Optimizing Data Security in Computer-Assisted Test Applications Through the Advanced Encryption Standard 256-Bit Cipher Block Chaining

M. Afridon[1], Agus Tedyyana[2], Fajar Ratnawati[3], Afis Julianto[4], M. Nur Faizi[5]
Department of Electrical Engineering, Politeknik Negeri Bengkalis, 28711, Indonesia[1, 5]
Department of Informatic Engineering, Politeknik Negeri Bengkalis, 28711, Indonesia[2, 3, 4]

***Abstract*—In the digital education era, the importance of Computer-Assisted Test programs is underscored by their efficiency in conducting assessments. However, the increasing incidence of data breaches and cyberthreats has made the implementation of robust data protection measures imperative. This study explores the adoption of the Advanced Encryption Standard 256-bit Cipher Block Chaining in CAT applications to enhance data security. Known for its strong encryption capabilities, AES-256-CBC is an excellent choice for securing sensitive test data. The research focuses on the application of AES-256-CBC within CAT systems during the independent admission process at Politeknik Negeri Bengkalis, a critical phase where the integrity of exam materials and student data is paramount. We evaluate the effectiveness of AES-256-CBC in encrypting user data and exam materials across different CAT systems, thus preserving data integrity and confidentiality. The implementation of AES-256-CBC helps prevent unauthorized access and manipulation of test results, ensuring a secure online testing environment. This research not only demonstrates the technical implementation of AES-256-CBC but also assesses its impact on enhancing the security posture of CAT applications at Politeknik Negeri Bengkalis. The findings contribute to the broader discussion on data security in educational technology, positioning AES-256-CBC as a potent solution for maintaining academic integrity in digital testing environments.**

***Keywords*—AES256-CBC; data security; computer-assisted test; academic integrity; encryption standards; digital assessment security**

I. Introduction

The integration of technology into educational processes has become imperative, significantly enhancing learning and assessment procedures but also elevating the risk of cyber threats [1]. As educational institutions increasingly adopt digital platforms for academic assessments and administration, the security of sensitive student data has emerged as a paramount concern. The escalation of complex cyberattacks underscores the urgent need for robust and advanced security systems [2]. A recent analysis by the Center for Strategic and International Studies reveals that by 2023, almost 30% of cyberattacks targeted colleges and schools, making the education sector particularly vulnerable to data breaches [3]. This statistic not only highlights the immediate need for enhanced protective measures, but it also illustrates the magnitude of the threat, urging the implementation of sophisticated security infrastructure to safeguard sensitive and private information. Furthermore, the 2021 data breach at the University of California vividly exposed the susceptibility of university information systems to ransomware attacks [4]. This incident, which compromised the personal information of thousands of students and employees, resulted in significant financial losses and eroded stakeholder confidence, underscoring the necessity for educational institutions to adopt a more thorough and proactive approach to data security. Institutions must ensure their systems not only meet current security standards but are also equipped to anticipate and counter future threats effectively [5].

Literature studies on data security in digital education systems show that the use of encryption technologies such as the Advanced Encryption Standard (AES) 256-bit cipher block chaining (CBC) is becoming crucial. This study shows that the AES-256-CBC provides effective protection against brute force attacks and side attacks, which are two common threats to cybersecurity [6]. This enhanced security has become possible because of the mathematical complexity of the AES-256, which makes it difficult to decrypt without a proper key. Moreover, recent research shows that many educational institutions are still at risk of data leaks because they do not implement adequate security standards [7]. It stresses the need for sustained improvement in data security policies and practices, including better training for information technology managers and system users. Studies conducted around the world show that consistent application of AES-256-CBC results in higher levels of security compared to older encryption algorithms [8]. The study also emphasizes the importance of secure key management and dynamic security policy adaptation to address growing threats. The use of encryption in educational systems not only limits unauthorized access but also guarantees data integrity [9]. This integrity is important not only for data security but also for the trust of stakeholders, which includes students, parents, and teaching staff in addition, the study highlights that an effective security policy should cover more than just the implementation of technical solutions. Aspects such as IT infrastructure physical security, access policies, and emergency response protocols are also critical in ensuring comprehensive data security.

The growing reliance on technology for both teaching and assessment purposes has led to the recognition of data security as a fundamental component of educational integrity. Computer-assisted test (CAT) applications [10], with their simplicity in use and accuracy in real-time scoring, have revolutionized exam conduct in educational settings. However, the digital transformation presents novel challenges, particularly

concerning data security. Since its inception, CAT technology has evolved extensively, enhancing test delivery and analysis in both educational and professional contexts. The latest advancements primarily involve the integration of adaptive testing techniques, which dynamically adjust to an examinee's ability level, thereby providing a more tailored and accurate assessment of skills and knowledge [11].

The integration of modern CAT systems into online learning platforms has enabled seamless interactions between the testing interface and educational content, fostering a more cohesive learning and assessment experience [12]. We design these systems to be versatile, accommodating various item types and testing strategies to address diverse educational needs. Despite these advantages, CAT systems face several operational challenges, such as calibrating the item pool, which requires initial testing on a large sample of examinees to ensure the reliability and validity of test items. Additionally, the design of CAT systems must consider factors such as test security, fairness, and the potential for test-taker manipulation. The need for advanced software and psychometric expertise to develop and maintain these systems underscores the difficulty of effectively implementing adaptive testing processes.

Amidst increasing incidents of data breaches and cyber threats, CAT applications have become frequent targets of cyberattacks due to their storage of sensitive and crucial data, such as student personal information and test results [13]. This vulnerability highlights the importance of expanding and consolidating data security measures to protect such sensitive data comprehensively [14]. This study looks at how to use the AES-256-CBC [15], which is well-known for its strong encryption and excellent defense against collision and pre-image attacks. This makes it a great choice for keeping sensitive data safe in CAT systems.

The focus of this research also extends to the application of AES-256-CBC at Politeknik Negeri Bengkalis during the process of admitting new students through independent tracks. This examination provides a detailed view of the application of data security technologies in Indonesia's higher education system, underscoring the responsibility of educational institutions to protect student data. The integration of AES-256-CBC not only brings technical improvements but also enhances confidence among students and other stakeholders, reinforcing the notion that robust data security can significantly improve an organization's reputation and foster a secure environment for both students and teachers when utilizing technology for exams.

This study aims to offer guidance to other educational institutions seeking to enhance the security of their examination applications by analyzing the implementation of AES-256-CBC at Politeknik Negeri Bengkalis. The insights derived from this analysis are valuable not only at the local level, but also globally, as they contribute to the broader discourse on cybersecurity threats in education. By strengthening data security measures, educational institutions can concentrate more on conducting learning and evaluation processes that are not only efficient but also secure, fostering an environment conducive to innovation and technological integration [16]. This research serves as a benchmark for developing cybersecurity policies and best practices in education, enabling policymakers and administrators to formulate more effective data security strategies based on clear, evidence-based guidelines.

The continuous evolution of cyber threats further underscores the robustness of data security in educational technology, necessitating an ongoing assessment and adaptation of security protocols [17]. As we embrace digital tools in education, it becomes crucial to implement systems that not only react to breaches but also proactively prevent them. This dual approach ensures that the security architecture evolves in parallel with emerging threats, maintaining the integrity and confidentiality of student data at all times. Ensuring the highest standards of data protection not only complies with regulatory demands but also addresses the ethical responsibility educational institutions hold towards their constituents [18]. Moreover, the strategic application of technologies such as AES-256-CBC in the education sector can serve as a model for other sectors where data sensitivity is paramount. By showcasing effective strategies for safeguarding data within the rigorous and often targeted environment of educational institutions, we can demonstrate the feasibility and effectiveness of advanced encryption methods. This initiative not only mitigates risks associated with data breaches but also advances the discourse on data security practices, fostering a broader understanding and implementation [19] of best practices across various domains.

The implementation of the AES-256-CBC algorithm significantly reduces the risk of data breaches and cyberattacks, ensuring that sensitive data, including student personal information and test results, remains protected from unauthorized access and manipulation. Enhanced data security also builds trust between educational institutions and their stakeholders, including students, parents, and teaching staff. This trust is essential for creating a positive and supportive learning environment where students and parents feel secure, and teachers are confident in using technology to manage exams safely. As educational institutions continue to face an increasing number of cyber threats, improved protection mitigates potential financial and reputational losses while simultaneously enhancing the learning experience through the safe and diverse use of digital technologies in education. This comprehensive approach to cybersecurity in educational settings not only secures data but also enriches the educational journey for all participants.

II. Materials and Method

A. Setting and Sample Selection Study

The study was conducted at the Politeknik Negeri Bengkalis, focusing on the use of CAT applications for the process of independent admission of new students in the 2024/2025 academic year. The samples include the CAT system currently in use at Politeknik Negeri Bengkalis, along with the data processing practices observed during the cycle of new student admission in 2024-2025. Administrators, IT staff, and prospective students are involved in providing insight into operational and security aspects.

B. Encryption Methodology

To secure the data processed through CAT applications, the Advanced Encryption Standard 256-bit Cipher Block Chaining

was implemented. This section details the critical data points within CAT applications that required encryption and describes the collaborative process with the IT department to integrate AES-256-CBC, replacing the previous encryption method.

C. Cipher Block Chaining Process

To explore the implementation of AES-256-CBC, we first identified critical data points in CAT applications that require encryption. We then integrated AES-256-CBC into the existing CAT system, replacing the previous encryption method. This process involves collaboration with the IT department to ensure that all technical aspects are dealt with, including key management and system compatibility.

Fig. 1, Encryption process using CBC, illustrates the encryption process using CBC model, a widely used method in cryptographic systems for securing data [20]. This mode of operation is particularly effective in enhancing data security by linking blocks of plaintext to produce a chain of ciphertext, ensuring that similar plaintext blocks result in different ciphertext blocks.

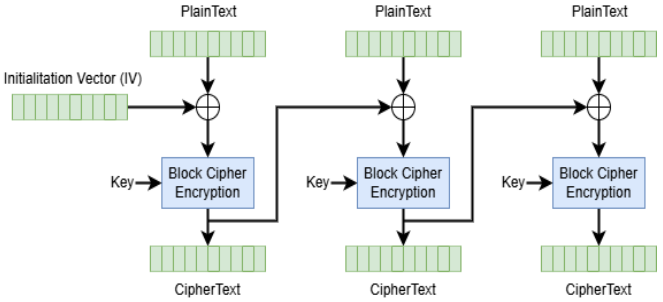

Fig. 1. Encryption process using CBC.

In CBC mode, the encryption process begins with an initialization vector (IV) [21]. To prevent ciphertext patterns, the IV must be unique and unpredictable for each encryption session. Unlike the encryption key, the IV does not need to be secret, but it should be random and not reused with the same key to maintain security.

The process starts with the IV, which is XORed (exclusive OR operation) with the first block of plaintext. This step is crucial as it mask the first block of plaintext, which adds an additional layer of security and ensures that the same plaintext blocks will produce different ciphertext blocks when encrypted under the same key but with different IV [22]. Following the initial XOR operation, a block cipher algorithm encrypts the resulting block using a specified encryption key. This encryption results in the first block of ciphertext.

The ciphertext from the previous block serves as the "new IV" for each subsequent plaintext block. We XOR this blockwith the next plaintext block, then use the same block cipher algorithm and key to encrypt the result. This chaining mechanism ensures that each block of ciphertext is dependent not only on the current plaintext block but also on all preceding plaintext blocks.

Each encryption step produces the ciphertext associated with each plaintext block [23]. Each piece of ciphertext is dependent on the initial IV and the sequence of plaintext blocks, creating a chain in which the correct decryption of each block requires the ciphertext of the preceding block (except for the first block, which requires the IV).

CBC mode's approach, where the encryption of each plaintext block is dependent on the previous ciphertext block, significantly increases security by introducing complexity and randomness into the process [24]. This method prevents plaintext patterns from appearing in the ciphertext, making it more resilient to cryptographic attacks such as pattern analysis. The CBC mode is highly regarded for its ability to propagate errors, meaning that a single bit error in a block of ciphertext will render that block and the following block indecipherable, which can be a useful security feature or a drawback, depending on the context of use.

Fig. 2 illustrates the decryption process using the CBC mode, a common operational mode for block cipher encryption algorithms. The enhanced security features of this method, which take advantage of the dependencies between encrypted data blocks, make it popular [25]. The CBC decryption process starts with the use of an initialization vector This IV is crucial, as it pairs with the first block of ciphertext to initiate the decryption process [26]. To ensure accurate output, the IV must match the one used during the encryption phase. Despite not being secret, the IV must be unique for each encryption session and not reuse the same key. We decrypt each block of ciphertext using the same key and block cipher algorithm as during the encryption. We decrypt and XOR the first block of ciphertext with the IV to create the first plaintext block. This operation transforms the decrypted data back to its original form before encryption.

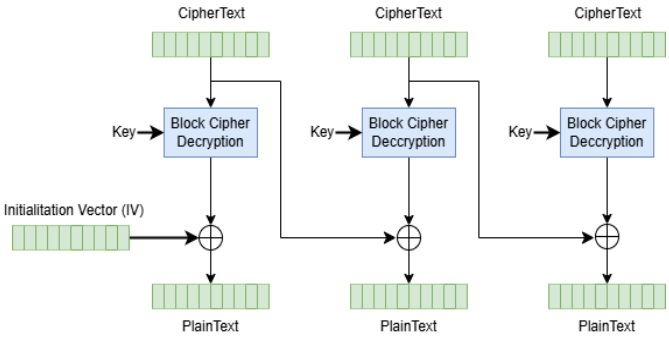

Fig. 2. Decryption process using CBC.

For subsequent blocks, the decryption process follows a chaining mechanism where each decrypted block is XORed with the previous ciphertext block. This sequential processing ensures that any error in a single block of ciphertext during transmission affects not only the current block but also the subsequent block, highlighting a unique dependency characteristic of CBC mode. The process sequentially reveals each piece of plaintext, mirroring the encryption steps in reverse order. This chaining method, where each block's decryption depends not only on its corresponding ciphertext block but also on the preceding ciphertext block, considerably enhances the security of the data transmission. It ensures that the plaintext pattern does not directly influence the ciphertext, making it more resistant to various cryptographic attacks.

The CBC mode's reliance on correct and secure handling of the IV and the chaining mechanism significantly increases system security [27][28]. However, it also introduces certain challenges, such as error propagation and the necessity for secure IV management. These factors must be carefully considered to ensure data integrity and confidentiality throughout its lifecycle. Overall, the CBC mode's decryption process effectively illustrates how cryptographic techniques can enhance data security by intricately linking each block of data to its predecessor, thereby securing the data against unauthorized access and potential security breaches [29].

D. Data Collection

Data collection methods include structured interviews with IT staff responsible for managing the CAT system currently in use at Bengkalis State Polytechnic. In addition, the system logs are reviewed to detect unauthorized access attempts and data breach incidents before and after the AES-256-CBC implementation.

E. Metric Evaluation

The effectiveness of the AES-256-CBC implementation is assessed using several metrics:

1) Comparing the frequency and nature of security incidents before and after implementation.

2) Checks any case of data abnormalities or loss by checking system logs and backup files.

3) Measures changes in system response time and stability to evaluate the impact of AES-256-CBC on the operating efficiency of CAT applications.

4) Conduct surveys with students and staff to measure their confidence in their data security after implementation.

F. Data Analysis

Data analysis in this study employs a blend of quantitative and qualitative methods to gain comprehensive insights into the system's performance and user experiences. We scrutinize system logs and performance metrics using quantitative techniques to objectively assess the enhancements made by integrating AES-256-CBC encryption into the CAT applications. This involves evaluating changes in system response times, error rates, and other relevant performance indicators that directly reflect the operational impact of the encryption methods implemented. We analyze interviews and focus group discussions on the qualitative side to capture the subjective perspectives of end-users and administrators. Understanding how users perceive these security improvements, including any changes in their satisfaction and trust in the system's security measures, is crucial. These interactions' responses help illustrate the practical implications of AES-256-CBC encryption on daily operations and user interactions with the CAT system.

This two-pronged approach tries to connect the technical improvements in security, like AES-256-CBC encryption, with how users feel about it and how well it works. By doing so, the study provides a holistic view of the impact of this encryption technology on CAT applications [30]. It also explores the balance between enhanced security measures and their real-world usability and acceptance, thereby offering valuable insights into both the effectiveness and the user experience of the upgraded system. This comprehensive analysis aids in determining if the security improvements align with user expectations and operational needs, ensuring that the technology not only secures the data but also enhances the overall functionality of the CAT system.

In order to provide a thorough understanding of the technical performance and user experience related to the AES-256-CBC implementation in the CAT applications, this study used a combination of quantitative and qualitative methodologies. We gathered and examined system logs and performance indicators with extreme care in order to assess the effects of AES-256-CBC encryption impartially. Prior to and following the encryption deployment, the system reaction times, error rates, and frequency of security events were among the key performance measures. We were able to evaluate the real-world advantages of incorporating cutting-edge encryption techniques into current educational technologies because this data gave us a quantitative assessment of the system's security resilience and operational effectiveness. We obtained qualitative insights through focus groups and structured interviews with end users, including students, administrative staff, and IT personnel at Politeknik Negeri Bengkalis, to supplement the quantitative data. The goal of these talks was to comprehend the differing viewpoints regarding the security enhancements brought about by AES-256-CBC. We specifically looked at user satisfaction, security perception, and confidence in the system's ability to safeguard private data. This qualitative feedback heavily influences the adoption and usability of the security features among the users who are directly engaging with the CAT system.

The combination of quantitative and qualitative data allowed for an in-depth examination of the encryption's efficacy [31]. Through the integration of results from both data streams, the study obtained a comprehensive understanding of the implementation's effects. This dual method helps identify any differences between the perceived and actual performance of the security measures, in addition to helping validate the technical measurements with real-world user feedback. The combined analysis has made it possible to better understand how well AES-256-CBC encryption satisfies the operational requirements and security expectations of educational institutions. It also indicated areas in which user training and technology implementation still needed improvement. These understandings are essential for creating focused plans to strengthen user confidence in digital learning environments and improve data security procedures.

III. Results and Discussion

A. Login Interface CAT

The login screen is the first gateway and the main line of defense inining the security of CAT applications in the Bengkalis State Polytechnic. This interface is designed not only to facilitate easy access for authenticated users but also to ensure that sensitive data and user personal information are protected from unauthorized access.

Fig. 3 is a login screen on the Politeknik Negeri Bengkalis CAT application displays a simple yet effective design, which includes fields for entering usernames and passwords. The

"Show Password" feature is provided to help users verify the characters they enter, reducing the risk of input errors that can hinder the login process. Security is deeply integrated into this design through the use of HTTPS to encrypt communications between clients and servers, as well as a security policy that ensures passwords are stored in encryption formats on the server, using state-of-the-art cryptography technologies such as AES-256-CBC.

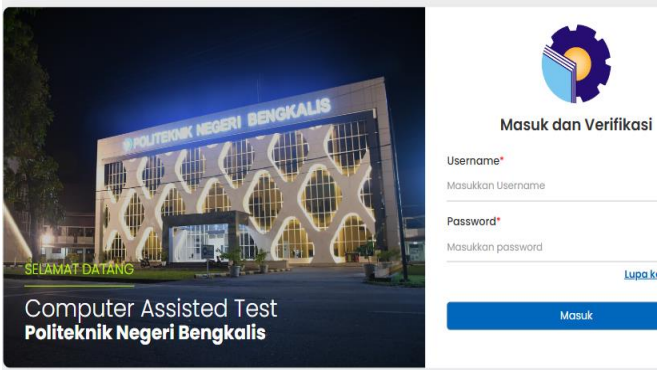

Fig. 3. Login interface CAT.

The interface also comes with additional security mechanisms such as limiting failed login attempts and security features to detect and respond to suspicious activity. It aims to prevent brute-force attacks and the use of stolen credentials, ensuring that only verified users can access the system. Every detail in the login system is designed to improve the overall security of the CAT application. For example, the user session is encrypted end-to-end, and the timeout is implemented automatically to reduce the risk of unauthorized access if the user forgets to log out. In addition, each login activity is recorded in the server log for security audits that allow real-time monitoring of suspicious activity.

B. Encryption Implementation

The PHP code is a crucial part of the security system for the CAT application at Politeknik Negeri Bengkalis. This code details the implementation of the AES-256-CBC algorithm, used for encrypting and decrypting sensitive data within the application. High security standards protect all data stored or transmitted through the CAT system thanks to this implementation.

```php
<?php
// Fungsi untuk mengenkripsi data
function encrypt($data, $key) {
    $iv = openssl_random_pseudo_bytes(openssl_cipher_iv_length('aes-256-cbc'));
    $encrypted = openssl_encrypt($data, 'aes-256-cbc', $key, 0, $iv);
    return base64_encode($encrypted . '::' . $iv);
}

// Fungsi untuk mendekripsi data
function decrypt($data, $key) {
    list($encrypted_data, $iv) = explode('::', base64_decode($data), 2);
    return openssl_decrypt($encrypted_data, 'aes-256-cbc', $key, 0, $iv);
}

// Kunci enkripsi (panjang kunci harus 32 byte untuk AES-256)
$key = '/Ce2c7w44n496kF3VKOXQEkIWyrfyKZzb+DTmLQ7TCM=';
```

Fig. 4. The PHP code AES-256-CBC algorithm.

In Fig. 4, the code consists of two main functions: encrypt() and decrypt(). The encrypt() function utilizes the AES-256-CBC algorithm to encrypt data. The function requires two parameters: the encrypted data and a secret key. Additionally, the code uses openssl_random_pseudo_bytes() to generate a random initialization vector, enhancing security and adding randomness to the encryption process. The system then encodes the encrypted data into Base64 format to facilitate its storage and transmission. The decrypt() function acts as the inverse of encrypt(). It decodes the encrypted data in Base64 format, then uses the same and secret key to decrypt it back to its original form. We strictly safeguard the encryption key, which is critical for both processes, to ensure security.

C. Implications of Security Measures

Politeknik Negeri Bengkalis uses AES-256-CBC to protect all information, including student personal data, exam answers, and evaluation results, from unauthorized access. This algorithm provides excellent protection against various cyberattacks due to the strength of its key and the complexity of the cipher used.

id	id_peserta	nilai_pilihan_ganda
1	16	eyJpdiI6InhOT3RxL09peDJZNkk0TVk5VUpVOWc9PSIsInZhbH...
2	70	eyJpdiI6InNiWkRTbDBqbEdYN000RDkxRU54R3c9PSIsInZhbH...
3	37	eyJpdiI6InpHcDhTbVpBUk1HbHB4cjlWV1RBbVE9PSIsInZhbH...
4	30	eyJpdiI6ImdkeFRUV2pmR2U3TS9WSko5YTh5ZEE9PSIsInZhbH...
5	60	eyJpdiI6Ill1TjkvN0lpSXRSNkpzUFFpRGJWZkE9PSIsInZhbH...
6	79	eyJpdiI6IkZzYlhXT2FHN01Qd3FJb1NaMDJXOFE9PSIsInZhbH...
7	83	eyJpdiI6IjZGRkdUWlZxYVRTSFhwalVYMjVsYlE9PSIsInZhbH...
8	69	eyJpdiI6IkJYSmlGYkZHNDZNNXpqME5jcmx4V0E9PSIsInZhbH...
9	77	eyJpdiI6Ikg3SVhtbi94WGFwbmxYTE5GR05OV2c9PSIsInZhbH...

Fig. 5. List of test identities.

Fig. 5, List of test identities shows a list of test identities matched to their encrypted data. Each line represents a unique set of data related to the test subject, which is secured using the AES-256-CBC encryption algorithm. The use of this encrypting not only protects the data from unauthorized access, but also ensures that each entry is unique, reducing the risk of data leakage or unauthorised modification.

Any information (examination ID and associated details) is encrypted, turning sensitive information into a format that can only be decryptable and understood by the system and authorized personnel. The AES-256-CBC encryption standard is used, which is known for its strength and resilience to a variety of cyber threats, including brute-force attacks and decryption attempts without proper key.

Fig. 6, Test question and its answer options are encrypted. This demonstrates how encryption technology can secure sensitive educational data, such as test results and answer choices. Politeknik Negeri Bengkalis applies encryption to all data elements in CAT applications, reaffirming their efforts to protect the integrity and confidentiality of academic information.

no	soal	pilihan_a	pilihan_b	pilihan_c	pilihan_d
1	eyJpdiI6IkZVWWNRZ3VXZzRXVTlPZDdUM2RvdVE9PSIsInZhbHVlIjoiY	eyJpdiI6IlhV	eyJpdiI6Im	eyJpdiI6IlB	eyJpdiI6Im
2	eyJpdiI6Im1xL2FlclVNMDRVSndueW03QmI2bkE9PSIsInZhbHVlIjoiZD	eyJpdiI6Im	eyJpdiI6Ii9	eyJpdiI6InI	eyJpdiI6Ik
3	eyJpdiI6ImlmQ1JxN3Vka2liTEgrSEFHVUxzbGc9PSIsInZhbHVlIjoiRFhSe	eyJpdiI6Im	eyJpdiI6IjC	eyJpdiI6Ikl	eyJpdiI6Ik
4	eyJpdiI6IjJNcmp4NHFaRjVpdElxSU9wdG4zVVE9PSIsInZhbHVlIjoiY0V	eyJpdiI6Im	eyJpdiI6Ikt	eyJpdiI6Ikl	eyJpdiI6Ijl
5	eyJpdiI6IlVOdS9BYVZOSGJWWFNCcHRTZVVDVlE9PSIsInZhbHVlIjoiRC	eyJpdiI6In	eyJpdiI6Ikx	eyJpdiI6IjL	eyJpdiI6Im
6	eyJpdiI6InA5SWRvK3pEUEF2ajBHMlBCR1I1SGc9PSIsInZhbHVlIjoiVGU	eyJpdiI6Inl	eyJpdiI6Iit	eyJpdiI6Ilk	eyJpdiI6In
7	eyJpdiI6IlFQUjJMWWg0cGNPMGV4b2c4N2x4SWc9PSIsInZhbHVlIjoi	eyJpdiI6Ilk	eyJpdiI6In	eyJpdiI6IjN	eyJpdiI6Iiz
8	eyJpdiI6Ik9keElJQ2ExWGJlU3ZWY0RZTjN6Wnc9PSIsInZhbHVlIjoiL09	eyJpdiI6Inl	eyJpdiI6Ik:	eyJpdiI6Ikt	eyJpdiI6Ijl
9	eyJpdiI6Ik5wcmM1SFhyLzVoNTJNWXRSOHhBbWc9PSIsInZhbHVlIjoi	eyJpdiI6IlJ	eyJpdiI6IjL	eyJpdiI6Im	eyJpdiI6Ilk
10	eyJpdiI6IkRZNUpQbk01Qld5WWJJSzNZclF0R0E9PSIsInZhbHVlIjoiZi92	eyJpdiI6Ijc	eyJpdiI6Ikl	eyJpdiI6IjV	eyJpdiI6Im
11	eyJpdiI6Ik8vS1o2bFUyR2hmMGZKNGJYOHNFYUE9PSIsInZhbHVlIjoiN	eyJpdiI6IlT	eyJpdiI6In	eyJpdiI6In:	eyJpdiI6Ijl
12	eyJpdiI6IkdFSk02VXZkR3JDaHZlcUo5SGM5bXc9PSIsInZhbHVlIjoidlplS	eyJpdiI6Ikk	eyJpdiI6Im	eyJpdiI6Im	eyJpdiI6Ilk
13	eyJpdiI6IjcvdHBkdDJUbEg1YU1sSUkrZjZkZUE9PSIsInZhbHVlIjoid3FZZ	eyJpdiI6Im	eyJpdiI6IjR	eyJpdiI6Inl	eyJpdiI6Iiz
14	eyJpdiI6IlJ1eDF3M3VhSXlJeFFzbkU4MWJTQWc9PSIsInZhbHVlIjoidlZl	eyJpdiI6Ikt	eyJpdiI6IlY	eyJpdiI6Iit	eyJpdiI6Ijl
15	eyJpdiI6Ikl3NDB4Mk1ZMWprOTc5SDArbDFxU1E9PSIsInZhbHVlIjoiRV	eyJpdiI6Ikk	eyJpdiI6Im	eyJpdiI6Im	eyJpdiI6Ijl
16	eyJpdiI6In75b2Vz7V7CbnV2dmlmazNEa1hPVGc9PSIsInZhbHVlIjoiN0k	eyJpdiI6Iit	eyJpdiI6In	eyJpdiI6IlV	eyJpdiI6Iil

Fig. 6. Test question and its answer options are encrypted.

In practice, the test management system encrypts each test question and its answer options before storing them in a database or displaying them. This process ensures that only individuals who have a valid decryption key, such as a system administrator or authorized developer, can access the actual data content. This is critical to preventing the leakage of examination information, which could result in a loss of academic integrity and fairness. Data encryption also helps to comply with strict data protection regulations, ensuring that educational institutions meet their legal obligations to student data security and privacy. It not only increases stakeholder confidence in the educational system used, but also strengthens the institution's reputation as a responsible and secure entity. Politeknik Negeri Bengkalis demonstrates, through the use of advanced encryption technology, how technology can enhance security in an educational environment, protect sensitive data from external and internal threats, and enhance a secure learning experience for all parties involved.

Fig. 7, test question and its answer options are decrypt in the exam scenario using the CAT system at Bengkalis State Polytechnic, the subjects presented to the participants have already undergone the process of decryption so that they appear in the form of text that is readable and accessible by the participants. This process describes how data previously secured with AES-256-CBC encryption is converted back to its original format for use during the test.

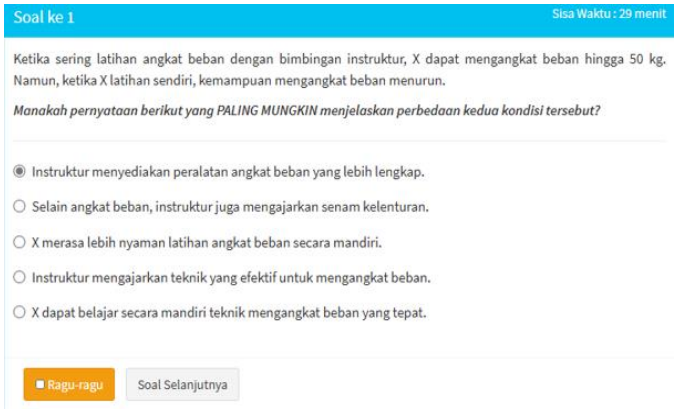

Fig. 7. Test question and its answer options are decrypt.

D. Administrative Dashboard Functionality

This interface display shows the effectiveness of CAT systems in managing and presenting test issues in a secure and organized manner. By ensuring that all subjects are encrypted during storage and only decoded during examination, Bengkalis State Polytechnic demonstrates its commitment to data security and academic integrity. Participants can answer questions with confidence, knowing that the system they use supports them with secure and sophisticated technology. It not only improves the test experience for participants but also affirms the importance of data security in an educational context.

Fig. 8. Administrative dashboard for the CAT system.

Fig. 8 shows a view of the administrative dashboard for the CAT system in Politeknik Negeri Bengkalis. The dashboard serves as a control center for system administrators in managing various aspects of the CAT system. Here is a narrative about the functions and components of this admin dashboard:

1) The dashboard is designed to provide quick and easy access to the range of administrative features needed to manage a computer-based test system. As a command center, the dashboard allows administrators to monitor and control the operation of the test system efficiently, ensuring that everything runs according to the established standards.

2) Provides an overview of system status and current activity.

3) Manages the modules or categories of tests available in the system.

4) Management of test participants' data, including registration and active status.

5) A place to configure and manage test questions and answers.

6) Generate reports related to various aspects of the test, including participant performance and data analysis.

7) Additional tools for system administration such as data backup, security settings, etc.

8) Ensures that the server time matches the current time. This function is important to ensure that the time recording during the test is done accurately. If there is a time difference, the administrator is instructed to check and adjust the server's time zone according to the system configuration.

These dashboards not only simplify the administration and management of tests but also ensure transparency and accuracy in the execution of tests. By leveraging these dashbords, administrators can reduce the risk of human error, improve

operational efficiency, and provide a better experience for users and test participants. In addition, accurate server time integration and centralized data management help in ensuring the integrity and reliability of the test system.

IV. CONCLUSION

This study successfully integrated and evaluated the AES-256-CBC within the CAT systems at Politeknik Negeri Bengkalis. The findings conclusively demonstrate that the implementation of AES-256-CBC significantly bolstered data security, sharply reducing the risk of unauthorized access and significantly strengthening user trust in the system's integrity. However, the research also revealed that the success of such security technology is not solely dependent on the strength of its encryption, but equally on the awareness and training of the involved users. Given the ever-evolving landscape of cyber threats, future research needs to go beyond the use of AES-256-CBC to explore other encryption technologies that might offer superior efficiency or security in an educational context. Additional studies are crucial to assess how effective security training can enhance cybersecurity awareness among CAT system users, including staff and students. Furthermore, understanding the psychological impact of data security, such as how security perceptions influence user trust and satisfaction, will provide valuable insights into improving user interactions with security technologies.

Moreover, there is a significant opportunity for innovation in the development and testing of security tools specifically designed for educational systems, which could further refine our methods for protecting sensitive information. Moving forward, continuous collaboration among security experts, educators, and IT technicians will be essential to ensure that our security infrastructure can adapt to evolving threats while supporting educational goals and innovation. This study underscores the critical need for robust encryption methods like AES-256-CBC in safeguarding educational data systems against increasing cyber threats. By firmly integrating advanced security measures, educational institutions can better protect both their operational integrity and the private information of their stakeholders. In turn, this commitment to high-standard security practices not only enhances the functionality of CAT applications but also fortifies the trust placed in them by students, educators, and administrative personnel alike.

To sustain and build upon the successes of this study, the next phase of research should also investigate the scalability of AES-256-CBC across different educational platforms and its effectiveness against a broader array of cyber-attacks. Exploring the integration of multi-factor authentication measures with AES-256-CBC could provide an additional layer of security, further enhancing educational data systems' resilience. These efforts will ensure that our technological defenses not only keep pace with cyber threats but also contribute to a secure and conducive learning environment.

REFERENCES

[1] A. Nusi and M. Zaim, "Philosophy of Education In Digital Transformation: Ethical Considerations For Students' Data Security In Online Learning Platforms," Jurnal Ilmiah Pendidikan Scholastic, vol. 7, no. 3, pp. 42–50, Dec. 2023, doi: 10.36057/jips.v7i3.629.

[2] G. K. Sudhina Kumar, K. Krishna Prakasha, and B. Muniyal, "ACH Reference Model- A model of Architecture to Handle Advanced Cyberattacks," in 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), IEEE, Apr. 2022, pp. 1–6. doi: 10.1109/ICAECT54875.2022.9808076.

[3] O. Trofymenko, N. Loginova, M. Serhii, and Y. Dubovoil, "CYBERTHREATS IN HIGHER EDUCATION," Cybersecurity: Education, Science, Technique, vol. 4, no. 16, pp. 76–84, 2022, doi: 10.28925/2663-4023.2022.16.7684.

[4] D. Kotis and C. Rath, "Strengthening our defenses: The role of the health - system pharmacist in cybersecurity management," JACCP: JOURNAL OF THE AMERICAN COLLEGE OF CLINICAL PHARMACY, vol. 4, no. 6, pp. 662 - 663, Jun. 2021, doi: 10.1002/jac5.1463.

[5] S. W. A. Hamdani et al., "Cybersecurity Standards in the Context of Operating System," ACM Comput Surv, vol. 54, no. 3, pp. 1–36, Apr. 2022, doi: 10.1145/3442480.

[6] A. Carlson, I. Dutta, and B. Ghosh, "Using the Collision Attack for Breaking Cryptographic Modes," in 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, Oct. 2022, pp. 1–7. doi: 10.1109/ICCCNT54827.2022.9984325.

[7] A. Mohammed et al., "Data Security And Protection: A Mechanism For Managing Data Theft and Cybercrime in Online Platforms Of Educational Institutions," in 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), IEEE, May 2022, pp. 758–761. doi: 10.1109/COM-IT-CON54601.2022.9850702.

[8] Y. S. Alslman, A. Ahmad, and Y. AbuHour, "Enhanced and authenticated cipher block chaining mode," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 4, pp. 2357–2362, Aug. 2023, doi: 10.11591/beei.v12i4.5113.

[9] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," Journal of Computer Information Systems, vol. 60, no. 3, pp. 201–211, May 2020, doi: 10.1080/08874417.2018.1432996.

[10] R. Amalia K, A. Wahana, and S. Wardani, "System CAT (Computer Assisted Test) information for Multimedia Department of Muhammadiyah Vocational High School 2 Moyudan Web-based," APPLIED SCIENCE AND TECHNOLOGY REASERCH JOURNAL, vol. 2, no. 1, pp. 30–36, May 2023, doi: 10.31316/astro.v2i1.5048.

[11] J. I. Oladele and M. Ndlovu, "A Review of Standardised Assessment Development Procedure and Algorithms for Computer Adaptive Testing: Applications and Relevance for Fourth Industrial Revolution," International Journal of Learning, Teaching and Educational Research, vol. 20, no. 5, pp. 1–17, May 2021, doi: 10.26803/ijlter.20.5.1.

[12] Y. Choi and C. McClenen, "Development of Adaptive Formative Assessment System Using Computerized Adaptive Testing and Dynamic Bayesian Networks," Applied Sciences, vol. 10, no. 22, p. 8196, Nov. 2020, doi: 10.3390/app10228196.

[13] X. Zhang, M. Xu, G. Da, and P. Zhao, "Ensuring confidentiality and availability of sensitive data over a network system under cyber threats," Reliab Eng Syst Saf, vol. 214, p. 107697, Oct. 2021, doi: 10.1016/j.ress.2021.107697.

[14] A. H. Mahmoud, H. H. Issa, N. H. Shaker, and K. A. Shehata, "Customized AES for Securing Data in Sensitive Networks and Applications," in 2022 39th National Radio Science Conference (NRSC), IEEE, Nov. 2022, pp. 164–170. doi: 10.1109/NRSC57219.2022.9971420.

[15] S. B. George, S. Jaimy, S. Jose, E. Daji, and A. Antony, "A Novel Model to Overcome Drawbacks of Present Cloud Storage Models using AES 256 CBC Encryption," Int J Comput Appl, vol. 183, no. 15, pp. 30–35, Jul. 2021, doi: 10.5120/ijca2021921481.

[16] W. Yaokumah and A. A. Dawson, "Network and Data Transfer Security Management in Higher Educational Institutions," in Research Anthology on Business Aspects of Cybersecurity, IGI Global, 2022, pp. 514–532. doi: 10.4018/978-1-6684-3698-1.ch024.

[17] X. Yin and Y. Chen, "Cyber Risk Recommendation System for Digital Education Management Platforms," Comput Intell Neurosci, vol. 2022, pp. 1–11, Apr. 2022, doi: 10.1155/2022/8548534.

[18] D. Florea and S. Florea, "Big Data and the Ethical Implications of Data Privacy in Higher Education Research," Sustainability, vol. 12, no. 20, p. 8744, Oct. 2020, doi: 10.3390/su12208744.

[19] D. M and J. Dhiipan, "A Meta-Analysis of Efficient Countermeasures for Data Security," in 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), IEEE, Dec. 2022, pp. 1303–1308. doi: 10.1109/ICACRS55517.2022.10029302.

[20] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "Design, Implementation, and Analysis of a Block Cipher Based on a Secure Chaotic Generator," Applied Sciences, vol. 12, no. 19, p. 9952, Oct. 2022, doi: 10.3390/app12199952.

[21] H. T. Assafli and I. A. Hashim, "Security Enhancement of AES-CBC and its Performance Evaluation Using the Avalanche Effect," in 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), IEEE, Sep. 2020, pp. 7–11. doi: 10.1109/IICETA50496.2020.9318803.

[22] M. Shan, L. Liu, B. Liu, and Z. Zhong, "Security enhanced cascaded phase encoding based on a 3D phase retrieval algorithm," Opt Lasers Eng, vol. 145, p. 106662, Oct. 2021, doi: 10.1016/j.optlaseng.2021.106662.

[23] R. Abu Zitar and M. J. Al-Muhammed, "Hybrid encryption technique: Integrating the neural network with distortion techniques," PLoS One, vol. 17, no. 9, p. e0274947, Sep. 2022, doi: 10.1371/journal.pone.0274947.

[24] Y. S. Alslman, A. Ahmad, and Y. AbuHour, "Enhanced and authenticated cipher block chaining mode," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 4, pp. 2357–2362, Aug. 2023, doi: 10.11591/beei.v12i4.5113.

[25] Y. S. Alslman, A. Ahmad, and Y. AbuHour, "Enhanced and authenticated cipher block chaining mode," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 4, pp. 2357–2362, Aug. 2023, doi: 10.11591/beei.v12i4.5113.

[26] C. A. Novianti, M. Khudzaifah, and M. N. Jauhari, "Kriptografi Hibrida Cipher Block Chaining (CBC) dan Merkle-Hellman Knapsack untuk Pengamanan Pesan Teks," Jurnal Riset Mahasiswa Matematika, vol. 3, no. 1, pp. 10–25, Oct. 2023, doi: 10.18860/jrmm.v3i1.22292.

[27] H. T. Assafli and I. A. Hashim, "Security Enhancement of AES-CBC and its Performance Evaluation Using the Avalanche Effect," in 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), IEEE, Sep. 2020, pp. 7–11. doi: 10.1109/IICETA50496.2020.9318803.

[28] O. Trabelsi, L. Sfaxi, and R. Robbana, "DCBC: A Distributed High-performance Block-Cipher Mode of Operation," in Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, SCITEPRESS - Science and Technology Publications, 2020, pp. 86–97. doi: 10.5220/0009793300860097.

[29] Y. S. Alslman, A. Ahmad, and Y. AbuHour, "Enhanced and authenticated cipher block chaining mode," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 4, pp. 2357–2362, Aug. 2023, doi: 10.11591/beei.v12i4.5113.

[30] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," Opt Lasers Eng, vol. 124, p. 105837, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105837.

[31] R. Mott, C. Fischer, P. Prins, and R. W. Davies, "Private Genomes and Public SNPs: Homomorphic Encryption of Genotypes and Phenotypes for Shared Quantitative Genetics," Genetics, vol. 215, no. 2, pp. 359–372, Jun. 2020, doi: 10.1534/genetics.120.303153.