Bistek 412

by Turnitin cek

Submission date: 18-May-2026 01:30PM (UTC+0800)
Submission ID: 2957839394
File name: Bistek_421_-_Similarity--.docx (1,016.57K)
Word count: 2675
Character count: 16271

Implementation Of Aes Algorithm With Data Encryption On Student Attendance For Information Security At One Of The Vocational High Schools In Bandung

ABSTRACT

The digital attendance system in educational institutions has streamlined the documentation of student attendance; however, many systems lack robust data security measures, leaving them susceptible to unauthorized access and manipulation. This study seeks to enhance data security in the student attendance system at a vocational high school in Bandung by implementing the Advanced Encryption Standard (AES-256) algorithm. The system is developed with the Waterfall methodology, encompassing the phases of analysis, design, implementation, and testing. The AES algorithm is used to encrypt sensitive data, including student identification numbers (NIS) and attendance records, prior to their storage in the database. The research findings indicate that the encrypted data is maintained as ciphertext, inaccessible without the decryption key, and does not impair system performance.

Keywords: AES, Encryption, Attendance System, Information Security, Waterfall

INTRODUCTION

Attendance is a vital component in education, providing a foundation for assessing student discipline and informing academic decisions. The digital attendance system greatly facilitates data processing, but without sufficient data security measures, the information is susceptible to unauthorized access. A vocational high school in Bandung has established a web-based attendance system but has not yet employed data protection measures such as encryption.

A system consists of a collective of humans collaborating consistently under established protocols to create a cohesive entity that performs designated activities to attain shared objectives (Kumar et al., 2020). In the context of attendance, absenteeism or presence refers to the act of documenting an individual's presence or absence at a specific location or during a scheduled activity, such as in the workplace or other settings (Sunil et al., 2020)To ensure information security, engineers employ the Advanced Encryption Standard (AES), a symmetric cryptographic algorithm for data protection that operates in multiple modes, including ECB, CBC, CFB, and OFB (Santoso et al., 2020). The encryption process converts original data (plaintext) into an unreadable format (ciphertext) without a designated key, thus safeguarding data against breaches or interception during storage or

transmission. In a membership information system, encryption protects sensitive data—such as identity numbers, addresses, and financial records—from unauthorized access. AES provides substantial security resilience due to its mathematical structure, which complicates traditional cryptanalysis (Khudair et al., 2023). Conversely, decryption reverses encryption by transforming ciphertext into plaintext using a legitimate key, which only authorized individuals can utilize to maintain data confidentiality; in membership systems, decryption generally transpires when administrators or authorized members retrieve encrypted data, such as during identity verification or when presenting personal information on the application dashboard (Hafsa et al., 2021).

The Unified Modeling Language (UML) in software engineering is a standardized language for creating visual diagrams that depict a software system, serving as a blueprint to enhance system understanding and design. UML is an essential tool for software engineers and system analysts, as proficiency in its fundamental concepts and diagrams enables the development of superior, more comprehensible, and easier-to-maintain systems (Priya et al., 2022). A fundamental element of UML is the use case diagram, which visually illustrates actors, use cases, and their interrelationships within a system. This research identifies four principal procedures performed within the forthcoming information monitoring system (Silfani, 2025). A crucial UML tool is the class diagram, with three elements: the middle component that contains all actions, while the top and bottom components contain attributes only (Shukur et al., 2023)). An activity diagram delineates system activities as a sequential series of actions, encompassing action initiation, possible decision points, and action termination; it can also depict processes with multiple concurrent actions and visualize objects, states, state transitions, and events (Adeniyi et al., 2023). A sequence diagram illustrates interactions among objects within a use case by presenting the chronological order of events and exchanged messages; each sequence diagram must encompass a use case definition with a distinct process, indicating that an increase in the number of use cases requires the development of supplementary sequence diagrams (Jindal et al., 2020).

This research employs the Advanced Encryption Standard (AES-256) to address current challenges, as it is a robust symmetric encryption method widely used to secure digital data. This study seeks to improve the security of attendance data to safeguard the confidentiality and integrity of information.

RESEARCH METHODS

This study employs a descriptive qualitative research methodology to carefully and precisely outline the development process of a student

attendance system. The study investigates the application of the Advanced Encryption Standard (AES-256) algorithm as a data security measure. The researcher gathered data through direct observation of attendance protocols at SMK Terpadu Ad-Dimyati, interviews with school officials, and the examination of previously used materials or methods. The research findings subsequently serve as the basis for the design and implementation of an attendance system with data encryption capabilities.

The researcher employed interviews, observations, and literature reviews to collect extensive data. The researcher conducted interviews with educators and school officials to gather information about current attendance processes, system requirements, existing limitations, and data security issues in the legacy system. Direct observations focused on the operational attendance system, including attendance recording, data storage, administrative functions, and the detection of issues, particularly related to information security. Simultaneously, the literature review entailed collecting references from books, journals, and relevant earlier research on data security, AES encryption, digital attendance systems, and information system development approaches.

This study employs the Waterfall technique for system development because it is well-suited to systems with well-defined requirements and a systematic development process. The initial phase, Requirement Analysis, delineates system requirements and data security concerns arising from the prior attendance system, while defining both functional and non-functional requirements to ensure the new system performs attendance processes securely and efficiently. The subsequent phase, System Architecture, emphasizes the creation of the system structure, encompassing database schemas, attendance routines, architectural designs, and the incorporation of AES encryption into data storage and retrieval mechanisms. During system execution, the developer creates the system utilizing the PHP programming language, the CodeIgniter framework, and a MySQL database, while implementing the AES-256 algorithm for data input and storage. The System Evaluation stage employs Black-Box Testing to confirm that all system functions perform as specified and that encryption and decryption processes function accurately.

RESULT AND DISCUSSION

The assessment of the current system entails scrutinizing the existing procedures at a vocational high school in Bandung. This phase is crucial, as faults made at this juncture will result in inaccuracies in later stages. This analysis seeks to attain a thorough comprehension of the system to be constructed.

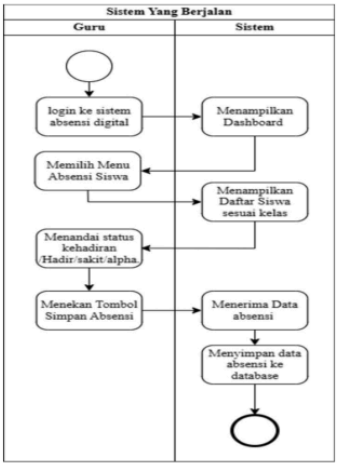


Figure 1. Running system

The figure demonstrates that the former student attendance system at a vocational high school in Bandung operated digitally but lacked data protection measures. As a result, the legacy system retained data, including Student Identification Numbers (NIS) and attendance records, in an unencrypted format. This vulnerability made the material extremely susceptible to unauthorized access, inappropriate alterations, and exploitation by nefarious individuals. Moreover, the database lacked encryption safeguards, thereby substantially increasing the likelihood of data tampering.

The problem-solving analysis indicates that the solution incorporates the Advanced Encryption Standard (AES-256) algorithm into the procedures for storing and retrieving attendance data. The system encrypts the data before storing it in the database. When the system requires data retrieval and presentation, it automatically decrypts the data using a securely stored secret key on the server. Implementing this approach enhances database security by encrypting data, making it much more difficult for unauthorized individuals to access or alter it.

The next phase entails system design, which delineates the workflow, user interfaces, and data processing techniques within the digital attendance application. This system design aims to provide a comprehensive overview of the system's core functionalities before the implementation phase, specifically as a web-based application.



Figure 2. Use Case Diagram

Table 1. Definition of Actor

No	Actor	Description
1	Admin	The party with full authority to manage all system data and functionality. Admins are responsible for recording student data, managing attendance data, and monitoring reports.
No	**Actor**	**Description**
2	Teacher	Parties who interact with the system to view attendance data and student absence reports for the classes or subjects they teach. Teachers do not have the right to add, change, or delete student data.

The Use Case Description delineates the interactions between actors and the system, as well as the system's responses to the actors executing particular functions. This scenario is predicated on the previously developed Use Case Diagram, ensuring that each procedure is meticulously recorded.

Table 2. Use Case Description Login

Use case name	Login
Actor	**Admin / Teacher**
Description	Admin logs in by entering valid credentials to gain access into the system.

Exception	wrong username/password; account not registered; connection/server failure while processing.
Pre-condition	The user already has a registered account in the system.
Actor	**System**
Normal Scenario	
1. The user opens the login page.	
	2. The system displays the login form.
3. The user enters their email/username and password.	
	4.The system validates the user credentials.
	5. The system directs the user to the dashboard
Post-condition: User successfully logs into the system with access rights according to role.	

Table 3. Use Case Description for Taking Attendance

Use case name	**Taking Attendance**
Actor	**Teacher**
Description	The teacher takes student attendance by marking the attendance status. (Present, Permission, Sick, or Alpha). The data is then encrypted before being saved to the database.
Exception	Connection to server failed; student data not found; error during encryption.
Pre-condition	The teacher has logged into the system.
Actor	System
Normal Scenario	
1. The teacher selects the “Attendance” menu.	
	2. The system displays a list of students in that class.
3. The teacher fills in each student's attendance status.	
4. The teacher presses the “Save” button.	
	5. The system performs data encryptionabsensi menggunakan AES-256.

	6. The system saves the ciphertext to the database.
	7. The system displays the message "Attendance successfully saved."
Post-condition: Data absensi siswa diperbarui sesuai tindakan Admin.	

Activity Diagram Login

This activity diagram depicts the sequence of actions for the administrator or educator during the attendance system login process.

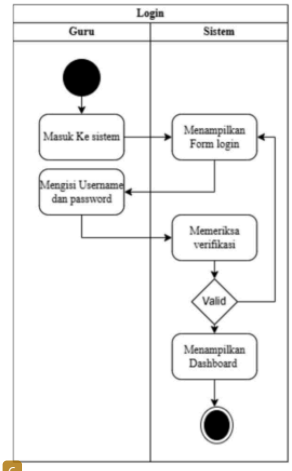


Figure 3. Login Activity Diagram

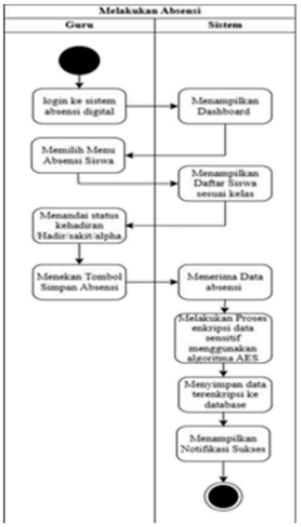


Figure 4. Activity Diagram for Taking Attendance

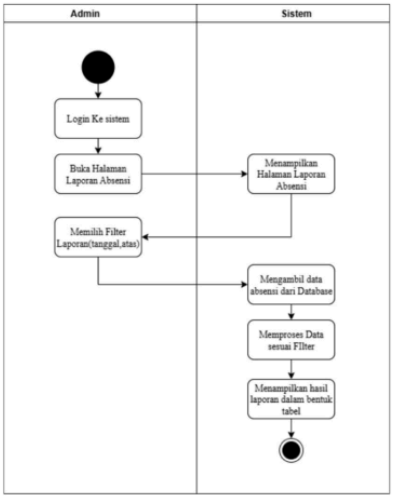


Figure 5. Activity Diagram of Attendance Report

The sequence diagram illustrates the interactions between actors and the system as they execute the process flow for a specific use case. The following is the sequence diagram derived from this research game:

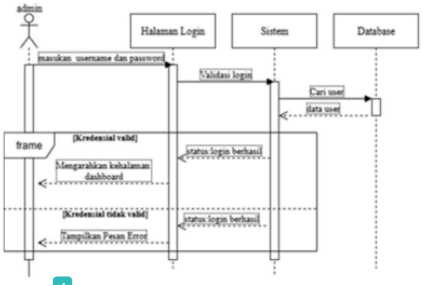


Figure 6. Login Sequence Diagram

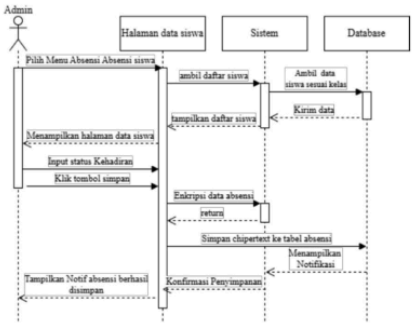


Figure 7. Sequence Diagram for Taking Attendance

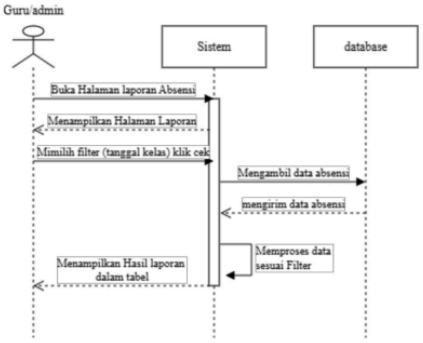


Figure 8. Sequence Diagram of Attendance Report

This class diagram aids in structuring the program before code implementation, ensuring mutual understanding of the system design among developers and stakeholders.

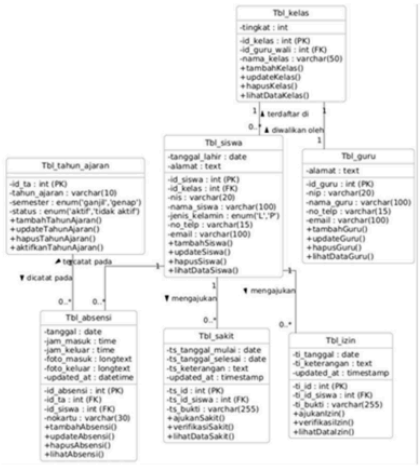


Figure 9. Class Diagram

The table structure design specifies each database attribute, including data types, character lengths, column features, and the function of each column within the interrelations among tables. This table layout acts as a guide for establishing the MySQL database within the system.

Student Table

This table is utilized to retain comprehensive information for each student.

Table 4. Student table structure

Field Name	Data Type	Long	Information
student ID	int	11	**Primary Key**, ID unik siswa
nis	varchar	20	Student ID Number
student_name	varchar	100	Student's full name
gender	enum('L','P')	-	Gender (Male/Female)
date of birth	date	-	Student's date of birth
address	text	-	Student's residential address
phone number	varchar	15	Student phone number
email	varchar	100	Student email address

class_id	int	11	Foreign Key to tbl_kelas, student class ID

This table is a transactional table that records each student's attendance.

Table 5. Attendance table structure

Field Name	Data Type	Long	Information
id_absensi	int	11	**Primary Key**, ID unik absensi
card number	varchar	30	RFID card number used by students
date	date	-	Absence date
clock_in	time	-	The time when students take attendance
clock_out	time	-	The time when students take attendance
photo_entry	longtext	-	Path or image data when attendance is entered
photo_out	longtext	-	Path or image data when absent out
ta_tta_id	int	11	**Foreign Key to TBQ academic year**
ta_id_ student	int	11	**Foreign Key to tbl_siswa**
updated_at	datetime	-	Last time data was updated

Interface Design

The user interface (UI) design aims to establish a visual framework for the system that is intuitive, efficient, and easy to navigate for all users. The following presents the interface design for the primary pages of the Student Attendance Information System:

Login Page

This page functions as the primary portal to access the system. All users, encompassing administrators, educators, and students, will access the system via this page by entering their individual credentials.

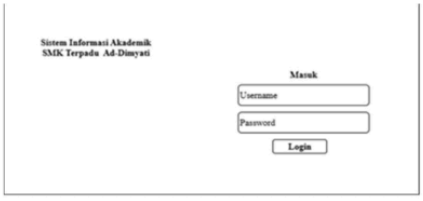


Figure 10. Login Page

This page enables administrators and educators to access and filter student attendance reports by class and date period. Engineered for utility, it provides multiple filters to produce tailored reports tailored to user requirements.

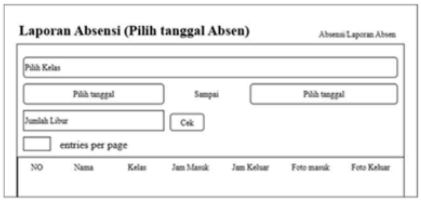


Figure 11. Attendance Report

This feature is the attendance report data export tool, which allows users to extract data in multiple formats. It is intended to facilitate administrative requirements and academic records.

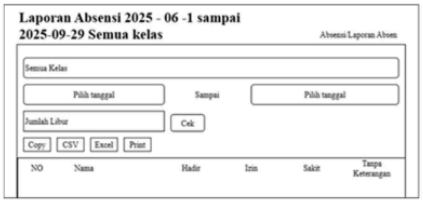


Figure 12. Export attendance report

Database Implementation

A specific interface was developed to directly retrieve data from the database, ensuring that security mechanisms function as intended. This interface displays the contents of the tbl_student table, emphasizing columns that hold sensitive information, such as student identity numbers and card numbers.

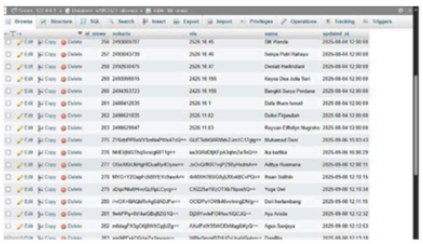


Figure 13. Display of student data in the database

The implementation step of the interface involves executing all the established interface designs. At this step, the visual designs (mockups) and system workflow are converted into functional, interactive, and responsive web pages.

Login Page: This page functions as the primary access portal for administrators and educators to enter the system. The implementation corresponds with the design, featuring fields for the username and password, as well as a login button for authentication.

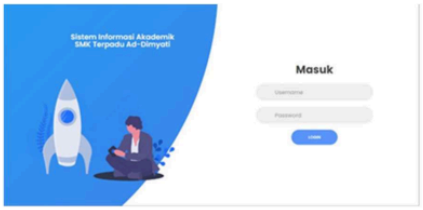


Figure 14. Implementation of the login page

This page generates and displays student attendance summaries. The implementation provides filtering capabilities by class and date range, enabling administrators or educators to generate targeted reports as needed. The report's findings are presented in a simple, organized tabular format.

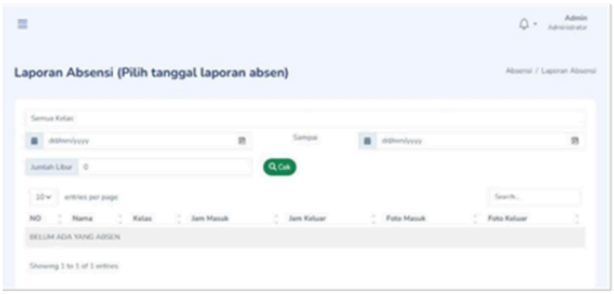


Figure 15. Implementation of attendance report

This section highlights the crucial report export functionality. You can download student attendance data for the designated dates here. Diverse format options, including CSV and XLSX, facilitate data analysis through spreadsheet software such as Microsoft Excel. Furthermore, you may print the report directly using the print option. This method grants you complete authority over the attendance records.

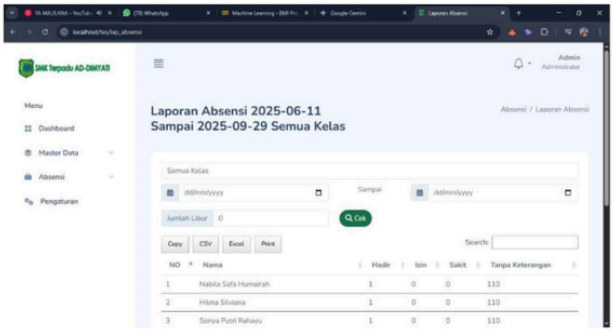


Figure 16. Implementation of student data export

Functional testing seeks to validate the accuracy of the AES encryption and decryption procedures, particularly the algorithm's capacity to convert plaintext into ciphertext and subsequently return it to the original plaintext without errors. This testing acts as a primary validation of the algorithm's implementation, with the methods outlined as follows:

1) Test Data: Employing a representative sample that encompasses diverse attendance data types, including Student Identification Numbers (NIS) and card numbers.

2) Procedure: Each test data element is encrypted and subsequently decrypted without delay.

3) Validation: Assessing the original plaintext against the decryption outcome.

Functional Validation Formula

$$\text{Success Rate} = \sum_{i=1}^{n} \delta(P_i, D(E(P_i))) n \times 100\%$$

Information:

1) Pi= Plaintext ke-ii

2) E(Pi) = Ciphertext hasil enkripsi PiPi

3) D(E(Pi))= Ciphertext decryption results

4) n = Number of test samples

5) δ = Kronecker Delta function for exact comparison

Table 6. Functional test results

No	Data Types	Plaintext	***Ciphertext*** (16-	**Decryption Results**	**Status**
1	Student ID	202411001	3f7a84c1…e9b2	202411001	✅ **Valid**

2	Card Number	0001234567	8c2e91f4…d5a7	0001234567	✅ **Valid**

CONCLUSION

The deployment of the AES-256 algorithm in the digital attendance system at a vocational school in Bandung has effectively improved the security of student attendance data. The encryption and decryption operations function with complete precision and attain a rapid performance of less than 2 milliseconds per data entry. The security test outcomes, including database evaluations, avalanche effect assessments, and entropy analyses, demonstrate that the ciphertext is random and difficult to alter, thereby enhancing the system's security and reliability.

It is advisable to enhance the system by incorporating teacher and staff attendance, thereby establishing a comprehensive attendance platform. Furthermore, implementing automatic notification systems for parents through WhatsApp or email can enhance real-time oversight of student conduct.

REFERENCES

© 20XX

Bistek 412

ORIGINALITY REPORT

4%	2%	1%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to NCC Education Student Paper	1%
2	policy.un.org Internet Source	1%
3	Submitted to Trine University Student Paper	1%
4	Submitted to University of Westminster Student Paper	<1%
5	elib.pnc.ac.id Internet Source	<1%
6	journal.admi.or.id Internet Source	<1%
7	Castro, Ivo Loureiro. "Enhancing Health and Fitness: A Hybrid Recommender System.", Instituto Politecnico do Porto (Portugal) Publication	<1%
8	comyuno.com Internet Source	<1%
9	Galih Wening Werdi Mukti, Hermawan Setiawan. "Designing and Building Secure Electronic Medical Record Application by Applying AES-256 and RSA Digital Signature",	<1%

IOP Conference Series: Materials Science and Engineering, 2020

Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		