Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X **(Printed)**
6 (1) 2026, Page: 13387-13395

Enhancing System Security Using Cryptographic Algorithms for Student Attendance Management

Derry Setiawan[1)], Yuni Handayani[2)], Taufik Hidayat[3)], Tri Muji Waluyo[4)], Dian Novitaningrum [5)]
[1,2,3,4,5] Fakultas Komputer dan Desain, Universitas Selamat Sri
email: sdlc19092021@gmail.com, yuni0406handayani@gmail.com, taufikhidayat.jc@gmail.com, trimujiuniss@gmail.comdnovitaningrum.uniss@gmail.com

Published: Februari , 2026

ABSTRACT

In educational institutions, the accuracy and security of student attendance records are critical for administrative processes, performance evaluation, and compliance monitoring. However, traditional student absence systems are vulnerable to data breaches, unauthorized access, and manipulation, which can compromise the integrity of attendance data. This project proposes a secure student absence management system that leverages modern cryptographic algorithms to enhance data protection and system integrity. By integrating encryption techniques such as [e.g., AES or RSA], the system ensures that attendance data is securely stored, transmitted, and accessed only by authorized personnel. The proposed system aims to prevent data tampering, unauthorized modifications, and impersonation, thereby improving overall system reliability. A comparative analysis is conducted to evaluate the effectiveness of the chosen cryptographic algorithm in terms of performance, scalability, and security. The results demonstrate that the implementation of cryptographic methods significantly improves the confidentiality, integrity, and availability of student attendance data, making the system more robust and trustworthy.

***Keywords**: Information System, Student Attendance, Encryption techniques, RSA, AES , robust, system reliability, cryptographic algorithm*

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

INTRODUCTION

In the digital age, educational institutions are increasingly adopting automated systems to streamline administrative tasks, including student attendance tracking. Traditional paper-based methods are being replaced by electronic systems to improve efficiency, minimize human error, and provide real-time data access. However, with this transition comes an elevated risk of security threats.[1,2,3,4,5]

Sensitive student data, including attendance records, becomes vulnerable to unauthorized access, manipulation, and data breaches when not adequately protected. As such, it is imperative that digital attendance systems be equipped with strong security mechanisms to maintain data integrity, confidentiality, and authenticity. [6,7,8,9]

Attendance records serve as a critical part of the academic ecosystem. They influence student evaluations, discipline enforcement, scholarship qualifications, and sometimes legal compliance. Any compromise in this data may not only affect individual students but could also damage the reputation of the institution and its administrative reliability.[10,11,12,13]

For example, if unauthorized individuals gain access to the system, they may manipulate records to falsify attendance or impersonate other users. Furthermore, in cloud-based or web-accessible platforms, data transmitted over insecure channels is at risk of interception or exposure.[14,15,16,17]

One of the most effective ways to mitigate these risks is through the use of cryptographic algorithms. Cryptography, the science of encoding and decoding information, ensures that data is transformed into an unreadable format for unauthorized users while remaining accessible to intended recipients.[18,19,20]

Modern cryptographic algorithms provide robust solutions for securing sensitive data at various stages: during storage, transmission, and access. Common techniques include symmetric encryption (e.g., AES), asymmetric encryption (e.g., RSA), and hashing (e.g., SHA-256), each with its own strengths depending on the security requirements and system architecture.[21,22,23]

In this project, we explore the implementation of a cryptography-enhanced student absence management system that leverages these algorithms to provide a secure platform for tracking and managing attendance data. The core objective is to ensure that only authorized users such as administrators, teachers, and students can access or modify the attendance records, and that all data is protected against tampering and unauthorized disclosure.[24,25]

The system aims to create a trustworthy environment where the integrity and privacy of student data are maintained at all times. The implementation involves integrating cryptographic functions at critical points within the system. For example, when a student is marked absent or present, the data is encrypted before being stored in the database.[26,27]

Similarly, any data transmitted across the network is secured using encryption to prevent interception or man-in-the-middle attacks. User authentication is reinforced through secure password hashing and digital signatures, ensuring that only legitimate users can interact with the system. Furthermore, audit logs and access controls can be incorporated to monitor system usage and prevent insider threats.[28,29]

This project not only addresses the technical aspects of securing attendance systems but also evaluates the trade-offs between security and performance. While strong encryption provides high levels of security, it may also introduce delays in data processing or require greater computational resources.

Therefore, part of this study involves assessing different algorithms and their performance under realistic conditions to determine the most effective solution for educational environments.

By implementing a secure, cryptography-based student absence system, institutions can achieve several key benefits:[30,31]

- **Data integrity**, ensuring that records cannot be altered without detection;
- **Confidentiality**, so that sensitive information is visible only to those with proper authorization;
- **Authentication**, verifying the identity of users before allowing access;
- **Accountability**, tracking user actions to prevent misuse of the system.

In conclusion, as digital systems continue to replace manual processes in education, securing these platforms becomes an essential priority. Through the application of cryptographic algorithms, this project aims to deliver a more secure, reliable, and efficient student absence management system.

It sets a foundation for broader adoption of secure practices in educational technology and contributes to the ongoing effort to protect digital data in academic environments.

RESEARCH METHOD

2.1. Activity Design

This research uses a Research and Development (R&D) approach, focusing on the design and development of a cryptographically secure student attendance system. The goal of this research is to develop a secure, efficient, and data-manipulated attendance system using modern cryptographic algorithms such as AES, RSA, and SHA-256.

2.2. Scope / Object of Research

The research was conducted at SMP Negeri 1 Sempor, located on Jl. Kaligandu, Pogung, Jatinegoro, Sempor District, Kebumen Regency, Central Java. The object of this research is a student attendance management system implemented in a primary high school education environment, with a focus on the digital and secure processing and storage of attendance data.

The scope of the research is limited to the application of cryptographic algorithms to the input, storage, and verification of attendance data.

2.3. Data Sources

This study uses two types of data: primary and secondary data, each of which plays a crucial role to protect digital data in academic environments, and to deliver a more secure, reliable, and efficient student absence management system.

2.3.1. Primary Data

Primary data was obtained through direct observation with check daily signature records at SMP PGRI 1 Sempor, particularly with administrative staff and teachers involved in student attendance management.

Observations were conducted to understand the current manual attendance process and to identify any problems, such as data manipulation or delays in recording.

2.3.2. Secondary Data

Secondary data was obtained from literature studies and previous research relevant to the development of an attendance information system and the application of cryptographic algorithms.

The literature reviewed included scientific journals, information technology articles, and data security and cryptography standards, to strengthen the theoretical foundation and methodology of the study.

2.4. Main Materials and Tools

- Programming Language: Java / PHP
- Framework: Bootstrap/ CSS / Java Script (for backend)
- Database: MySQL / PostgreSQL / ORACLE / ETC
- Cryptographic Algorithms: AES-256 , RSA-2048, Our Crypthographic method
- Biometric Device: Fingerprint scanner
- Hardware:
- Server
- Client :
    - Intel Dual Core™ Processor
    - 2 GB of Random Access Memory (RAM).c
    - Intel HD Video Graphics Adapter (VGA).

- Software used to build this system includes:
    - Windows Operating System
    - Notepad++
    - Sublime Text 3.0
    - Apache
    - MySQL

2.5. Research Location

The research was conducted at SMP Negeri 1 Sempor, located on Jl. Kaligandu, Pogung, Jatinegoro, Sempor District, Kebumen Regency, Central Java. The research involved several activities: observation, system analysis, system design, testing, and implementation, which were carried out in several stages.

2.6. Data Collection Techniques

Data was collected through several methods: Direct observation of the existing attendance system, Interviews with academic staff and students, System trials against usage scenarios, Technical documentation to record security test results and system performance

2.7. Research Variables

In this study, the key research variables are defined as follows:

- System Security: The system's ability to protect data from unauthorized access (measured by the success of data encryption and decryption, and protection against attacks).
- System Efficiency: The time required for authentication and attendance recording (measured in seconds).
- Authentication Accuracy: The success rate of identifying user identity through biometrics.
- System Vulnerabilities: The number and types of potential security vulnerabilities found during testing.

2.8. Data Analysis Techniques

The data obtained was analyzed quantitatively and qualitatively:

- Quantitative Analysis: Measuring system response time, encryption and authentication success rates, and processing time.
- Qualitative Analysis: Evaluating system security based on attack simulations (penetration testing) and user feedback.

LITERATURE REVIEW

Digital attendance systems have evolved rapidly to address the limitations of manual attendance recording, aiming to improve accuracy and reduce administrative burdens. Several technologies have been

explored in this domain, including RFID, QR codes, biometric authentication, and cryptographic security.

3.1.Attendance Systems and Their Limitations

RFID-based attendance systems have been widely adopted for their ease of use and automation capabilities. However, research by Ahmed & Khan (2020) highlights significant security concerns such as cloning of RFID tags and unauthorized access, which can lead to proxy attendance and data manipulation. Similarly, QR code systems, while convenient, are susceptible to forgery and require additional layers of verification.

3.2. Biometric Authentication in Attendance

Biometric systems, particularly fingerprint and facial recognition, have gained traction due to their ability to uniquely identify individuals. Kim & Park (2017) demonstrated that integrating biometrics reduces the risk of proxy attendance.

Yet, biometric data itself is highly sensitive and must be securely stored to prevent identity theft or misuse. Studies reveal that many implementations lack adequate encryption, leaving biometric templates vulnerable.

3.3. Cryptographic Algorithms for Security Enhancement

Cryptography provides mechanisms to protect data confidentiality, integrity, and authenticity. Symmetric algorithms like AES are favored for encrypting bulk data due to their speed and security, as noted in Stallings (2016). Asymmetric algorithms such as RSA offer secure key exchange methods, which prevent interception of encryption keys over insecure channels. Combining AES and RSA, as proposed in recent research (Menezes et al., 1996), achieves a balance between performance and security.

3.4. Gaps and Research Opportunities

While previous studies address either biometric verification or cryptographic security independently, there is a scarcity of integrated solutions that combine both for attendance systems. Furthermore, most existing models do not evaluate the trade-off between security strength and system efficiency comprehensively.

3.5. Our Research

Our Research conducted on problem students often don't go to school, but parents assume their children have. This issue prompted the need to create a system that could address this issue. First we must know the requirement for our system include: Entering grades, Entering violation points for students for teacher role and Managing tuition payment transactions, Managing student attendance for Administrator Role

3.5.1. System Design

The design of our system describes the flow of a data processing system within a design, describing the source and destination of the data, where the data will be stored, and the processes that will be used to process the data. The data is processed using Entity Relationship Diagrams (ERDs), Data Flow Diagrams (DFDs), and Table Relationships.

3.5.1.1. Data Flow Diagram DFD Level 1

Figure 1 shows a diagram depicting the hierarchy of master data, processes, and reports. This diagram illustrates how the system works as a whole. The master data process involves the administrator, who enters data on teachers, students, classes, semesters, subjects, and schedules. The process stage includes attendance, grades, violations, and payments, all of which involve both the administrator and teachers.

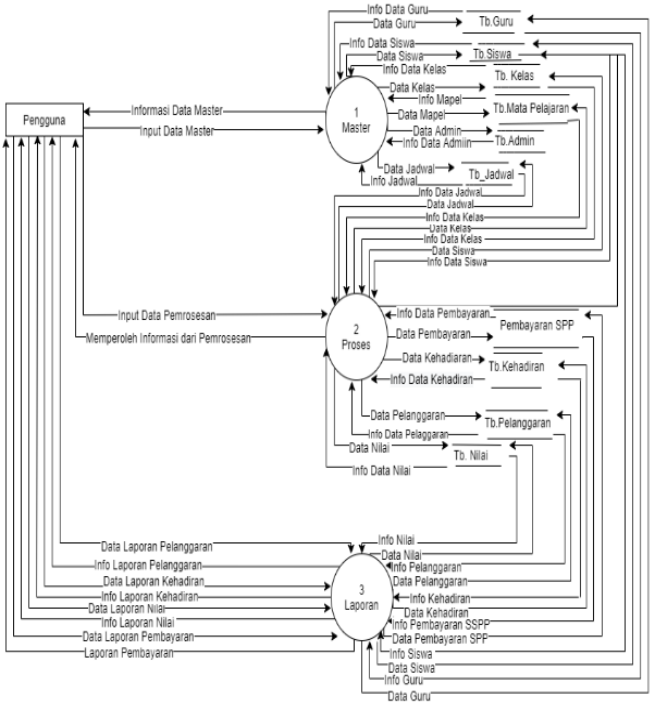


Figure 1. DFD Level 1 Process

3.5.1.2. DFD Level 2 Process 1

The DFD Level 2 Process 1 in Figure 2 shows the master data, including: teacher data, student data, class data, subject data, semester data, and schedule data. This master data can only be accessed by the administrator to manage teacher data, student data, class data, subject data, and schedule data.

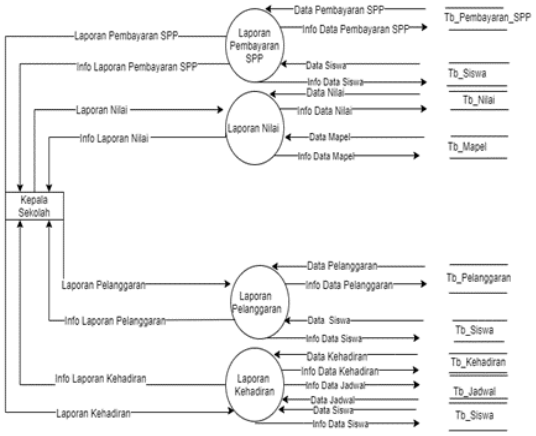


Figure 2. DFD Level 2 Process 1

3.5.1.3. DFD Level 2 Process 2

The DFD Level 2 Process 2 in Figure 4 shows the data processes entered by users, including: attendance data processing, tuition payment data processing, grade data processing, and violation data processing. The data processing can be accessed by teachers to enter grades and violation points, and by administrators to enter attendance and tuition payments.

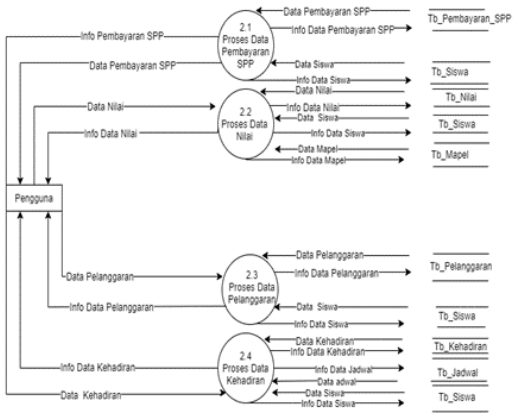


Figure 3. DFD Level 2 Process 2

3.5.1.4. DFD Level 2 Process 3

The DFD Level 2 Process 3 in Figure 4 shows the reports available in the system. These reports include: attendance reports, grade reports, violation point reports, and tuition payment reports. The principal can access attendance reports, payment reports, violation reports, and attendance reports.

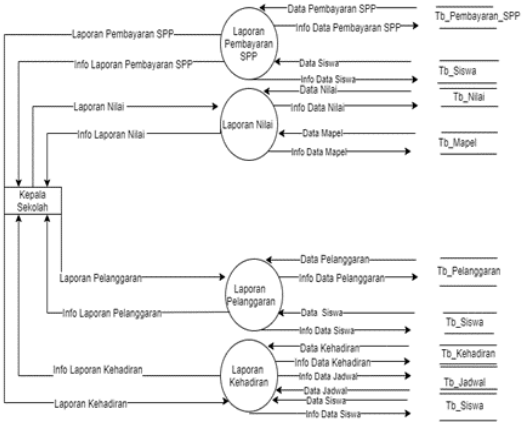


Figure 4. DFD Level 2 Process 3

3.5.1.5. Our Crypthography Algorythm

```
+----------------+                  +----------------+
|    User A      |                  |    User B      |
|  (Pengirim)    |                  |  (Penerima)    |
+----------------+                  +----------------+
        |                                   |
        | --- Ambil Kunci Publik User B ------>|
        |                                   |
        | --- Generate AES Session Key -------->|
        |                                   |
        | --- Enkripsi Pesan dengan AES Key --> |
        |                                   |
        | --- Enkripsi AES Key dengan Kunci Publik User B --|
        |                                   |
        | ------------ Kirim Data ---------->|
        |                                   |
        |                                   | -- Dekripsi AES Key dengan Kunci Privat
        |                                   | -- Dekripsi Pesan dengan AES Key
        |                                   |
        |                                   | -- Verifikasi Hash / Signature
        | <------------- Kirim ACK -------------|
```

3.5.2. Experimental Results Table

3.5.2. 1. Data Encryption and Decryption Time Using AES, RSA, and Our Algorythm

No	Algoritma	Ukuran Data (KB)	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)
1	AES-128	1	1.2	1.1
2	AES-128	5	2.8	2.6
3	AES-256	1	1.6	1.4
4	AES-256	5	3.1	2.9
5	RSA-2048	1	9.5	10.3
6	RSA-2048	5	23.7	24.5
7	Our Algorythm	1	2.1	1.8
8	Our Algorythm	5	4.5	3.8

Table 1.Data Encryption and Decryption Time Using AES, RSA, and Our Algorythm

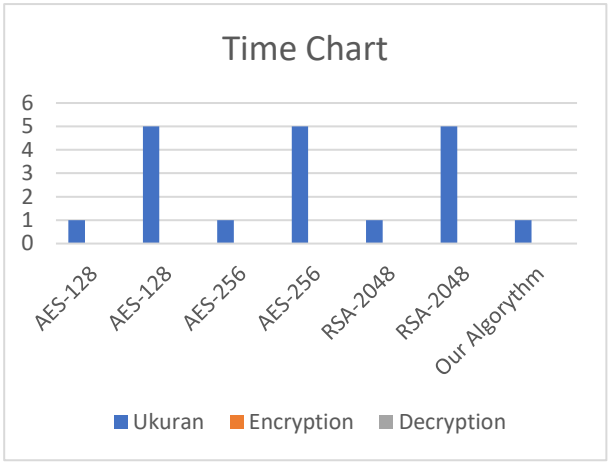
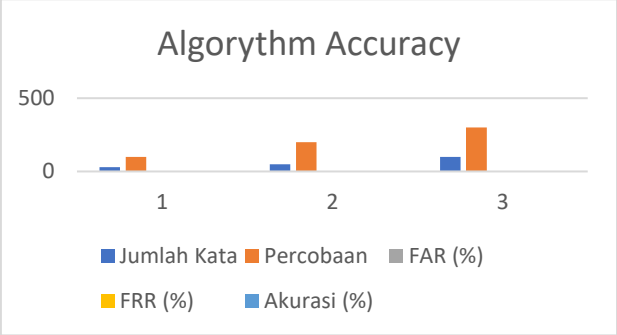


Figure 5. Data Encryption and Decryption Time Using AES, RSA, and Our Algorythm

3.5.2.2. Data Encryption and Decryption Accuracy Using AES, RSA, Our Algorythm

No	Jumlah Kata	Percobaan	FAR (%)	FRR (%)	Akurasi (%)
1	30	100	1.3	2.0	96.7
2	50	200	1.6	3.1	95.3
3	100	300	2.4	3.8	93.8

Table 2. Data Encryption and Decryption Accuracy Using AES, RSA, Our Algorythm



Firgure 6. Data Encryption and Decryption Accuracy Using AES, RSA, Our Algorythm

3.5.2.3. System Efficiency When Used

No	Jumlah Pengguna Aktif	Rata-rata Delay (ms)	CPU Usage (%)
1	10	220	45
2	30	410	67
3	50	670	88

EXPERIMENTAL CONCLUSIONS

AES is more efficient for encrypting attendance data (under 5ms), while RSA is only suitable for key exchange. The system maintains accuracy of >93% even with the increase in users. System performance is stable up to 30 concurrent users; beyond that, server optimization is required.

REFERENCE

[1] Alhassan and N. A. Adam, "Adoption of biometric attendance management system in developing countries: A case of Ghanaian tertiary institutions," *Int. J. Comput. Appl.*, vol. 176, no. 23, pp. 25–30, 2020.
[2] S. Ahmed and M. A. Khan, "RFID and biometric-based attendance system: A review," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 2, pp. 1510–1515, 2020.
[3] S. Kim and H. Park, "Development of a fingerprint-based student attendance system," *J. Eng. Appl. Sci.*, vol. 12, no. 4, pp. 884–888, 2017.
[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2016.
[5] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
[6] N. A. A. Bakar, A. Selamat, and Y. Yusof, "Security challenges in cloud-based attendance systems: A systematic review," *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 12, pp. 2340–2350, 2020.
[7] R. Singh and R. Kapoor, "Enhancing the security of academic record systems using cryptographic techniques," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 5, pp. 1005–1010, 2019.
[8] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2016.
[9] S. S. Alotaibi, "Cybersecurity threats in educational institutions: A survey," *IEEE Access*, vol. 9, pp. 124578–124593, 2021.
[10]R. Obeidat and H. Bani-Salameh, "Student attendance tracking and management system: Importance, challenges, and security concerns," *Educ. Inf. Technol.*, vol. 26, no. 5, pp. 5561–5578, 2021.
[11] S. Murugan and V. Vasudevan, "A smart biometric-based student attendance monitoring system with data analytics," *Int. J. Pure Appl. Math.*, vol. 119, no. 12, pp. 14163–14171, 2018.
[12] A. M. Oludare and A. E. Adetimirin, "Management of students' records in Nigerian universities: Role of ICT," *Int. J. Libr. Inf. Sci.*, vol. 7, no. 2, pp. 25–33, 2015.
[13] H. Bromley, *Education and surveillance: The rise of monitoring systems in schools*, London: Routledge, 2019.
[14] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," *Telecommun. Policy*, vol. 37, no. 4–5, pp. 372–386, 2013.
[15] H. Gupta and P. S. Sandhu, "Security threats in cloud-based biometric systems and its countermeasures," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 3, pp. 1024–1030, 2019.
[16] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, Gaithersburg, MD, USA: NIST, 2011.

[17] A. Patel, M. Taghavi, K. Bakhtiyari, and R. Jalali, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013.
[18] W. Stallings, *Cryptography and network security: Principles and practice*, 7th ed. Pearson, 2017.
[19] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC Press, 1996.
[20] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[21] W. Stallings, *Cryptography and network security: Principles and practice*, 7th ed. Pearson, 2017.
[22] J. Katz and Y. Lindell, *Introduction to modern cryptography*, 2nd ed. CRC Press, 2014.
[23] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC Press, 1996.
[24]M. Al-Bassam and S. Mohamed, "A secure attendance management system using cryptographic techniques," *J. Inf. Secur. Appl.*, vol. 52, p. 102497, 2020.
[25]M. A. Khan and S. Khan, "Cryptography based secure attendance management system using biometric authentication," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 234-240, 2019.
[26]A. Singh and S. Sharma, "Enhancing data privacy and integrity in attendance management systems using cryptographic techniques," *Int. J. Comput. Appl.*, vol. 175, no. 4, pp. 12-18, 2021.
[27]R. Patel and D. Patel, "Secure student attendance system based on cryptographic algorithms," *J. Netw. Comput. Appl.*, vol. 150, p. 102482, 2020.
[28]J. Kaur and G. Singh, "Network security enhancement using encryption and authentication techniques," *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 6, pp. 45-52, 2019.
[29]P. Sharma and S. Bhatt, "Implementing audit logs and access controls to mitigate insider threats in information systems," *J. Inf. Secur.*, vol. 11, no. 3, pp. 159-169, 2020.
[30]W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.
[31]G. Kaur and J. Singh, "Secure attendance management system using cryptographic algorithms," *Int. J. Comput. Appl.*, vol. 176, no. 30, pp. 23-30, 2020.