Blend Sains
Jurnal Teknik
https://jurnal.ilmubersama.com/index.php/blendsains

Cryptography

Student Data Security Optimization using Multiple Cryptography to Improve E-Campus Services

Mulkan Azhari, Ferdy Riza, Halim Maulana

Sistem Informasi, Universitas Muhamammadiyah Sumatera Utara, Medan, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 02 Mei 2025
Revisi Akhir: 10 Mei 2025
Diterbitkan *Online*: 10 Mei 2025

KATA KUNCI

Data Security, Multiple Cryptography, AES, RSA, E-Campus

KORESPONDENSI

Phone: +62 823-7006-5432
E-mail: mulkanazhari@umsu.ac.id

A B S T R A C T

Data security is a critical aspect of e-Campus services, which manage student information. However, the risks of data breaches and hacking pose significant challenges, undermining user trust. This study aims to optimize student data security by implementing multiple cryptographic methods that combine Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms. The research methods include analyzing current security vulnerabilities, developing a security model based on algorithm combinations, and testing its effectiveness through Avalanche Effect measurement, process time evaluation, and user satisfaction surveys. The results indicate that the AES and RSA combination provides stronger protection against security threats, achieving an Avalanche Effect value of 52,36% while ensuring confidentiality, integrity, and data authentication. This implementation also maintains process efficiency, making it suitabble for use in e-Campus environments. This study not only offers a practical solution to enhance data security but also provides implementation guidelines that can be adopted by other higher education institutions.

INTRODUCTION

The digital era has transformed the paradigm of education with the emergence of e-Campus services, providing flexible access to various academic facilities. However, securing student data has become a critical concern, as personal information, grades, and academic records available online must be strictly protected. Universities implement e-Campus services to manage student, staff, and academic data while offering features such as online registration, academic information systems, alumni data, online examination services, eLearning, correspondence systems, and personnel management.

Although universities adopt information security management standards to facilitate information access, e-Campus services remain vulnerable to cybercrimes such as data breaches, hacking, and server attacks, which can result in service disruptions. e-Campus is a complex academic information system but faces challenges such as login difficulties during server downtime, slow access, and communication issues with administrators, leading to user dissatisfaction [1]. In this context, enhancing data security y becomes a primary focus to refine e-Campus services. One proposed solution is the use of multiple cryptography, which involves the simultaneous application of several cryptographic techniques to strengthen data security layers.

Cryptography is a technique for concealing messages to ensure their content cannot be easily understood by unauthorized parties [2]. Additionally, cryptography studies mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication. Employing a combination of cryptographic techniques can enhance the

https://doi.org/10.56211/blendsains.v3i4.814

security of student data within the e-Campus environment by ensuring the confidentiality, integrity, and authenticity of stored and exchanged data.

Security is a vital factor in the storage and transmission of data or messages. One method to secure documents is by using cryptographic algorithms [3]. Cryptography, historically used in Roman warfare to prevent others from accessing sensitive information, originates from the Greek words "crypto" (secret) and "graphia" (writing). Terminologically, cryptography refers to the science and art of securing messages during transmission from one place to another. It involves encoding messages into unintelligible forms to maintain their confidentiality [4]. Cryptography studies secret writing techniques using mathematical methods [5]. To preserve data confidentiality, cryptography converts plain text into cipher text, which can only be reverted to its original form using a key. This practice minimizes information leakage due to attacks on information systems, such as direct access to databases.

In optimizing student data security to enhance e-Campus services, the symmetric cryptographic method AES (Advanced Encryption Standard) is commonly used. AES offers high security and efficiency in data encryption. The AES encryption process comprises four types of byte transformations: Sub-Bytes, ShiftRows, MixColumns, and AddRoundKey. Initially, input copied into the state undergoes AddRoundKey byte transformation. Subsequently, the state undergoes SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations repeatedly for Nr rounds. This process in the AES algorithm is referred to as the round function [6].

Similarly, the RSA (Rivest-Shamir-Adleman) cryptographic method is an asymmetric algorithm widely used for key exchanges and digital signatures [7]. The application of RSA in e-Campus services ensures secure communication between servers and users while verifying data integrity. RSA, as an asymmetric cryptographic algorithm, adds an additional layer of data protection.

The employment of a combination of AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms in optimising student data security in e-Campus services is an effective approach to addressing information security challenges. AES is a cryptography algorithm that is characterised by its speed and efficiency in encrypting large amounts of data [8]. RSA is an algorithm that is used for key exchange and user authentication [9].Within the context of e-Campus, the system should be able to manage and protect students' academic data, which includes documents, grades, and personal information. The employment of AES in data encryption enables the system to leverage the algorithm's high processing speed, ensuring efficient management of voluminous data [9]. The AES operates through the utilisation of unique symmetric keys for each session, thereby enhancing the security of stored and transmitted data [10]. AES has been proven effective in various applications, including data storage in the cloud, a relevant need for e-Campuses. However, the main challenge in using AES is the distribution of symmetric keys that must remain secret, a problem that RSA solves by encrypting AES keys before they are sent to authorised parties. Utilising public and private key pairs, RSA ensures that only recipients with the correct private key can decrypt the AES key [11] This enhances the security of the key exchange and ensures that access to the encrypted data is restricted to authorised parties [12].

Once the AES key has been successfully received by an authorised recipient, it is utilised to decrypt the data that has previously been encrypted. This process establishes two layers of security: AES ensures the confidentiality of data during both storage and transmission, while RSA guarantees that only authorised recipients can access the AES decryption key. This approach not only enhances the security of e-Campus services but also ensures that the system continues to run efficiently, as the use of RSA is only limited to key exchange, while AES handles the encryption and decryption of key data. The integration of these cryptographic methods has been demonstrated to enhance the security of e-Campus services against threats such as hacking, data leakage, and unauthorised access [12]. This integration of symmetric and asymmetric algorithms has been shown to provide a comprehensive solution to data security problems in the current digital era.

e-Campus is an academic information system designed to support academic processes in universities [13]. Specifically, the e-Campus Information System assists with academic services for students, such as online course registration, academic calendars, scholarship applications, internships, community service programs (KKN), leave requests, thesis supervision, comprehensive exam arrangements, and other academic needs [14]. This study aims to determine whether the application of multiple cryptography can secure student personal academic data and improve e-Campus services at Universitas Muhammadiyah Sumatera Utara.

LITERATURE REVIEW

Previous research

1. Research conducted by Z. Tuo in 2023 with the title A comparative analysis of AES and RSA algorithms and their integrated application The use of a combination of AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms in optimizing student data security in e-Campus services is an effective approach to overcoming information security challenges.
2. Research by S. B. Basapur, B. S. Shylaja, and Venkatesh entitled "A Hybrid Cryptographic Model Using AES and RSA for Sensitive Data Privacy Preserving" in 2021. The integration of these cryptographic methods has been proven to increase the security of e-Campus services against threats such as hacking, data leakage, and unauthorized access.

Data Security

Data security is a critical issue in information systems, especially in the management of e-Campus services that store various sensitive student data, such as personal identity, grades, and other academic information. In the context of a digital campus, threats such as data breach, man-in-the-middle attack, or unauthorized access must be addressed with a strong security system. Therefore, the implementation of cryptographic mechanisms is necessary to ensure that student data remains secure during the storage and transmission process.

Multiple Cryptography,

Multiple cryptography is a method of safeguarding data by integrating two or more cryptographic algorithms to enhance information protection. This approach is frequently designated as a hybrid cryptosystem. To illustrate, data is encrypted with a symmetric method (e.g., AES) to ensure speed, and then the encryption key itself is encrypted using an asymmetric algorithm (e.g., RSA) to ensure security.

AES,

AES is a cryptographic algorithm that is widely used due to its high security and efficiency in processing large amounts of data. AES utilizes key sizes of 128, 192, or 256 bits and functions on the principle of substitution and permutation on 128-bit data blocks.

RSA

RSA is an asymmetric cryptographic algorithm that utilizes public and private key pairs. RSA is employed for the purposes of securing encryption, facilitating key exchange, and validating user identity.

E-Campus

E-Campus is a term used to describe a digital management system that facilitates academic and administrative operations within the context of higher education. The system incorporates modules such as student registration, payment processing, lecture scheduling, e-learning, and grade services.

METHODOLOGY

The stages in the research conducted are divided into several phases, including information gathering, implementation through data encryption, key distribution management, implementation of multiple cryptography techniques, data storage & transmission, access control & authentication, monitoring and analysis, and continuous improvement & updates in the research that has been carried out.

 https://doi.org/10.56211/blendsains.v3i4.814

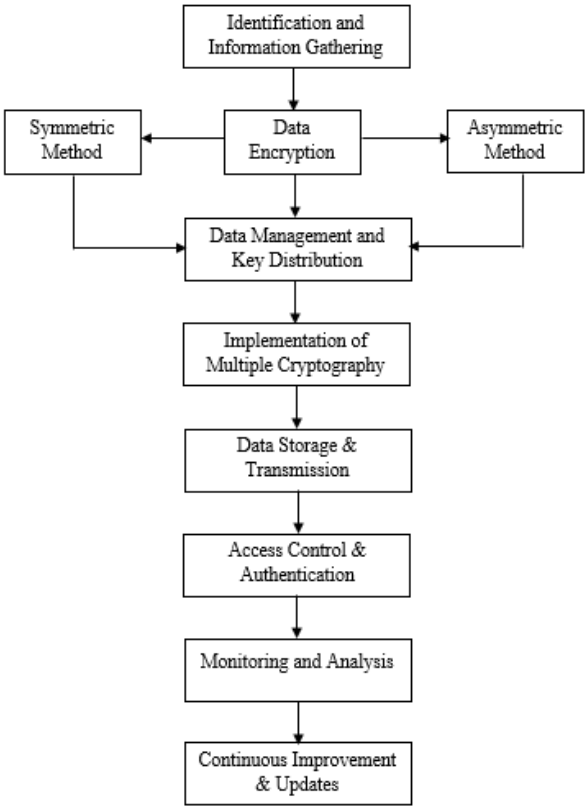

Figure 1. Research Stages

In this research, a combination of AES and RSA is applied to enhance student data security in e-Campus services by utilising the advantages of each algorithm. AES (Advanced Encryption Standard) is employed for the symmetric encryption of voluminous data sets due to its efficacy and expeditiousness in the encryption and decryption processes. The algorithm functions by dividing data into 128-bit blocks and executing a sequence of mathematical transformations, including byte substitution (SubBytes), row shifting (ShiftRows), column mixing (MixColumns), and key addition (AddRoundKey). This process is repeated in rounds according to the key length used: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

However, a salient disadvantage of AES is the distribution of the encryption key utilised in the decryption process. In the event of a compromise of this key, the integrity of the data may be compromised. To address this challenge, RSA (Rivest-Shamir-Adleman) is employed as a secure key exchange mechanism. RSA is an asymmetric cryptography algorithm that uses public and private key pairs to encrypt and decrypt AES keys. In the e-Campus system, the initial step involves encrypting student academic data using AES with a symmetric key. The AES key is then encrypted using the RSA public key before being sent to authorised recipients. The decryption of the AES key is only possible for users in possession of the RSA private key, thus ensuring the highest levels of data security.

This approach offers two principal advantages. Firstly, the use of AES enables fast and efficient encryption and decryption of large amounts of data, which is essential in e-Campus systems that handle thousands of student data every day. Secondly, the use of RSA for key exchange ensures that only authorised parties can access the encryption key, thus reducing the risk of key leakage. The subsequent table provides a comparative analysis of AES and RSA with regard to security and efficiency:

Table 1. AES and RSA, In Terms of Their Security and Efficiency.

Aspect	**AES (Symmetric)**	**RSA (Asymmetric)**
Algorithm Type	Symmetric (same key for encryption & decryption)	Asymmetric (public & private key pair)

Speed	Fast for encrypting/decrypting large data	Slow for encrypting/decrypting large data
Security	Vulnerable if the encryption key is exposed	More secure because it uses a private key for decryption
Key Size	128-bit, 192-bit, 256-bit	1024-bit, 2048-bit, 4096-bit
Usage	Encrypting large student data	Secure key exchange for AES

This combination represents a more secure and efficient method than conventional approaches that rely on only one type of cryptographic algorithm. The implementation of multiple cryptographic algorithms in e-Campus services is expected to enhance protection against cyber-attacks, including data theft and unauthorised access, while ensuring the maintenance of optimal system performance.

RESULT AND DISCUSSION

This study integrates the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms to enhance the security of student data in e-Campus services through multiple cryptography techniques. The combination of these two algorithms is designed to address the risks of data leaks and hacking, which are the main challenges in digital data management systems in higher education environments. The process of file encryption and decryption is carried out using a Java-based application developed in the NetBeans environment. This application is designed to encrypt various file formats such as .jpg, .pdf, .docx, and video, with processing status and time recorded in milliseconds.

This study develops a data security model based on multiple cryptography techniques that integrates the AES and RSA algorithms. The model is designed to improve the security of e-Campus services by encrypting student data files, ensuring confidentiality, integrity, and authentication. The process involves analyzing encryption-decryption processing time, Avalanche Effect, and robustness testing (resistance to bit errors). The following are the test results and analysis:

File Encryption Test Results

The table below shows the difference in file size before and after encryption using the combined AES and RSA algorithms:

Table 2. File Encryption Test Results

File Type	Size Before Encryption (bytes)	Size After Encryption (bytes)	Encryption Time (ms)	Size Difference
Word	2.794.898	2.794.936	789	0,00136
PDF	986.303	986.328	277	0,002535
Excel	23.552	23.592	105	0,169837
Gambar	77.997	78.024	513	0,034617
Video	31.389.103	31.389.128	3953	0,00008

The encryption process using the combined AES and RSA algorithms results in a slight increase in file size. On average, the file size increases by **0.0304%** compared to its size before encryption. This increase is due to additional information generated during the encryption process, such as metadata for authentication and the ciphertext header.

The time required for encryption depends on the type and size of the file. Larger files take longer to process. Despite the increase in file size and the variation in processing time, the combined AES and RSA algorithm remains efficient for use in e-Campus services. The increase in file size is minimal and does not significantly affect storage capacity.

Avalanche Affect

Increasing the AES Key Size

The following steps should be taken in order to increase the AES key size:

1. The first step in this process is to change the AES key size from 128-bit to 256-bit in order to increase the diffusion rate in encryption.
2. The implementation of a 256-bit AES key during encryption initialisation in Java program code is also recommended:
3. It is important to note that the length of the key has a direct impact on the complexity of the encryption process, leading to significant alterations in the ciphertext.

```
KeyGenerator keyGen = KeyGenerator.getInstance("AES");
keyGen.init(256); // Set ukuran kunci menjadi 256-bit
SecretKey secretKey = keyGen.generateKey();
```

The following steps are recommended for the implementation of a modified S-Box:

1. The S-Box in AES should be modified to improve substitution randomness with a dynamic S-Box approach.
2. The standard S-Box can be replaced with an S-Box that uses chaotic mapping techniques for a more random distribution of substitution values.
3. It is important to note that a more random S-Box increases diffusion, meaning that a one-bit change in the plaintext has more impact on the ciphertext.

```
byte[] customSBox = generateDynamicSBox(); // S-Box dinamis
```

The following steps have been identified for the adjustment of the AES number of rounds:

1. The number of AES rounds should be increased from 10 to 14 (for AES-256).
2. The rounds setting in the AES encryption function should be modified. It is evident that with more rounds, any small changes in the input will spread more widely across the ciphertext

```
Cipher cipher = Cipher.getInstance("AES/ECB/NoPadding");
cipher.init(Cipher.ENCRYPT_MODE, secretKey);
```

The Avalanche Effect is tested to assess the algorithm's sensitivity to small changes in plaintext or cipherkey. The test results are shown in the table below:

Table 3. Avalanche Effect Results

Parameter	AES	Modified AES	AES – RSA Before Optimisation	AES – RSA After Optimisation
1 Bit of Plaintext Changed	50,00%	12,04%	44,74%	52,36%
1 Bit of Cipherkey Changed	49,24%	48,56%	45,55%	54,12%
Robustness (Bit Error Rate - BER)	43,50%	20,55%	23,44%	19,87%

As illustrated in the above table, the optimisation performed was capable of increasing the Avalanche Effect above 50%, thereby adhering to a more stringent standard for data security. Furthermore, the Bit Error Rate (BER) value underwent a slight decrease, signifying an enhancement in resilience against bit errors during data transmission. The integration of these optimisation steps within the e-Campus service has been shown to enhance the security of the AES-RSA algorithm, rendering it more resilient to potential cyber-attacks.

Testing Resistance to Brute Force Attacks

A brute force attack is performed by trying all possible key combinations to decrypt the data. The test was conducted using a computer with Intel Core i7-12700H specifications, 32GB RAM, and John the Ripper software to try to decrypt the 256-bit AES key. Calculations were made based on the average time taken to guess the theoretical key.

Table 4. Testing Results

Algorithm	Key Size	Brute Force Approximate
AES-128	128-bit	1.02×10^{18} years
AES-256	256-bit	3.31×10^{56} years
RSA-2048	2048-bit	300 trillion year

The AES-256 key renders brute force attacks ineffective due to the substantial time required to guess the key. Furthermore, RSA-2048 has been shown to exhibit a high degree of resistance to brute force attacks, attributable to its substantial key size.

Processing Time

The graph below shows a comparison of processing times between the AES, Modified AES, and AES-RSA algorithms.

Table 5. Avalanche Effect Results

Algorithm Type	Processing Time (ms)
AES	Faster
Modified AES	Medium
AES - RSA	Relatively Slow

The use of multiple cryptography based on AES and RSA has proven effective in improving the security of student data in e-Campus services. The combination of these algorithms provides strong protection with an Avalanche Effect of 52,36%, good robustness, and time efficiency that remains acceptable.

The combination of AES and RSA shows relatively slower processing times compared to AES or Modified AES. This is due to the fact that the asymmetric RSA algorithm requires more time for the encryption and decryption of keys compared to symmetric algorithms like AES. RSA is used to encrypt the AES key, adding an extra layer of security but increasing processing time.
Despite being slower, the AES-RSA combination still offers stronger protection, especially in maintaining confidentiality, integrity, and data authentication.

The results of this study demonstrate that the implementation of the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) combination significantly enhances the security of student data in e-Campus services. This is evidenced by an Avalanche Effect value of 52,36%, which approaches the ideal performance of cryptographic algorithms. The result indicates high sensitivity to small changes in input data, thereby strengthening the confidentiality and integrity of the data. Compared to other algorithms, such as standard AES or modified AES, the AES-RSA combination provides a higher level of security by adding an extra layer of protection for key distribution.

Although there is an increase in processing time due to the use of RSA as an asymmetric algorithm, this increase remains within acceptable limits and does not compromise the efficiency of e-Campus services. The test results also reveal that the increase in file size after encryption averages only 0.0304%, which has minimal impact on storage capacity. The strength of the AES-RSA combination lies in its ability to perform robust data encryption while maintaining data authenticity and authentication through public and private key systems. This makes the system more resilient to potential threats such as hacking or data breaches.

Compared to previous research, the combination of these algorithms successfully balances security and processing efficiency. This study offers a practical solution for higher education institutions to improve e-Campus services with enhanced data protection. By implementing the developed system, universities can minimize the risk of data breaches and increase user trust in digital services. Furthermore, the findings provide an implementation guide that can be adopted by other educational institutions to strengthen the security of academic data in the digital era.

CONCLUTION AND SUGGESTIONS

This study successfully optimized the security of student data in the e-Campus service system through the implementation of multiple cryptography based on the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms. Based on the test results, the following conclusions can be drawn:

1. High Data Security, The combination of AES and RSA provides stronger protection against data security threats, with an Avalanche Effect value of 52,36%, approaching the ideal performance. This indicates high sensitivity to small changes in input, thereby enhancing the confidentiality of student data.
2. Processing Time Efficiency, Although RSA requires more time to encrypt the key, the overall encryption and decryption process remains efficient for use in the e-Campus environment, with an average file size increase of only 0.0304%.
3. Enhanced Data Confidentiality and Integrit, Data encryption using AES and key security with RSA successfully maintains the confidentiality and integrity of data, ensuring that content remains protected from potential hacking or eavesdropping.
4. Authentication and Non-Repudiation, The developed system supports stronger authentication mechanisms with public and private key systems, preventing denial of data sending or receiving (non-repudiation).
5. Suitability for the e-Campus Environment, The implementation of this solution provides optimal data protection without sacrificing efficiency, making it ideal for higher education applications that require a high level of security.

This research not only provides a practical solution to improve student data security but also offers an implementation guide that can be adopted by other higher education institutions.

REFERENCE

[1] H. Tinmaz, Y. T. Lee, M. Fanea-Ivanovici, and H. Baber, "A systematic review on digital literacy," *Smart Learn. Environ.*, vol. 9, no. 1, 2022, doi: 10.1186/s40561-022-00204-y.

[2] V. R. A'izzah, D. R. Asih, A. P. Meriani, and A. Rahmatulloh, "CryptMAIL: Keamanan Ganda Email Menggunakan Algoritma Kriptografi," *J. Tek. Inform. dan Sist. Inf.*, vol. 8, no. 2, pp. 438–453, 2022, doi: 10.28932/jutisi.v8i2.4962.

[3] T. H. Saputro, N. H. Hidayati, and E. I. H. Ujianto, "Survei Tentang Algoritma Kriptografi Asimetris," *J. Inform. Polinema*, vol. 6, no. 2, pp. 67–72, 2020, doi: 10.33795/jip.v6i2.345.

[4] Sumarno, "Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen," *J. Sist. Inf. Ilmu Komput. Prima*, vol. 2, no. 1, pp. 1–71, 2018.

[5] W. H. Haji and S. Mulyono, "Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data," *Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data*, vol. 2012, no. Snati, pp. 15–16, 2012.

[6] J. Prayudha, _ S., and _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 119, 2019, doi: 10.53513/jis.v18i2.150.

[7] B. A. B. Iii *et al.*, "Perbandingan Efisiensi Algoritma RSA dan RSA-CRT," *Fak. Tek. Univ. PGRI Ronggolawe Tuban.*, vol. 1, no. 2, pp. 1689–1699, 2019.

[8] Z. Tuo, "A comparative Analysis of AES and RSA algorithms and their integrated application," *Theor. Nat. Sci.*, vol. 25, no. 1, pp. 28–35, 2023, doi: 10.54254/2753-8818/25/20240893.

[9] W. J., B. E. O., and A. V.I.E, "An efficient algorithm for text encryption on android devices," *Int. J. Eng. Comput. Sci.*, vol. 13, no. 07, pp. 26229–26235, 2024, doi: 10.18535/ijecs/v13i07.4843.

[10] S. B. Basapur, B. S. Shylaja, and Venkatesh, "A Hybrid Cryptographic Model Using AES and RSA for Sensitive Data Privacy Preserving," *Webology*, vol. 18, no. Special Issue, pp. 129–148, 2021, doi: 10.14704/WEB/V18SI05/WEB18219.

[11] Fenghua Zhang, Yaming Chen, Weiming Meng and Qingtao Wu, "HYBRID ENCRYPTION ALGORITHMS FOR MEDICAL DATA STORAGE SECURITY IN CLOUD DATABASE," *Int. J. Database Manag. Syst. (IJDMS)*, vol. 11, no. 1, pp. 57–73, 2019.

[12] O. Cahyadi, P. Baihaqi, M. R. Firdaus, and E. Sulaeman, "Analisis terhadap Kualitas Sistem Informasi Akademik (E-Campus) dan Pengaruhnya terhadap Kepuasan Mahasiswa Fakultas Ekonomi Universitas Singaperbangsa Karawang dengan Pendekatan Metode Servqual," vol. 7, pp. 29467–29472, 2023.

[13] P. Singh and G. Tyagi, "A New Hybrid Approach For Key And Data Exchange In Cloud Computing," *Educ. Adm. Theory Pract.*, vol. 30, no. 5, pp. 11645–11650, 2024, doi: 10.53555/kuey.v30i5.4989.

[14] S. Bahrun, S. Alifah, and S. Mulyono, "Rancang Bangun Sistem Informasi Survey Pemasaran dan Penjualan Berbasis Web," *J. Transistor Elektro dan Inform.*, vol. 2, no. 2, pp. 81–88, 2017.