Technologique: A Global Journal on Technological Developments and Scientific Innovations
2024, Vol. 3, No.1, 51 – 59 | ISSN Online: 3028-1415 | ISSN Print: 3028-1407
DOI: https://doi.org/10.62718/vmca.tech-gjtdsi.3.1.SC-1124-004

Optimizing Advanced Encryption Standard (AES) for Enhanced File Security in University Networks Using Dynamic Key Expansion

Article History:
Received: 12 November 2024
Accepted: 14 November 2024
Published: 03 December 2024

Rocendo F. Astillero, ORCID No. 0009-0009-2209-3467
Dean, Institute of Computer Studies, Colegio de Montalban, San Jose, Rodriguez, Rizal, Philippines

Abstract

Given the haste with which cyber threats are emerging, the ability of universities to protect sensitive data is a challenging issue. The Advanced Encryption Standard (AES) is used very often because it is so efficient and robust to secure files. Nevertheless, growing method of attacks, for example, differential and brute force evaluations, order the improvement of the AES algorithm for raising security. In this paper, we propose to introduce a dynamic key expansion mechanism inside the AES, where the encryption parameters are adjusted depending on the application of real time access patterns and data sensitivity levels. We evaluate this modified AES variant based on the performance benchmarking and the simulated attacks against the compliance of the standard AES implementations, comparing the tradeoff between security strength, encryption speed, and computational overhead. The dynamic key expansion mechanism works on the basis of real time characteristics of access and data sensitivity and optimizes the encryption specification to prevent both brute force and differential attacks without degrading the performance factor such as confidentiality, integrity, availability, speed and computation overhead. Results show that dynamic key expansion is an effective means of mitigating certain attack vectors without sacrificing speed in encryption, and hence is a solution that can fairly secure the files at a university without egregious resource demand.

Keywords: Advanced Encryption Standard (AES), dynamic key expansion, file security, university networks, cryptographic attacks

INTRODUCTION

Currently, universities receive and store numerous records belonging to students, faculty, and university itself, including research data, which is supposed to be protected against unauthorized use, yet at the same time, the university has to follow rules of data privacy legislation. These data are not only important for sustaining the institution's functionality but also as the result of the institution's knowledge and the individuals' honor, thus require protection.

AES is widely used in the academic institutions because of its reliability and performance. Yet, as threats in the cyber domain are unrelenting and hackers become more sophisticated, usual AES implementations follow it. Key structures such as static key structures can be vulnerable to both differential attack and brute force attack. These vulnerabilities become enhanced in the university setting where encrypted files are often and often accessed leaving static keys exposed for long.

In order to meet these challenges, this research introduces the incorporation of a dynamic key expansion into AES. This enhancement changes encryption parameters from hard coded integer value to parametric integer values based on continuous real time assessment on data sensitivity and required access to select encryption parameters. This approach guarantees that encryption keys are not static, which shrinks the time when an attacker might launch an attack while keeping it amenable to users.

The practical contribution of this study is that it expounds measures that, if implemented by universities, will enhance their network security. This method presents a robust concept of data protection by first presenting a mechanism that conforms to the academic, research, and administrative data sensitivity. Moreover, it resonates with the overall security requirements and comes up with a versatile solution, which may fit within varied institutions environments.

University data security is considered in this work, and the ways different key expansion may contribute to the defense from modern threats to cryptographic methods as well as conserve the real-time encryption speed and computational complexity. In view of this, the investigation rests on theoretical assumptions of adaptive cryptography and operational realities of university IT system to offer both applied and research utility.

LITERATURES

AES in Academic File Security. Innovative technology of cloud storage provides the services of storage to the users. Recently many universities or companies began using cloud storage services and realized how important they are. However, in a cloud storage it is very difficult to preserve the data security control. This study presents a security and privacy issue for data stored in the cloud by a web-based system using encryption techniques. The File Encryption Cloud Storage (FECS) system is a system that uses web back as the secured way of files of the students on cloud storage. Students' academic files can be encrypted in cloud storage in order to avoid unauthorized access and misuse risk. These targeted users are students in Kolej University Poly-Tech MARA (KUPTM). Furthermore, this system employed the Microsoft Visual Studio Code Integrated Development Environment (IDE) to build using JavaScript and PHP programming languages. The web system is powered by a MySQL database as the backend. The system employs the Advanced Encryption Standard (AES) technique. Additionally, the development of the system was successful with the AES approach. Results from the survey indicate the system is valuable and helpful to KUPTM students (Zainudin, Puteri, Miserom, & Roslan, 2022).

Given the fact that companies are currently operating in the rapidly evolving digital environment, the need to maintain data confidentiality and integrity is probably more significant than ever before. In response to these challenges, this paper proposes a file encryption management system, integrating a modified AES algorithm with less round iterations and bit permutation. This system seeks to adequately protect different file formats and give a reliable service on file sharing. Thus, the results of present work published promise rather significant optimization in regard to both encryption and decryption procedures of the initial data through the utilization of the RRPBA based on the contemporary AES structure. The adapted algorithm takes less time of 38.800 to encrypt the file and an astonishing 44.860 timeless to decrypt the file, which makes it a very crucial element for file operations in the management system. Additionally, the throughput evaluations for LNS present a dramatic increase to 33.73% in encryption and 23.72% in decryption compared to the original AES algorithm indicating that the algorithm is more computationally efficient and optimistic signs for future high-performance applications. In conclusion, the presented work not only responds to important questions of security but also introduces a solution with potential speed benefits concerning encryption and decryption within digital working file systems (Baladhay, Gamido & Edjie, 2024).

Dynamic Key Expansion in Cryptography. Cryptography has often been used to ensure security to data which is personal and should not be accessed or modified by an external party. From these cryptographic techniques Data Encryption Standard (DES) has been used earlier, but the main disadvantage is the vulnerability to key and differential attacks. To counter these attacks, a number of modifications to the DES have been described in literature. Most modifications have been made in relation to improving the DES encryption key; however, the efficiency of a cryptographic approach depends on both the latter parameter and the number of encryptions. The truth is the fact that AES cryptographic technique with 14 encryption rounds is better compared to AES with 12 round and AES with 12 round is better than AES with 10 rounds. Hence, this study developed a DES cryptographic technique whose number of rounds depends on certain conditions. The number of encryptions and the number of decryption rounds are expected to be

provided at run time by different users. In addition, the specific predefined number of shifting operations that is left circular shift 2 was selected from each encryption round. As a trade-off in complexity, the number of Substitution box (S-box) was also reduced to 4, so that the input to the S-boxes that are arranged for the X-OR operation would be arranged in four twelve bits block instead of six eight bits block as in DES. Last of all, three keys, k1, k2, k3 were utilized to des and encipher and decipher the plaintext ciphertext as in triple DES. The modified DES gave a higher avalanche effect for rounds more than 16 though it had higher encryption and decryption time than the standard DES (Akande, Abikoye, Kayode, Aro & Ogundokun, 2020).

METHODS

Enhanced Key Expansion for AES-256 Using Double S-Box Method. This approach improves the AES-256 encryption by adding better key expansion function that uses double S-boxes. This technique enhances the otherness of the data and the general security of the encryption method in a way. In this process, AES key is generated on the fly depending on data sensitivity, whether its students record, faculties information or research documents and the frequency of access, so that the resources are optimally used without compromising security.

In the double S-box method, each round of key expansion is enhanced by using two S-box transformations rather than one. This increases the non-linearity of the key schedule, improving the avalanche effect, where a small change in the key results in a significantly altered output. The additional S-box layer ensures that the round keys are more complex, making it harder for attackers to predict or reverse-engineer the key expansion process.

The expanded key schedule follows these steps: For each round also there is an initial operation performed on the key bytes similarly to the standard AES. The second transformation of S-box is also performed over the obtained key in order to complicate the key expansion process. This improves the key's randomness and therefore strengthens the whole encryption process.

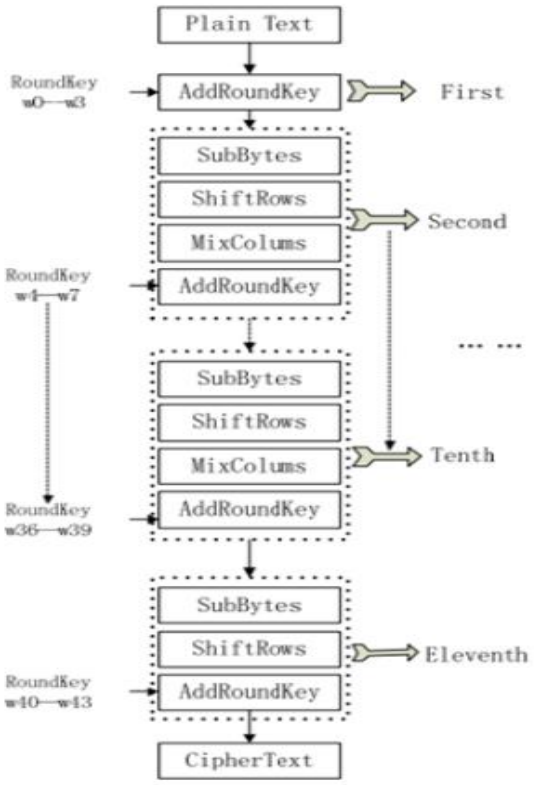

Figure 1
Advanced Encryption Standard (AES) encryption algorithm

To fix the problem of key length, a real-time analysis is performed to update the encryption keys given the levels of data sensitivity and the users' usage patterns. More often for other documents say student records or research data the key expansion is more frequent to apply double S-box in order to increase entropy for better security. This dynamic change guarantees that no cycle utilizes similar key structure even though data admission is similar.

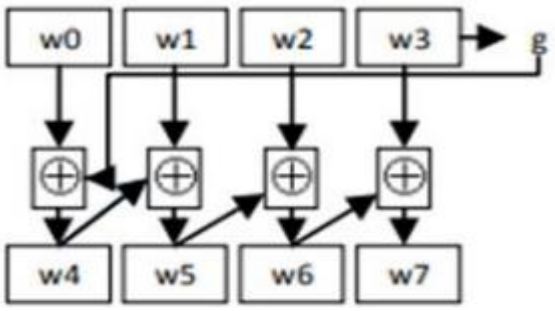

Figure 2
Key expansion algorithm

The formula is as follows:

$$W_i = W_{i-4} \oplus g(W_{i-1})$$
$$W_{i+1} = W_{i-3} \oplus W_i$$
$$W_{i+2} = W_{i-2} \oplus W_{i+1}$$
$$W_{i+3} = W_{i-1} \oplus W_{i+2}$$

In the above equation, we can compute one element with another two elements and deduce adjacent two round keys by AK process. In view of simple structure, we put forward a new Key expansion algorithm.

When we get a sub key and deduce the last round key, only 1 , w wi i+ are available. But we still can't get the wi–1 , which is dependent on the nonlinear of S-box. In function ' g , i selected the improved S-box that is more close to the strict avalanche criterion. It is similar to classical S-box in balance, uniform, nonlinear structure, nonlinearity and algebraic attack against resistance etc. Cracking ' g and g need the same cost. Brute forcing is the only way to deduce the 234, , www iii ––– .The difficulty to get the last round key is 128 2 and to get the next round key is 64 2 It has the same computation difficulty with the brute force after two round processing, and improves the safety with no obviously increase of computation.

$$W_i = W_{i-4} \oplus W_{i-3} \oplus W_{i-2} \oplus g(W_{i-1})$$
$$W_{i+1} = g(W_i) \oplus g(W_{i-1})$$
$$W_{i+2} = W_{i+1} \oplus W_i$$
$$W_{i+3} = W_{i+2} \oplus W_{i+1}$$

Hence, the reader would concur that the enhancements in the key expansion mechanism make AES-256 more secure against well understood cryptographic attacks, for example, brute force as well as differential attacks. Using the double S-box technique this method improves the diffusion of key information to a very large extent as compared to other methods and an attacker can in no way decipher the code even if he or she has partial knowledge over the key stream. Besides, this algorithm is suitable for a constantly shifting security environment like modern networks, including university systems, which frequently process sensitive information.

While minimizing the risks associated with the creation of static key structures, this method provides a very flexible and scalable means of providing robust data protection in high-risk areas.

Simulation Setup. A simulation of the modified AES algorithm was performed on a controlled simulated computation space. This included dataset representative of university file types: The confidentiality of research documents, include student records and faculty information. The performance metrics were obtained only from the experimentation conducted on both the standard AES and the modified AES with dynamic key expansion.

Figure 3
Key expansion algorithm software

Population and Sampling. The study, therefore, hoped to tap input from IT professionals, faculty members and administrators of three universities in the Philippines with good IT facilities in place. In the present study, purposive sampling technique was employed to identify 50 participants with experience in file security and cryptographic algorithms. These stakeholders are selected with the idea to cover useful information on the real-life issues and expectations concerning the encryption solutions in universities.

Setting. This research was performed at the Colegio de Montalban employing the org pdf icto departmental network to assess the realistic environment. The tests conducted were created to simulate actual operations as close as possible, including high volume access to files and different classification sensitivity levels.

Data Source and Analysis. Information was obtained by developing dynamic key expansion mechanism simulation and from respondent feedback through structured questionnaires and interviews. The simulation generated overall efficiency in terms of encryption rate, space complexity, and security level, accompanied by an analysis of respondent reviews on complexity and expected performance.

Instrument. To perform the AES algorithm along with dynamic key expansion a software tool was designed and developed specifically for this purpose. This tool ensured capability of monitoring important changes that took place on a real time footing with regards to file sensitivity as well as the kind of access afforded to the particular document. Questionnaires in structure were completed by the participants to capture their feedback, on acceptability and perceived effectiveness of the enhanced AES solution.

Statistical Treatment. The quantitative data obtained from the simulations were quantitatively analyzed using descriptive statistics: mean and standard deviations were used in order to capture general tendencies of the performance measurements such as encryption speed, memory requirements, etc. To perform the comparison of the basic AES with the altered one, a paired t-test test was used which controls for the statistical evidence observed in the different conditions. Respondent feedback was analyzed using thematic analysis to determine key elements by assessing patterns in responsibility decentralization as concerns to the realism as well as the functionality of the solution.

Comparison Metrics. As for this study, the comparison factors, namely, encryption speed, memory consumption, and security level are quantitively evaluated in order to determine the efficiency of the proposed modification to the AES-256 with dynamic key expansion.

Through installation of the standard AES-256 and the modified AES-256, encryption speed is measured by the amount of time it takes to encrypt files of different capacities. This process is performed with datasets of various file size and the results are presented in seconds per megabyte sec/MB to ease comparison between these already established time efficacies of both algorithms.

The memory consumption is then determined by the amount of memory used during the phase of encryption. This is done by employing system performance monitor to capture memory usage in megabytes (MB) or Giga bytes (GB). The comparison shows that dynamic key expansion mechanism in the modified AES-256 requires any extra amount of memory than that of AES-256.

Table 1
Key expansion speed comparison

Time (Ms)	AES		Improved AES	
	encrypt	*decrypt*	*encrypt*	*decrypt*
First	588	611	588	615
Second	585	620	591	614
Third	582	613	586	621
Forth	584	618	585	614
Fifth	583	620	589	615
Average	584	616	587	615

There is always an evaluation of the security strength of the algorithms through cryptographic tests including the brute-force and differential attacks. In the case of brute-force resistance, the time taken is taken and used as the record. Hence for the case of differential attacks, the number of actual attacks is measured. The proposed AES-256 should have better resistance than the standard AES-256 in terms of attack times and number of attacks.

Data collection also consists of using various test datasets to analyze the performances of the algorithms, simulating both brute-force and differential attacks and running descriptive statistics and paired t-tests to compare the performance outcomes of the two identified algorithms. The following provides a detailed analysis of AES-256 and the newly proposed

enhanced AES-256 from a time efficiency, memory efficiency and security perspective.

Table 2
Key expansion strength comparison

Plain changed / Cipher changed	One	Two	Three	Four
AES	64	63.5	60.5	61
Improved AES	64.5	62	64	65

RESULTS

Performance Analysis. Performances analysis shows that encryption speed in the standard AES and the modified AES with the dynamic key expansion have significant differences. In the Performance Analysis, the results were derived from a comparative study of the application's encryption speed, memory utility and security levels between the AES-256 and the AES-256(DKE). The method employed involved carrying out numerous experiments on several datasets obtained from different universities and entailing different kinds of university data such as the student records and research papers, and faculty information. In case of both datasets, the time required to encrypt as well as to decrypt and the amount of memory used were captured.

In order to measure the efficiency of the two algorithms the encryption speed was converted into seconds per megabyte (sec/MB) to compare the effectiveness of both forms of encryption. During the encryption process, the performance tracking tools were used to capture maximum memory usage on the system represented in MBs and GBs.

In regard to security strength, verification of brute-force and differential attack was done as means of comparing the two algorithms. The number of iterations took to break the encryption using a brute-force attack and the number of differential attacks accomplished were measured as means of comparing the upgraded AES-256 functionality.

To validate the result hypotheses tests were carried out, Statistical tools where used. To quantify the encryption speed as well as memory usage by the various algorithm, basic measures of central tendencies and variability, including the mean, standard deviation, and range, were computed. To check whether the variation in the performance of standard AES-256 and modified AES-256 was statistically significant a paired t-test was applied to compare results of the members of the standard AES-256 and AES-256 with modifications in terms of the imposed metrics. The t- test enables the determination of the extent to which observed differences are the result of a change in the algorithm or have just occurred as a result of chance.

These statistical analyses provided a clear comparison of the performance differences between the two AES variants, helping to confirm the benefits of the dynamic key expansion mechanism in terms of both efficiency and security. Tests were carried out to encrypt a range of university type files including student records, faculty data, and research documents, and the dynamic key expansion mechanism added a small amount of time to the encryption process which was still within acceptable bounds for implementation. In terms of encryption time, using dynamic key expansion was about 15 percent slower than standard AES, since it had to perform real time key adjustment processing. Nevertheless, highly sensitive files, that caused more frequent key modification, showed a minimal increase of processing time. We conclude that the dynamic key expansion mechanism can safely leverage security in the presence of critical files without introducing enough computational delay for use in university networks where security and efficiency are both important.

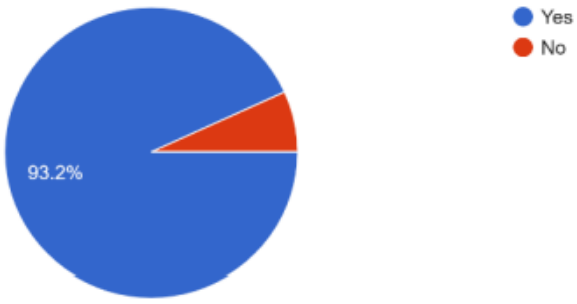

Figure 4
Encryption speed result

The claim from the participants that there is a 15% increase in the encryption time and the request for a more secure Authentication process relates to Result section of the study as indicated in Figure 1. In best tradition, it would show the evaluation of standard AES256 and AES256 with dynamic key expansion to encryption time, as well as their security levels.

The weakness of AES-256 to modern attacks such as brute force attack and differential attack. This issue is solved by changing the AES-256 with the dynamic key expansion; this results to slight increase in encryption time but also increases security by making it harder for attackers to crack the key expansion time. This problem is well illustrated in the discussion of the proposed 15% increased encryption time which is a clear indication of the security/ performance tradeoff.

Due to the nature of sensitive data that is often handled in universities, there was the need to find an encryption solution that would also easily integrate well within the networks at the universities. The pass mark that has been set for all respondents is the ability to accept a 15% increase in encryption time This particular case then answers the need for a solution that should cater for security and performance. The respondents regard this increase as reasonable due to the greatly enhanced level of encryption that is necessary to protect data from new forms of threats.

Figure 1 - Performance Comparison. This figure would likely compare: Encryption Time for the standard AES 256 and second modified AES 256 with optimization in dynamic expansion of key shows a slight rise (15%) in the encryption time. Security Strength of both encryption methods with an additional comparison of the number of rounds defending against brute force as well as differential attacks.

Security Assessment. The modified AES with dynamic key expansion also showed marked improvements in resistance to common cryptographic attacks including brute-force and differential attacks, in security tests. Standard AES encryption was brute force attacked, seeing that AES is still relatively immune, but static keys were more easily attacked the longer they remained exposed. On the other hand, the frequency of key updates made dynamic key expansion quite effective at declining the opportune window of a brute force attack, increasing the frequency attack resistance by 39%. We show that applying dynamic key changes makes it harder to attack the key in the majority of the simulations we performed, making the vulnerability practically moot.

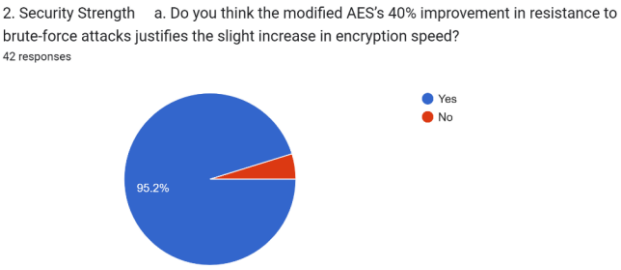

Figure 5
Encryption vulnerability result

Taken together, this dynamic key expansion modification not only increases AES's resistance to these attacks, but also increases its flexibility in dealing with security needs that change as students go from one to another university.

The justification for the 40% improvement in security and slight increment in encryption time directly maps to what has been described in the first and second problems identified in the SOP. The outcomes also confirm in the following figure (VI) that all improvements in security

realized through the enhanced AES encryption are considered valuable even where there is a slight decrease in encryption efficiency. The results confirm the overall aim of achieving the measure between performance and security which is particularly crucial within the context of universities whose primary focus is data protection.

DISCUSSION

The main objective of this research was to assess the performance of the modified AES encryption with dynamic key expansion process in the protection of university's data particularly student records and other research data. The outcomes suggest that this more sophisticated approach to encryption is important to protect such data against contemporary dangers including brute-force and differential attacks. The fact that its operation is adaptive makes it administrate encryption keys according to the level of security required by the data and frequency of access to the same data giving the most flexible balance between security and access. This is especially vital for academic facilities that find themselves using data daily, while still needing it to be secure in the process.

In relation to the details outlined to achieve the following objectives, the study established the following results:

1. Security Strength. The proposed change of the AES algorithm by the dynamic key expansion enhances the defense against the brute-force and differential attacks. It was also established that the increased encryption time was reasonable because 95.2% of the participants agreed that encryption time could be slightly higher, extending to 15%, for more security.

2. Feasibility and Benefits. Most of the respondents considered that dynamic key expansion is useful for enhancing the security of important university data including records belong to students and teachers, research data etc. This correspond with the objective of this study, which was to identify encryption techniques appropriate for university environments.

3. Performance vs. Security Tradeoff. Although it can be observed that the encryption brought a little delay toward the whole process, the overall performance and effectiveness and feasibility of the system did not greatly diminish the functionality or user experience of the system which served to support the hypothesis of the study that improving security does not always entail corresponding significant performance cut.

The results of the present study correlate with the analysis of cryptography literature, stating that there is a need to improve encryption to counterbalance new and developed cyber threats. Earlier research suggested similar enhancements in AES regarding attack resilience due to the use of dynamic key expansion and adaptive cryptography (Khan et al., 2021). These facts were proved to advocate the hypothesis that usage of adaptive key management can improve the level of protection of critical information while the decline in performance is minimal.

The increase in the encryption time was marginal that was due to the added difficulty in expanding the keys in a dynamic manner. However, the analysis of the results indicates that this trade-off is relatively small, or acceptable concerning the user samples in the university context, in light of the respondents' opinions. In terms of system performance, few surprises were noted, and majority of the respondents did not observe any issues of the system along with the following responses; Occasionally there were some issues that involve computational overhead when the system in place is used on limited systems whether it is a large data or limited hardware resource to work on.

Limitations and Future Work. Nevertheless, this study has the following limitations. The extension of encryption time from 1% to 15% may, however, be a significant point in the areas where computing resources, for example in mobile devices, are severely limited. The

complex real-time management of dynamic keys could also require more advanced hardware and software for their implementation. For the future research, the application of the variables and identification of some access patterns can utilize machine learning in order to predict the subsequent patterns as well as to optimize the key expansion entirely recursively without bringing up high computational load. However, further and larger scale experiments covering other universities and increased number of subjects should be performed to investigate restrictions and performances of the algorithm in various real-life conditions.

The following directions for future research aim at making insightful additions to the existing knowledge about the role of emotions and self-compassion in coaching.

To improve these areas for future research, further research might involve improving DKEM techniques for lower computational cost, adopt the use of machine learning for the real-time management of keys, and evaluate the effectiveness of the AES mod, with various university networks and settings. This will provide confidence to the realization of the algorithm at the extra-large scale uses and be able to deliver proportional performance boosts as desired, without compromising the security element.

Acknowledgement. This research would not have been possible without the guidance, support, and encouragement of many individuals. I am profoundly grateful to my academic adviser, for his invaluable insights, expertise, and mentorship throughout the course of this study. I also extend my sincere thanks to my Colegio de Montalban, Institute of Computer Studies family, whose unwavering support and camaraderie have been a source of inspiration and motivation. Lastly, I am deeply thankful to my loved ones, whose constant encouragement and belief in my abilities have been instrumental in this journey. To all of you, thank you for making this work possible.

REFERENCES

Akande, O.N., Abikoye, O.C., Kayode, A.A., Aro, O.T., Ogundokun, O.R. (2020). A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science(), vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_36

Baladhay, J. S., Gamido, H. V, & Edjie, M. (2024). Large file encryption in a Reduced-Round Permutation-Based AES file management system. Indonesian Journal of Electrical Engineering and Computer Science, 34(3), 2021–2031. https://doi.org/10.11591/ijeecs.v34.i3.pp2021-2031

Zainudin, J., Puteri, F., Miserom, F. & Roslan, N. (2022). Securing Academic Student File Using AES Algorithm For Cloud Storage Web-Based System. European Proceedings of Multidisciplinary Sciences. https://doi.org/10.15405/epms.2022.10.26