements is intensified and focused on software. To find out the needs, identification is carried out according to the needs of services that will be integrated into the PKKMB system. The initial stage was carried out by observing the conventional methods previously used in PKKMB activities related to evidence of activities, duties, and attendance of PKKMB participants. This research builds a PKKMB system in which there is an attendance system using the Advanced Encryption Standard (AES) algorithm with the Base64 algorithm on a dynamic data model. Dynamic data is a code provided for the attendance validation process. At this stage, it is carried out by the researcher and assisted by a research assistant. Design. This stage of the process is carried out by designing software. Done with diagrams: System diagrams and described on feature diagrams.

Design. This process stage is carried out by software design. This is done by creating a system diagram in the feature diagram where the security of the barcode system includes cryptographic encryption. A design that describes the flow of the PKKMB system based on an integrated information system that contains various features.

Code. This stage of the process is done by code generation. The already-created design is translated into a programming language. The WEB programming language is PHP, which uses the MariaDB database[35]. At this stage, the Chief researcher and Programming Assistant carry out it.

Testing. The Testing Phase focuses on the internal logistics of the software, ensuring that all states and external functionality have been tested; That is, carrying out tests to uncover errors and ensure that the specified input will produce actual results that match the required results [36], [37]. This research uses a random sampling method to test cryptographic algorithms and test the usability of using the attendance application. Testers use several techniques, including Character Error Rate (CER), Avalanche Effect (AE), response time testing (RT), and Usability Testing.

4. Results and Discussion

4.1. RESULT

4.1.1. ANALYSIS

At this stage of the process, requirements gathering is intensified and focused on the software. To determine needs, identification is carried out according to service needs that will be integrated into the PKKMB system. The initial stage was carried out by observing conventional methods previously used in PKKMB activities regarding the presence of PKKMB participants. At the analysis stage, data was obtained that the implementation of PKKMB with an information system must be independent and can be validated automatically. This separate process is presented because in practice students are expected to focus more on PKKMB activities and be able to recap activities after implementing PKKMB. The independent process can make it easier and faster for students to progress through PKKMB to obtain a certificate. Some integrations of previous systems carry out the implementation of these separate systems. Namely, there is integration of QR Code-based attendance with cryptographic security which can be done independently.

4.1.2. DESAIN

This process stage is carried out by software design. This is done by creating a system diagram presented in Figure 2, described in the feature diagram where the security of the barcode system includes cryptographic encryption, explained in Figure 6.

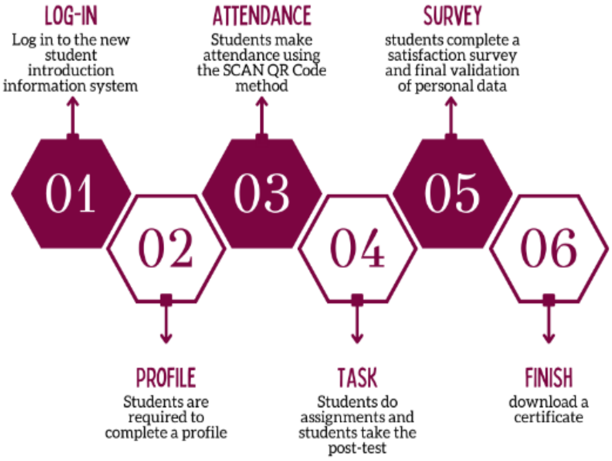

LOG-IN
Log in to the new student introduction information system
01
02
PROFILE
Students are required to complete a profile
ATTENDANCE
Students make attendance using the SCAN QR Code method
03
04
TASK
Students do assignments and students take the post-test
SURVEY
students complete a satisfaction survey and final validation of personal data
05
06
FINISH
download a certificate

Figure 3. PKKMB System Integration Flow Design

The design in Figure 3 illustrates the flow of the PKKMB system based on an integrated information system. One feature service will be developed in security, namely Presence. Development of a security-based QR Code system with an Encryption Code so that the QR Code is challenging to manipulate. Design the features diagram as shown in Figure 4. In the design, there is an old module and the integration of a new module, namely the QR Code presence. The features in the PKKMB system also become more concise because there are only two actors, namely the committee and new students. The committee is a high-level access held by the PKKMB coordinator. It regulates several provisions in the system, including opening login access, determining schedules, and supervising PKKMB results. The second actor is Maba, where the process in this system is carried out independently until the new students get a certificate. The features present in the information system are described in Figure 4. Feature Figure 4 has five modules: user data, attendance, task, survey, and certificate. The main feature in the implementation of cryptographic security is the attendance module.

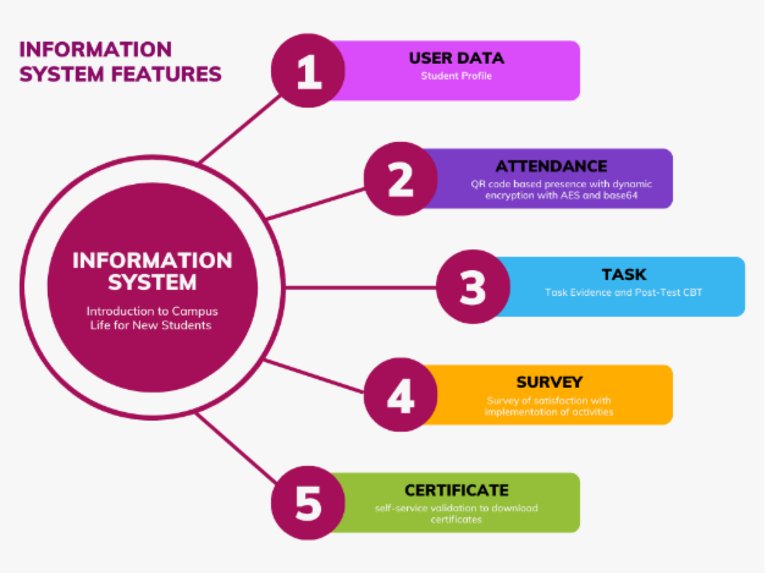

INFORMATION SYSTEM FEATURES
INFORMATION SYSTEM
Introduction to Campus Life for New Students
1
USER DATA
Student Profile
2
ATTENDANCE
QR code based presence with dynamic encryption with AES and base64
3
TASK
Task Evidence and Post-Test CBT
4
SURVEY
Survey of satisfaction with implementation of activities
5
CERTIFICATE
self-service validation to download certificates

Figure 4. Features Diagram

4.1.3. CODE

Code. This stage of the process is done by code generation. The already-created design is translated into a programming language. The WEB programming language used is PHP, which uses the MariaDB database. The attendance menu in Figure 5 is a new feature of this system. Students conduct independent attendance by scanning the QR Code provided by PKKMB assistants and encoding cryptographic algorithms using native PHP. The algorithm used is the AES 256bit algorithm, which is converted into a base64 hash algorithm to be used as a barcode on the attendance system[38], [39]. The barcode generation feature is done dynamically, where each attendance scan has a different code. QR Code Template As in Figure 4, the main code that shows the presence of students at PKKMB activities. QR Code is encrypted with Encode 64 and AES algorithms. The QR Code process is safe because you cannot duplicate the QR Code that the committee does daily.

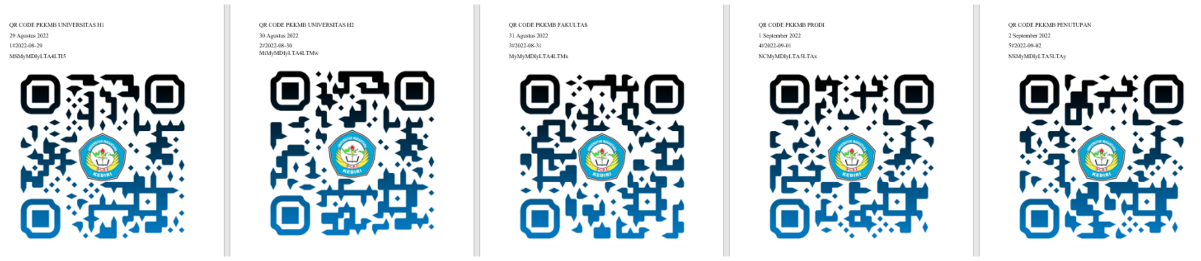


Figure 5. QR Code

The encryption process is a process that converts plain text into ciphertext that aims to secure confidential data or message content so that cryptanalysts do not intercept it. At the same time, the decryption process is the opposite of the encryption process, which converts ciphertext into plain text. In decryption, the file's contents in ciphertext must be altered back into the original message or file (plain text). For this reason, it is necessary to analyze the file's contents in terms of accuracy or compatibility, whether the file to be decrypted can return to the original file perfectly or not. Algorithm 1 is a pseudocode flow from the integration of the QR Code security algorithm.

Algorithm 1 Procedure for Understanding AES With Base64_256bit

```
Input:
  plaintext: plaintext string
  key: 256-bit block (32 bytes)
Output:
  encoded_ciphertext: Base64 encoded string of the AES ciphertext
Constants:
  Nb = 8  // Number of columns (32-bit words) comprising the state
  Nk = 8  // Number of 32-bit words comprising the key
  Nr = 14  // Number of rounds, which is a function of Nk
Subroutines:
  SubBytes(state):
      for each byte in state:
          replace byte with the corresponding value from S-box
  ShiftRows(state):
      rotate each row of state to the left by row index (0, 1, 2, 3)
  MixColumns(state):
      for each column in the state:
          replace column with new values based on matrix multiplication in GF(2^8)
  AddRoundKey(state, roundKey):
      for each byte in state:
          state[byte] = state[byte] XOR roundKey[byte]
  KeyExpansion(key):
      generate round keys from the cipher key
  AES_Encrypt(block, key):
      state = block
      roundKeys = KeyExpansion(key)
      AddRoundKey(state, roundKeys[0:Nb])
      for round from 1 to Nr-1:
          SubBytes(state)
          ShiftRows(state)
          MixColumns(state)
          AddRoundKey(state, roundKeys[round*Nb:(round+1)*Nb])
      SubBytes(state)
      ShiftRows(state)
      AddRoundKey(state, roundKeys[Nr*Nb:(Nr+1)*Nb])
      return state
  Pad(plaintext):
      padding_length = 32 - (length of plaintext % 32)
      append padding_length bytes of value padding_length to plaintext
      return padded plaintext
  Base64_Encode(data):
      return base64 encoded string of data
Main Algorithm:
  padded_plaintext = Pad(plaintext)
  blocks = split padded_plaintext into 32-byte blocks
  encrypted_blocks = []
  for each block in blocks:
      encrypted_block = AES_Encrypt(block, key)
      append encrypted_block to encrypted_blocks
  concatenated_encrypted = concatenate all encrypted_blocks into one byte array
  encoded_ciphertext = Base64_Encode(concatenated_encrypted)
  return encoded_ciphertext
```

Explanation of Pseudocode steps:

SubBytes: Each byte is replaced with the corresponding value from the S-box.

ShiftRows: Rows are shifted cyclically.

MixColumns: Columns are mixed using matrix multiplication in GF(2^8).

AddRoundKey: XOR each state byte with the round key.

KeyExpansion: Generates round keys from the cipher key.

AES_Encrypt: Performs AES encryption on a single 256-bit block (32 bytes).

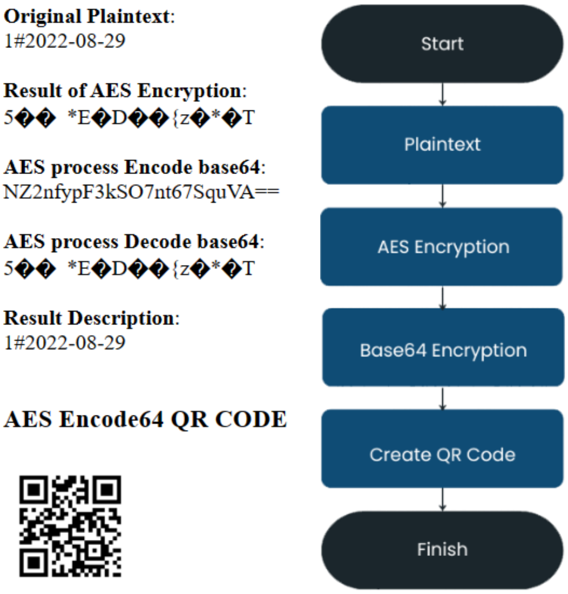
Pad: Pads the plaintext using the PKCS7 padding scheme so that the length is a multiple of 32 bytes.

Base64_Encode: Encrypts encrypted data in Base64 format.

Main Algorithm:

a. Perform padding on plaintext.
b. Breaks padded plaintext into blocks of 32 bytes.
c. Encrypt each block with AES.
d. Combines all encrypted blocks.
e. Encodes the combined ciphertext using Base64.

By using a 256-bit block length, this algorithm ensures that the plaintext is encrypted with a higher level of security before being encoded into Base64 format. Figure 5 is the plaintext flow until the QR Code is created.



Original Plaintext:
1#2022-08-29

Result of AES Encryption:
5�� *E�D��{z�*�T

AES process Encode base64:
NZ2nfypF3kSO7nt67SquVA==

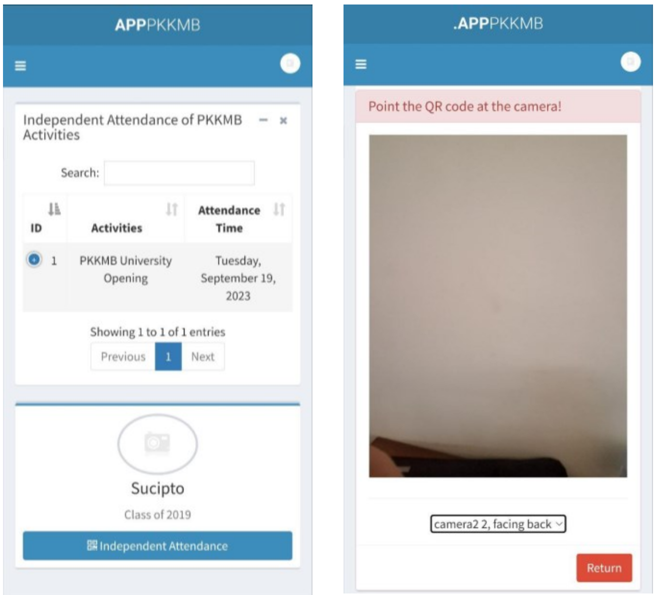
AES process Decode base64:
5�� *E�D��{z�*�T

Result Description:
1#2022-08-29

AES Encode64 QR CODE

Figure 6. Cryptographic Process QR Code

The encryption process in Figure 6 begins with the specified dynamic plaintext, e.g., plaintext “1#2022-08-29”. Plaintext is then encrypted using AES 256bit algorithm, then converted using base64 hash algorithm and created QR Code—system implementation as shown in figure 6. The flow starts from The process for attendance by clicking on the attendance button and pointing the camera at the QR Code, as shown in Figure 7. If the QR Code is appropriate, the attendance data will enter the system, and if the QR Code does not match or duplicate, the data will be rejected.



Independent Attendance of PKKMB Activities

ID	Activities	Attendance Time
1	PKKMB University Opening	Tuesday, September 19, 2023

Showing 1 to 1 of 1 entries

Sucipto

Class of 2019

Point the QR code at the camera!

Figure 7. QR Attendance

4.1.4. TESTING

The Testing phase focuses on the logical internals of the software, ensuring that all statements have been tested, and on the functional externals; That is, conducting tests to uncover errors and ensure that the specified inputs will produce actual results that correspond to the required results—the initial test used three tests performance, namely Character Error Rate (CER). Character Error Rate (CER) is a metric used to evaluate the accuracy of text recognition systems, such as Optical Character Recognition (OCR) or speech-to-text systems. It measures the rate of errors in the character-level transcription of a piece of text compared to a reference or ground truth text[40].

$$CER = \frac{S+D+I}{N} \qquad ...(1)$$

Where:
S is the same number of characters on predictions and references.
D is the number of characters deleted in the forecast compared to the authority.
I am the number of characters inserted in the estimates compared to the head.
N is the total number of characters in the connection.

Test results using CER obtained a value of 0%. The result indicates that the plaintext and description results return the same value. Second Examiner using Avalanche Effect. The Avalanche Effect is a concept primarily associated with cryptography and information security. It refers to a desirable property of cryptographic algorithms, particularly cryptographic hash functions and encryption algorithms, where a slight change in the input data (even a single bit) should produce a significantly different output or ciphertext.

$$AE = \frac{1}{n}\sum_{i=1}^{n}\frac{H(D_m)-H(D_{mi})}{H(D_m)} \quad ...(2)$$

Where:
n is the number of bits changed between the original message and the modified message,
H(D_m) is the entropy of the original message,
H(D_{mi}) is the entropy of the modified message.

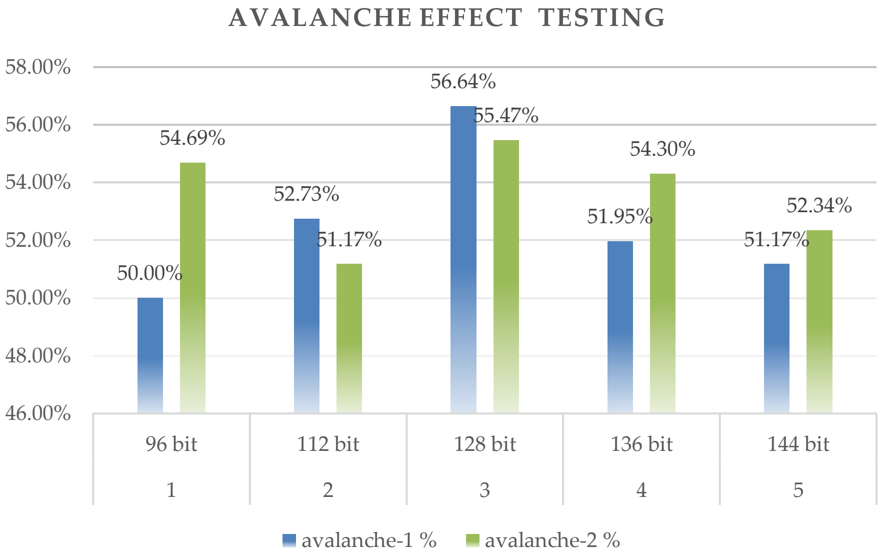


Figure 8 Avalanche Effect Testing

AE testing uses 10 Test scenarios with the same 5-bit data types. The test result is in Figure 8, with a minimum mark of 50% and the highest development of 56%. AE testing does not contain specific standards within the minimum percentage limit. In some previous studies, it has a value range of 50%[41], [42]. The next test uses Response Time. In general, response time refers to the amount of time it takes for a system, process, or entity to react to a stimulus or complete a task. It is often used to measure how quickly a system or component can respond to a user's request or an external event.

$$RT = T_{\text{end}} - T_{\text{start}} \quad ...(3)$$

Where:
"End Time" is when a system or entity completes a task or responds to a request.
"Start Time" is when a request or task is first received or started.

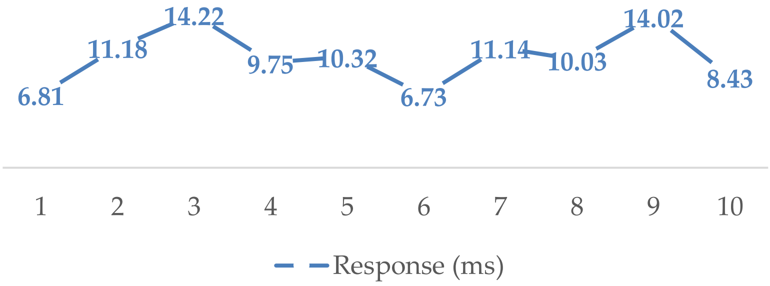


Figure 9. Response Time Testing

RT test results with 10-time access test scenarios. The test results in Figure 9 are presented in milliseconds—tests with a minimum mark of 6.73ms and a highest of 14.22ms. After the PKKMB system information system development, testing is carried out using the usability method. Usability is now known as the primary key that determines the success of an interactive system or product. Usability is also referred to as a characteristic of product quality where the sub-characteristics consist of the ability to be recognized appropriately (appropriate recognizability), ease of learning (learnability), ease of operation (operability), error protection by users (user error protection), the beauty of the interface appearance (user interface aesthetics), and accessibility (accessibility)[43], [44], [45]. Data collection in conducting usability evaluation in information systems is carried out by guiding procedures for conducting Heuristic Evaluation to facilitate evaluators in conducting tests, assessment forms, and consent forms to become evaluators. The assessment uses a Likert scale of 1-5, with a value of 1 as the lowest usability problem and five as the highest usability problem[46], [47]. The data collected as an assessment of the user preference test questionnaire was carried out using two stages: preparation of questionnaires from the Post-Study System Usability Questionnaire (PSSUQ) type questionnaire and testing the validity of the data obtained by the questionnaire in Fig 10.

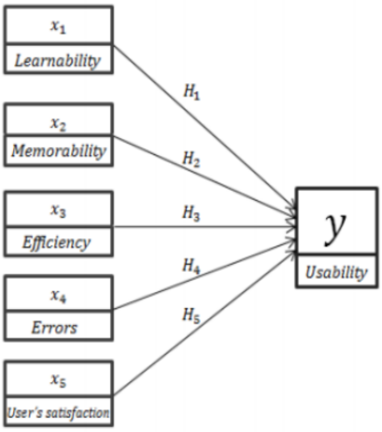


Figure 10. Usability Framework

The evaluation was carried out by giving ten main questions to the panellists who had been selected. The questions are by the Heuristic Evaluation model[48], [49] in providing input or evaluation of PKKMB Information System Integration with the addition of security to the presence of QR Code with Cryptography. Table 1 shows a list of questions discussed by the expert panel to conduct an Information Systems evaluation. The following is a list of questions in the questionnaire testing:

a. Learnability: Ease in learning the use of information systems and ease in obtaining information specifically needed
b. Memorability: Ease in remembering how to use information systems and carrying out the same task.
c. Efficiency: Obtaining concise information, completing tasks quickly, and easily navigating himself or his knowledge to use information systems through exploring features and content available on information systems rapidly.
d. Errors: Few errors or errors are detected in the information system when used by the user, and errors detected can be corrected quickly using language that the user quickly understands.
e. User Satisfaction: the information system gives a pleasant impression to use. Measure user opinion if you are uncomfortable using the information system because of some difficulties that affect task failure in the scenario.
f. Usability: Overall, how much PKKMB information system integration of the QR Code presence security module with Cryptography can satisfy users in performing tasks, searching for information, and others?

Table 1. Expert Panel Questions

No	Nielson Model	Question
1	Visibility of system status: the interface on the system provides information to users about the condition of a process within a certain period	Does the user get information about the progress process of the system with appropriate feedback in a reasonable time?
2	Match between the system and the natural world: the system uses the user's language with words and phrases familiar to the user.	What is the concept of using the system, and how is Indonesian good for users? Does the system use conform to the real world and display logical information?
3	User control and freedom: The User can control certain conditions and get out of a specific situation due to choosing the wrong system function.	Will users be able to do what they want in navigating and selecting system functions?
4	Consistency and standards, consistency of interfaces on the system, and standards	Do design elements have the same meaning or effect in different situations?
5	Error prevention is the handling of errors that the user may make.	Can users make mistakes where good design will prevent them?
6	Recognition rather than recall is an interface component on the system that is easily recognized by users and minimizes user recall.	Are interface components easy to identify? Are users forced to recall information from one part of the system to another?
7	Flexibility and efficiency of use, flexible and efficient use of the system.	Is the task method efficient? Can the user adjust his actions, or must he do many steps to get a process?
8	Aesthetic and minimalist design, the appearance has aesthetics/beauty and does not disturb the user when interacting with the system.	Does the existing display's beauty help the user determine the process or vice versa?
9	Help users recognize, diagnose, and recover from errors; the system makes identifying, analyzing, and exiting mistakes easy.	Is the error message expressed in plain language (without code)? Does the notice accurately describe the problem and suggest a solution?
10	Help and documentation: The system provides help features and documentation.	Is help information provided, searchable, and focused on user tasks?

The questionnaire was carried out on October 15-30, 2022, in distributing the questionnaire by disseminating information through Microsoft Forms 365. Realization of the Distribution of QR Code Attendance Questionnaire Results was randomly carried out on 40 respondents. In the assessment, the results of the average user assessment of 5 components and the conclusion of usability from integrating the PKKMB information system, as well as the addition of QR Code attendance with Cryptography, are like Table 2 using a scale of 5. Based on the assessment obtained, it can be seen that, in general, respondents are satisfied with the usability performance of PKKMB information system integration, the addition of CBT modules, and QR Code attendance with Cryptography with an average value of 4.57, the lowest assessment is obtained in the error component and the highest is the learnability component.

Table 2. User Test Results

Component	Average Grades
Learnability	4,70
Memorability	4,63
Efficiency	4,54
Error	4,48
User Satisfaction	4,56
Usability	4,52

In the development of the information system development process, is still the initial grand launching of PKKMB activities carried out in August. So what is done by the system provides a little detailed information because this system is intended to be learnable, so that information is not conveyed in detail. The language used as an introduction in the information system is optimal. The selection of Indonesian on information and foreign language absorption in the technical module used is by using everyday language so that the user will quickly understand the intention the information system wants to convey. The use of navigation on web-based information systems so that multiplatform can be accessed without any significant obstacles, but some things interfere because it needs a particular web domain link to access the system. IOS users could be more optimal on QR Code attendance, requiring some adjustments.

The design elements displayed already use good colours with the concept of a Design System that contains the identity of a product, such as colour palette, typography, icons, and components so that the text displayed can be read correctly. The interaction between the user and the application when scanning data validation, the rest of the user will be passive because the data is more information and processes by itself. Using image logos and existing QR Codes is by the appropriate ratio so that users will easily recognize images and make it easier to scan QR Codes.

The method of assigning users to each menu in the existing information system is simple; this causes users not to be burdened with the task of memorizing the steps that must be done to get the desired results. One of the things that makes task efficiency easily achieved in this application is the need for more user interaction in providing interactive input into the application. The beauty of the design used is good in helping users understand the information in the application in shape, colour, font, and position. Concerns about the beauty of the invention that contradicts the ease of function of the application do not occur in this application.

The error information displayed by the information system needs to be more technical. The error message should be more straightforward and solutive so that the user quickly understands it. When the active user area cannot be displayed, the news in the application is too technical, and the user needs to be given information to solve the problem. The help of using the application for users on the About page is still straightforward and only covers part of the information system. Ideally, every time you enter a feature, there is a help menu in each context, but even if this is not fulfilled, the help is still quite informative, and users have been helped. Detailed indicators on the test can be seen in Table 3.

Table 3. Nielson indicator

No	Nielson	Principle Fulfillment	Indicator Usability Nielson Model	User ratings	Compliance	
					Yes	No
1	Visibility of system status	Fulfilled	System Pleasant to use	Fulfilled	in	
2	Match between the system and the natural world	Fulfilled	Easy to understand	Fulfilled	in	
3	User control and freedom User	Unfulfilled	System Pleasant to use	Fulfilled	in	
4	Consistency and standards	Fulfilled	Easy to establish	Fulfilled	in	
5	Error prevention	Unfulfilled	Several errors were detected	Unfulfilled		in
6	Recognition rather than recall	Fulfilled	Easy to remember	Fulfilled	in	
7	Flexibility and efficiency of use	Fulfilled	Easy to reach quickly	Fulfilled	in	
8	Aesthetic and minimalist design	Fulfilled	Comfort to Use	Fulfilled	in	

No	Nielson	Principle Fulfillment	Indicator Usability Nielson Model	User ratings	Compliance	
					Yes	No
9	Help users recognize, diagnose, and recover from errors. Sistem	Unfulfilled	Easy to fix	Unfulfilled		in
10	Help and documentation System	Unfulfilled	Easy to fix	Unfulfilled		in

4.2. DISCUSSION

Based on the Four Test Results, the attendance system with which it can be divided into two tests. In the first group, the test regarding the algorithm's ability is tested using CER, AE, and RT. The second test is to find out the use of the attendance application after the QR Code is added to the cryptographic algorithm. Here's more context about each of these metrics and their critical role in ensuring system security and usability, addressing issues ranging from resistance to attacks to providing a seamless user experience.

a. Character Error Rate (CER):

The importance of using CER measures the accuracy of character recognition systems, such as Optical Character Recognition (OCR) or text recognition [50]. In the context of security, CER ensures that text-based security measures on algorithm integration can be strongly assessed against attacks by incorrectly recognizing characters [50]. In the context of usability, CER which has a high value accurately improves the user experience of applications that have been built on this system.

b. Avalanche Effect:

The importance of AE refers to how sensitive cryptographic algorithms are to changes in input. Good cryptographic algorithms show this effect strongly, meaning that a small change in the input (e.g. one bit) will result in a very different output [51]. In the context of Security AE ensures that even small changes to the input data significantly alter the encrypted output, making it difficult for an attacker to infer the relationship between the input and the output through analysis [51]. In the context of Usability AE While it does not directly impact usability in terms of user interaction, a strong AE contributes to the overall security of systems that use encryption.

c. Response Time:

The importance of RT to measure how quickly the system responds to user requests or input [52]. Rapid RT security can contribute to security by reducing the opportunity for attackers to exploit vulnerabilities through time-lapse attacks or denial-of-service attempts [52]. In the context of rapid Usability RT improves the user experience, ensuring that interaction with the system feels smooth and responsive, which is critical for user satisfaction and productivity.

Tests with cryptographic additional security show that the initial test of the algorithm on the results of the CER Test obtained a value of 0%. The CER finding a low score indicates that the accuracy works well on the character or text recognition system [50]. In the context of encryption testing, CER obtained the appropriate comparison results between the decrypted text and the original text [53]. In the next test, the Avalanche effect is used where this test is to get high efficiency in encryption techniques. AE is one of the most important factors, and it is calculated as the number of bits reversed with a small change in a key, plain text, or initialization vector. The AE results shown in Table 7 are consistent with results above 50%. The changed AE value for 50% of the ciphertext bits shows a good avalanche effect. The strong avalanche effect shows that encryption algorithms resist different cryptographic attacks [51]. A good AE value indicates a hash function where a small change in the input of the hash function will result in a significantly different output [54]. The last test to test the quality of the algorithm is RT testing. RT is the process of evaluating the performance of an algorithm by calculating how long it takes to complete a certain task. This is especially important for encryption algorithms because it shows how fast the algorithm can encrypt and decrypt data [55]. The RT results in this study had an average of 10,263ms. RT results on the algorithm show the efficiency of the encryption algorithm [52]. The last stage is to conduct usability testing to find out the process of testing the attendance system with real users to ensure that the product is easy to use, effective, and satisfying to users [56]. This test involved 40 respondents with a random sampling system taken from potential system users. The results of the usability test got an average score of 4.57. These tests show that the app is well-received by users [57]. Compared to previous research [22], [58], We use a larger bit operation of 256bit in the use of integration between algorithms with dynamic keys. Other research [26], [29] In the application of the cryptography algorithm, it only focuses on the CER test but has not conducted other tests such as in this study to find out how feasible the algorithm is to be used at the end-user level. The findings based on the test results on modifying the Advanced Encryption Standard (AES) using base64 on the dynamic data model show good results. The limitation of this research is the absence of provisions for providing alternative keys for the integration of modified algorithms. Future research will focus on modifying the algorithm scheme to obtain alternative keys for dynamic data.

5. Conclusion

This study proposes security optimization on the QR Code with Advanced Encryption Standard (AES) by using base64 on a dynamic data model. The results of several tests include a similarity performance test using a Character Error Rate (CER) of 0%, an Avalanche Effect (AE) test with a value of 53.05%, and a response time (RT) test of 10.26ms. The test uses usability on the application with an average score of 4.57. The results of several tests show that the algorithm modification process gets good results and the system is acceptable to users. The findings in this study show that the integration of algorithms embedded in QR Codes in self-service systems provides an improvement in terms of security in the information system. The improvement of QR Code capabilities in this research has an impact on the research of cryptography text algorithms to always provide more security improvements to QR Codes for transaction activities, especially self-service services.

This research can study alternative encryption algorithms that are better when used as alternatives or in conjunction with the AES algorithm. Further research can develop more robust and effective security solutions by using various security tests with a combination of public and private keys. Moreover, research can explore how users perceive QR Code security and how they view it. Understanding the awareness, trust, and desire of users to use encrypted QR Codes can provide useful information for security development and implementation.

Acknowledgements
The author would like to thank the Institute for Research and Community Service at Universitas Nusantara PGRI Kediri which has provided financial support for this research through the Basic Research Scheme.

References

[1] A. Madhesh, “Quality of life of higher education students with disabilities at Shaqra University,” *Res Dev Disabil*, vol. 138, p. 104520, 2023, doi: https://doi.org/10.1016/j.ridd.2023.104520.

[2] M. A. Briggs, C. Thornton, V. J. McIver, P. L. S. Rumbold, and D. J. Peart, “Investigation into the transition to online learning due to the COVID-19 pandemic, between new and continuing undergraduate students,” *J Hosp Leis Sport Tour Educ*, vol. 32, p. 100430, 2023, doi: https://doi.org/10.1016/j.jhlste.2023.100430.

[3] C. Johnson *et al.*, “Student support in higher education: campus service utilization, impact, and challenges,” *Heliyon*, vol. 8, no. 12, p. e12559, 2022, doi: https://doi.org/10.1016/j.heliyon.2022.e12559.

[4] C. Xie, “Construction of Smart Campus Cloud Service Platform Based on Big Data Computer System,” *Procedia Comput Sci*, vol. 208, pp. 583–589, 2022, doi: https://doi.org/10.1016/j.procs.2022.10.081.

[5] M. Mohzana, “The Impact of the New Student Orientation Program on the Adaptation Process and Academic Performance,” *International Journal of Educational Narratives*, vol. 2, no. 2, pp. 169–178, Apr. 2024, doi: 10.55849/IJEN.V2I2.763.

[6] L. Diop, C. T. Diop, A. Giacometti, and A. Soulet, “Pattern on demand in transactional distributed databases,” *Inf Syst*, vol. 104, p. 101908, 2022, doi: https://doi.org/10.1016/j.is.2021.101908.

[7] Y. Mansouri, V. Prokhorenko, and M. A. Babar, “An automated implementation of hybrid cloud for performance evaluation of distributed databases,” *Journal of Network and Computer Applications*, vol. 167, p. 102740, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102740.

[8] M. Asif-Ur-Rahman *et al.*, “A semi-automated hybrid schema matching framework for vegetation data integration,” *Expert Syst Appl*, vol. 229, p. 120405, 2023, doi: https://doi.org/10.1016/j.eswa.2023.120405.

[9] S. Melzer, O. C. Eichmann, H. Wang, and R. God, “Simulation of Database Interactions for Early Validation of Digitized Enterprise Processes,” *Procedia Comput Sci*, vol. 219, pp. 658–665, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.336.

[10] M. Pirani, A. Cucchiarelli, and L. Spalazzi, “Paradigms for database-centric application interfaces,” *Procedia Comput Sci*, vol. 217, pp. 835–845, 2023, doi: https://doi.org/10.1016/j.procs.2022.12.280.

[11] O. . O. Mayowa, E. . W. Adedayo, O. . O. Olamide, J. A. P. Awokola, and Q. . B. Sodipo, “Design and Implementation of a Certificate Verification System using Quick Response (QR) Code,” *LAUTECH JOURNAL OF COMPUTING AND INFORMATICS* , vol. 2, no. 1, pp. 35–40, Jul. 2021, Accessed: Jun. 19, 2024. [Online]. Available: http://laujci.lautech.edu.ng/index.php/laujci/article/view/36

[12] R. V. Imbar, B. Renaldy Sutedja, and M. Christianti, “Smart Attendance Recording System using RFID and e-Certificate using QR Code-based Digital Signature,” *8th International Conference on ICT for Smart Society: Digital Twin for Smart Society, ICISS 2021 - Proceeding*, Aug. 2021, doi: 10.1109/ICISS53185.2021.9533199.

[13] P. H. Kumar, J. P. V. H. S. S. Lingesh, B. M. Ram, A. P. N. Priyanka, K. V. Babu, and U. K. Vamsi, “Touchless Attendance System using QR Code and Power Apps,” *International Journal of Research in Engineering, Science and Management*, vol. 5, no. 5, pp. 279–281, Jun. 2022, Accessed: Aug. 25, 2022. [Online]. Available: http://www.journals.resaim.com/ijresm/article/view/2128

[14] C. Song *et al.*, “Collection of patient-generated health data with a mobile application and transfer to hospital information system via QR codes,” *Computer Methods and Programs in Biomedicine Update*, vol. 3, p. 100099, 2023, doi: https://doi.org/10.1016/j.cmpbup.2023.100099.

[15] J. Raja, J. Rajeswari, and S. Jayashri, “A secured QR pattern based E health care CAD system for CXR image analyzes,” *Optik (Stuttg)*, vol. 273, p. 170344, 2023, doi: https://doi.org/10.1016/j.ijleo.2022.170344.

[16] P. Escobedo *et al.*, “QRsens: Dual-purpose quick response code with built-in colorimetric sensors,” *Sens Actuators B Chem*, vol. 376, p. 133001, 2023, doi: https://doi.org/10.1016/j.snb.2022.133001.

[17] M. A. Kusuma, P. Sukarno, and A. A. Wardana, “Security System for Digital Land Certificate Based on Blockchain and QR Code Validation in Indonesia,” *ICACNIS 2022 - 2022 International Conference on Advanced Creative Networks and Intelligent Systems: Blockchain Technology, Intelligent Systems, and the Applications for Human Life, Proceeding*, 2022, doi: 10.1109/ICACNIS57039.2022.10055114.

[18] I. Makhdoom, M. Abolhasan, and J. Lipman, “A comprehensive survey of covert communication techniques, limitations and future challenges,” *Comput Secur*, vol. 120, p. 102784, Sep. 2022, doi: 10.1016/J.COSE.2022.102784.

[19] X. Huo and X. Wang, “Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system,” *Results in Engineering*, vol. 20, p. 101589, Dec. 2023, doi: 10.1016/J.RINENG.2023.101589.

[20] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, “FPGA implementation of a chaos-based image encryption algorithm,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9926–9941, Nov. 2022, doi: 10.1016/J.JKSUCI.2021.12.022.

[21] Sucipto *et al.*, “Hidden Treasures of Kediri’s Medicinal Plants: A Collaborative Effort to Map and Validate Authentic Information Using Innovative QR Code Security and Cryptography,” *IOP Conf Ser Earth Environ Sci*, vol. 1242, no. 1, p. 012036, Sep. 2023, doi: 10.1088/1755-1315/1242/1/012036.

[22] Y. Wahyu Agung Prasetyo, R. Rahim, M. A. Manuhutu, and S. Sujito, “QRIS and GOST: A Symbiotic Approach for Secure QR Code Transactions,” *International Journal of Electronics and Communication Engineering*, vol. Volume 10, no. 5, pp. 138–147, May 2023, doi: 10.14445/23488549/IJECE-V10I5P113.

[23] S. Das Mohapatra, S. C. Nayak, S. Parida, C. R. Panigrahi, and B. Pati, “COVTrac: Covid-19 Tracker and Social Distancing App,” *Advances in Intelligent Systems and Computing*, vol. 1299 AISC, pp. 607–619, 2021, doi: 10.1007/978-981-33-4299-6_50.

[24] G. Xue *et al.*, “ScreenID: Enhancing QRCode Security by Utilizing Screen Dimming Feature,” *IEEE/ACM Transactions on Networking*, vol. 31, no. 2, pp. 862–876, Apr. 2023, doi: 10.1109/TNET.2022.3203044.

[25] T. Yuan, Y. Wang, K. Xu, R. R. Martin, and S. M. Hu, “Two-Layer QR Codes,” *IEEE Transactions on Image Processing*, vol. 28, no. 9, pp. 4413–4428, Sep. 2019, doi: 10.1109/TIP.2019.2908490.

[26] F. Anwar, E. H. Rachmawanto, C. A. Sari, and de Rosal Ignatius Moses Setiadi, “StegoCrypt Scheme using LSB-AES Base64,” *2019 International Conference on Information and Communications Technology, ICOIACT 2019*, pp. 85–90, Jul. 2019, doi: 10.1109/ICOIACT46704.2019.8938567.

[27] A. R. Pathak, S. Deshpande, and M. Panchal, “A secure framework for file encryption using base64 encoding,” *Lecture Notes in Networks and Systems*, vol. 75, pp. 359–366, 2019, doi: 10.1007/978-981-13-7150-9_38/COVER.

[28] A. M. Logunleko, K. B. Logunleko, and O. O. Lawal, “An End-to-End Secured Email System using Base64 Algorithm,” *Int J Comput Appl*, vol. 175, no. 28, pp. 1–6, Oct. 2020, doi: 10.5120/ijca2020920669.

[29] E. S. Selvapriya and L. Suganthi, “Design and implementation of low power Advanced Encryption Standard cryptocore utilizing dynamic pipelined asynchronous model,” *Integration*, vol. 93, p. 102057, Nov. 2023, doi: 10.1016/J.VLSI.2023.102057.

[30] R. S. Pressman, *Software Enggineering: A Practitioner’s Approach (7th Edition)*. New York: McGraw-Hill, 2010.

[31] K. D. Prasetya, Suharjito, and D. Pratama, “Effectiveness Analysis of Distributed Scrum Model Compared to Waterfall approach in Third-Party Application Development,” *Procedia Comput Sci*, vol. 179, pp. 103–111, 2021, doi: https://doi.org/10.1016/j.procs.2020.12.014.

[32] T. Thesing, C. Feldmann, and M. Burchardt, “Agile versus Waterfall Project Management: Decision Model for Selecting the Appropriate Approach to a Project,” *Procedia Comput Sci*, vol. 181, pp. 746–756, 2021, doi: https://doi.org/10.1016/j.procs.2021.01.227.

[33] M. Bianchi, G. Marzi, and M. Guerini, “Agile, Stage-Gate and their combination: Exploring how they relate to performance in software development,” *J Bus Res*, vol. 110, pp. 538–553, Mar. 2020, doi: 10.1016/J.JBUSRES.2018.05.003.

[34] S. Pradhan and V. Nanniyur, “Large scale quality transformation in hybrid development organizations – A case study,” *Journal of Systems and Software*, vol. 171, p. 110836, Jan. 2021, doi: 10.1016/J.JSS.2020.110836.

[35] M. Gilsing, J. Pelay, and F. Hermans, “Design, implementation and evaluation of the Hedy programming language,” *J Comput Lang*, vol. 73, p. 101158, 2022, doi: https://doi.org/10.1016/j.cola.2022.101158.

[36] H. Zhang, X. Hu, J. Li, and H. Guan, “A comprehensive test framework for cryptographic accelerators in the cloud,” *Journal of Systems Architecture*, vol. 113, p. 101873, 2021, doi: https://doi.org/10.1016/j.sysarc.2020.101873.

[37] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, “Cryptography Algorithms for Enhancing IoT Security,” *Internet of Things*, vol. 22, p. 100759, 2023, doi: https://doi.org/10.1016/j.iot.2023.100759.

[38] S. M. Wadi and N. Zainal, “Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption,” *Procedia Technology*, vol. 11, pp. 51–56, 2013, doi: https://doi.org/10.1016/j.protcy.2013.12.161.

[39] M. Bedoui, H. Mestiri, B. Bouallegue, B. Hamdi, and M. Machhout, “An improvement of both security and reliability for AES implementations,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, Part B, pp. 9844–9851, 2022, doi: https://doi.org/10.1016/j.jksuci.2021.12.012.

[40] F. Merchan, K. Contreras, R. A. Gittens, J. R. Loaiza, and J. E. Sanchez-Galan, “Deep metric learning for the classification of MALDI-TOF spectral signatures from multiple species of neotropical disease vectors,” *Artificial Intelligence in the Life Sciences*, vol. 3, p. 100071, 2023, doi: https://doi.org/10.1016/j.ailsci.2023.100071.

[41] D. M. A. Cortez, A. M. Sison, and R. P. Medina, “Cryptographic Randomness Test of the Modified Hashing Function of SHA256 to Address Length Extension Attack,” in *Proceedings of the 2020 8th International Conference on Communications and Broadband Networking*, in ICCBN ’20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 24–28. doi: 10.1145/3390525.3390540.

[42] S. D. Sanap and V. More, “Performance Analysis of Encryption Techniques Based on Avalanche effect and Strict Avalanche Criterion,” in *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, 2021, pp. 676–679. doi: 10.1109/ICSPC51351.2021.9451784.

[43] F. A. C. Parapat, G. P. Kusuma, and M. R. N. Majiid, “Automation testing using silk test workbench for website,” *Procedia Comput Sci*, vol. 216, pp. 128–135, 2023, doi: https://doi.org/10.1016/j.procs.2022.12.119.

[44] S. Massaro *et al.*, “Surveying volcanic crises exercises: From open-question questionnaires to a prototype checklist,” *Journal of Volcanology and Geothermal Research*, vol. 440, p. 107850, 2023, doi: https://doi.org/10.1016/j.jvolgeores.2023.107850.

[45] P. Quifer-Rada, L. Aguilar-Camprubí, I. Gómez-Sebastià, A. Padró-Arocas, and D. Mena-Tudela, “Spanish version of the mHealth app usability questionnaire (MAUQ) and adaptation to breastfeeding support apps,” *Int J Med Inform*, vol. 174, p. 105062, 2023, doi: https://doi.org/10.1016/j.ijmedinf.2023.105062.

[46] T. Yamashita, “Analyzing Likert scale surveys with Rasch models,” *Research Methods in Applied Linguistics*, vol. 1, no. 3, p. 100022, 2022, doi: https://doi.org/10.1016/j.rmal.2022.100022.

[47] K. Anjaria, “Knowledge derivation from Likert scale using Z-numbers,” *Inf Sci (N Y)*, vol. 590, pp. 234–252, 2022, doi: https://doi.org/10.1016/j.ins.2022.01.024.

[48] O. Leßenich and S. Sobernig, “Usefulness and usability of heuristic walkthroughs for evaluating domain-specific developer tools in industry: Evidence from four field simulations,” *Inf Softw Technol*, vol. 160, p. 107220, 2023, doi: https://doi.org/10.1016/j.infsof.2023.107220.

[49] R. Silva, A. C. Lima, E. Andrade, A. I. Martins, and N. P. Rocha, “Heuristic Evaluation of the Usability of a Mechanical Ventilator Interface through a Simulator,” *Procedia Comput Sci*, vol. 219, pp. 1232–1239, 2023, doi: https://doi.org/10.1016/j.procs.2023.01.406.

[50] J. Memon, M. Sami, R. A. Khan, and M. Uddin, “Handwritten Optical Character Recognition (OCR): A Comprehensive Systematic Literature Review (SLR),” *IEEE Access*, vol. 8, pp. 142642–142668, 2020, doi: 10.1109/ACCESS.2020.3012542.

[51] S. D. Sanap and V. More, “Performance analysis of encryption techniques based on avalanche effect and strict avalanche criterion,” *2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021*, pp. 676–679, May 2021, doi: 10.1109/ICSPC51351.2021.9451784.

[52] N. Ahmad and S. M. R. Hasan, “A new ASIC implementation of an advanced encryption standard (AES) crypto-hardware accelerator,” *Microelectronics J*, vol. 117, p. 105255, Nov. 2021, doi: 10.1016/J.MEJO.2021.105255.

[53] F. R. Willett, D. T. Avansino, L. R. Hochberg, J. M. Henderson, and K. V. Shenoy, “High-performance brain-to-text communication via handwriting,” *Nature 2021 593:7858*, vol. 593, no. 7858, pp. 249–254, May 2021, doi: 10.1038/s41586-021-03506-2.

[54] D. Upadhyay, N. Gaikwad, M. Zaman, and S. Sampalli, “Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications,” *IEEE Access*, vol. 10, pp. 112472–112486, 2022, doi: 10.1109/ACCESS.2022.3215778.

[55] X. Huo and X. Wang, “Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system,” *Results in Engineering*, vol. 20, p. 101589, Dec. 2023, doi: 10.1016/J.RINENG.2023.101589.

[56] S. Ariyani, M. Sudarma, and P. A. Wicaksana, “Analysis of Functional Suitability and Usability in Sales Order Procedure to Determine Management Information System Quality,” *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 5, no. 2, pp. 234–248, Aug. 2021, doi: 10.29407/INTENSIF.V5I2.15537.

[57] M. Yunus, I. S. Sakkinah, U. E. Rahmawati, A. Deharja, and M. W. Santi, “Electronic Health Records (EHR) Usability and User Experience Evaluation: A Case Study,” *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 7, no. 2, pp. 192–201, Aug. 2023, doi: 10.29407/INTENSIF.V7I2.19090.

[58] I. Wahyudi, Syahrullah, D. S. Anggreni, and R. Laila, “Implementation Aes-128 Encryption For Enhanced Data Security In Central Sulawesi Provincial Inspectorate,” *Advance Sustainable Science Engineering and Technology*, vol. 6, no. 3, pp. 0240302–0240302, Jun. 2024, doi: 10.26877/ASSET.V6I3.560.