El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

THE NEED FOR DYNAMIC RANDOMIZATION ADVANCED ENCRYPTION STANDARD (DR-AES) ALGORITHM

M. Adamu[1], O.I. Oyefolahan[2], O.A. Ojerinde[3]
[1]Department of Computer Science, Federal Polytechnic, P.M.B. 55, Bida, Niger State
[2]Department of Information Technology, Federal University of Technology, Minna, Niger State
[3]Department of Computer Science, Federal University of Technology, Minna, Niger State
Corresponding Author: bejian2004@gmail.com

Abstract

This article provides an overview of the various techniques to improve security and performance of the Advanced Encryption Standard (AES). The techniques discussed cover AES algorithms, including key extension methods, dynamic encryption, shift registers, rounding, hardware architecture, and dynamic SBOX. Several articles were reviewed in the field of AES published from 2017-2023, in which related papers were obtained from Google Search, ACM, IEEE explore and Google scholar. Research and innovation in these areas aim to strengthen AES against emerging threats, improve its resilience to advanced cryptanalysis techniques, optimize performance across platforms, fix vulnerabilities in hardware implementations, and provide long-term security in the face of ever-evolving threats. With the increasing reliance on online application, distributed systems architectures and slow symmetric encryption diffusion property in AES algorithm, there is a growing need for Dynamic Randomized AES to safeguard data in dynamic and potentially untrusted environments. Continuous research and development of Dynamic Random AES techniques will enhance a robust and reliable encryption standard to protect sensitive information.

Keywords: Encryption, decryption, round key, S-Box, Mix Columns, cipher

1.0 Introduction

Technology is the backbone of contemporary society, impacting everything from governance and market systems to international commerce, travel, and communication. The digital revolution, propelled by the emergence of the Internet and the World Wide Web, has made our society more advanced and efficient. The virtual realm offers numerous advantages and fosters unparalleled connectivity. Platforms like Facebook, Facebook Messenger, WhatsApp, YouTube, and QQ instant messaging have significantly contributed to the surge in internet utilization. This trend is supported by other research findings, which indicate a higher prevalence of social network usage among internet users in developing countries. [1]. Over recent years, there has been a swift advancement in technology, particularly with the emergence of wireless and mobile communications, which has resulted in a substantial growth in Internet usage. The introduction of new wireless applications and technologies contributes to the daily exponential surge in the volume of electronic data [2].

Furthermore, due to these new technologies, we are not able to protect our private data, so the number of cybercrimes is increasing day by day. Currently, more than 60% of commercial transactions take place online, which requires a high level of security. The scope of cyber security is not limited to information protection in the IT area, but also includes various other areas, such as cyberspace. They also require a high level of

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

security as they store vital information about an individual whose security has become a necessity. [3].

Alternatively, the primary perpetrators of cybercrime are often dissatisfied individuals within the organization itself, who may not possess advanced knowledge of cyberattack techniques. Their intimate understanding of the system in question typically grants them the ability to launch attacks or exfiltrate sensitive information with ease. In a different vein, terrorists pose a distinct kind of threat, aiming to demolish, incapacitate, or nefariously manipulate crucial infrastructure. Their actions are intended to compromise national security, inflict significant human losses, destabilize the economic foundation, and erode the collective confidence and morale of the public. Figure 1 depicts the various origins of cyber threats [4]

Fig 1: Sources of cyber threats [4]

The two charts in Figure 2 and 3 provide an overview of the number of cybercrime reports reported in the United States from 2007 to 2016.

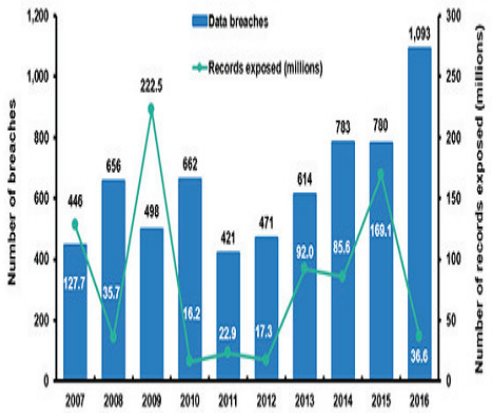

Fig 2: Numbers of breaches from the year 2007 up to 2016

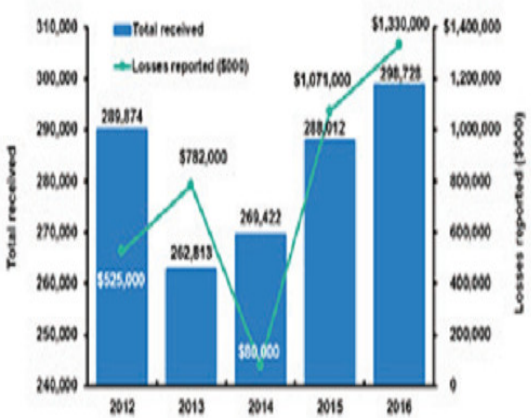

Fig 3: Numbers of complaints from the year 2007 up to 2016 [5]

Despite adequate security measures, cyber-attacks are increasing rapidly. This can come in the form of malware, phishing, password attacks, hyperlink downloads, and virus attacks [6]. According to the Indian Economic Times, encryption takes care of the process of converting plaintext to gibberish and vice versa. It is a means of storing and transmitting data in a specific form so that only those for whom it is intended can read and process it. "Cryptographer" comes from the Greek words kryptos (krnptos), meaning hidden or secret, and praphia (graphia), meaning to write. Cryptographic Algorithm is the study of techniques to ensure confidentiality and authenticity of information [7]. The simple

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

working of encryption and decryption functions is shown in Figure 4.

Fig 4: Working of encryption and decryption [8]

Symmetric and asymmetric encryption are two prevalent forms of encryption techniques. Symmetric encryption, or symmetric key encryption, ensures secure communication between the sender and receiver through a shared secret key. On the other hand, asymmetric encryption, also known as public key encryption, facilitates secure communication using a pair of keys, one public and one private, with the private key kept secure. In both symmetric and asymmetric encryption, the size of the key plays a crucial role in securing communication. Symmetric encryption uses a smaller key size compared to asymmetric encryption, which can make it comparatively less secure for protecting highly sensitive data. [9]. The computation time for cryptographic methods is broken down into the time it takes to encrypt/decrypt, generate keys, and exchange keys. The time to encrypt and decrypt involves transforming plaintext (the message) into ciphertext and back again. The duration required to generate keys is influenced by the length of the key, which varies between symmetric and asymmetric encryption. Meanwhile, the time for key exchange is influenced by the communication pathway between the sender and receiver, as depicted in Figure 5 [9].

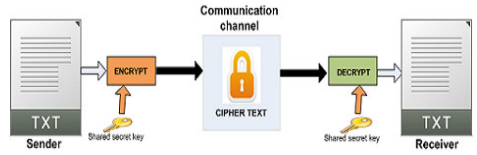

Fig. 2. Symmetric Cryptography

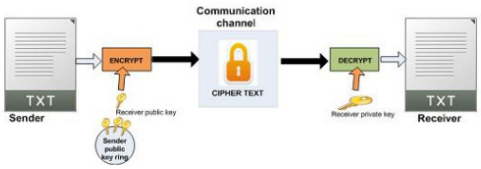

Fig 5: Symmetric cryptography [9].

Numerous cryptographic algorithms exist to safeguard information, including DES, 3DES, Blowfish, AES, RSA, ElGamal, and Paillier, each with its distinct characteristics. The challenge lies in identifying the most effective security algorithm that provides robust protection while efficiently generating keys and encrypting and decrypting data. The choice of security algorithms hinges on the specific strengths and weaknesses of each algorithm, as well as their appropriateness for various applications and the requirements they must fulfil [9]. The basic classification of cryptography also be shown in figure 6.

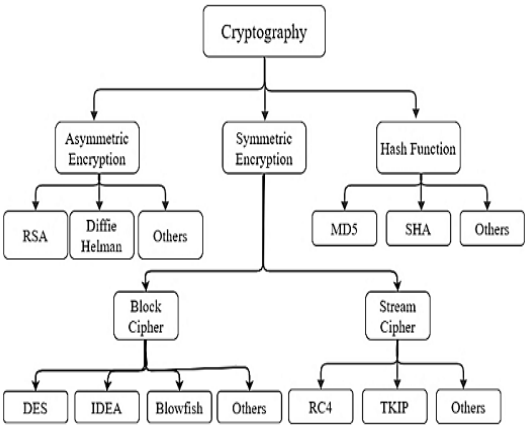

Fig 6: Basic Classification of Cryptography [10]

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

2.0 AES Algorithm

Early on January 2, 1997, the National Institute of Standards and Technology, part of the United States of America, announced the start of efforts to build an AES. At the time, NIST enlisted the world's top cryptographers for help by presenting their thoughts or perspectives on the accurate computation of cryptography that would be dubbed the "Advanced Encryption Standard" and would become established in its curriculum, with 15 computations identified as having potential were and on the growing hopes grew AES. NIST's goal is for AES to demonstrate uncategorized, disclosed, and accessible gibberish cryptographic computations to the world [11].

AES's primary strength lies in its substantial key sizes of 128, 192, and 256 bits. With a 128-bit key, for example, breaching its security would require navigating through 2^128 possible combinations, making AES a highly secure protocol. Its mode of operation, consistent across both encryption and decryption processes, can be challenging to execute in software. Despite this, AES is extensively utilized across various domains such as internet privacy, wireless communications, business dealings, and the storage of messages, data, voice, or images, owing to its robust security features [12]. Data and information security is a central challenge in cloud services. Therefore, it is of vital important to use a preventative method to protect your data and information. There is a preventative method called encryption that can be used to prevent an intruder from having access to certain information. The proposed encryption algorithm involves a symmetric cryptographic key called the encryption and decryption key. The AES algorithm was proposed for data transmission security [13].

The algorithm employs a structured sequence of repeated rounds for encrypting and decrypting sensitive information, making it applicable across both hardware and software globally. Cracking AES-encrypted data to retrieve the actual information poses a significant challenge due to its complex encryption process. No evidence was found until the day this algorithm was cracked. AES has three different key sizes, such as AES 128, 192, and 256 bits, and each of these ciphers has a block size of 128 bits. However, the brief appearance of the cipher means that it performs calculations on blocks of data [14].

The Advanced Encryption Standard (AES) can be implemented on a variety of platforms such as microcontrollers, CPUs, GPUs, and FPGAs. For example, OpenSSL is a full-featured commercial cryptographic toolkit for TLS and SSL that supports various AES modes of operation such as Electronic Code Book (ECB), Encryption Blockchain (CBC), and Exit Feedback (OFB) [15]

The AES algorithm closely mirrors the Rijndael algorithm, with distinctions primarily in block and key sizes. Rijndael supports variable block lengths and key sizes, which can be chosen as multiples of 32 bits within the range of 128 to 256 bits. Conversely, AES standardizes the block size at 128 bits, while restricting key sizes to 128, 192, or 256 bits only. The number of encryption rounds in AES is determined by the chosen key length. An illustration of the encryption process for a 10-round AES algorithm is provided in figure 7 [16].

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

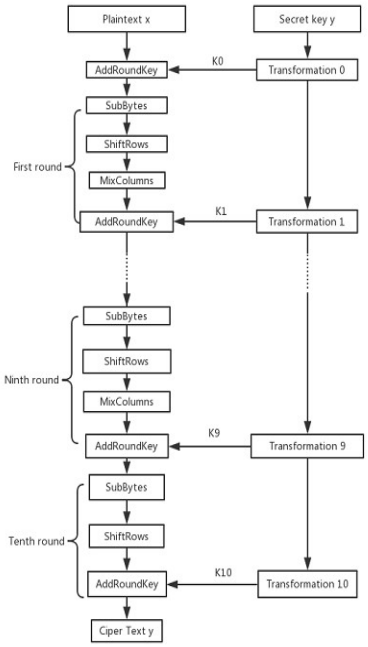

Fig 7: AES encryption process [16].

The AES algorithm's architecture is built around four fundamental operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. These operations are applied sequentially to the entire 128-bit block of plaintext, often referred to as the algorithm's state. This state is structured as a matrix containing 16 bytes, arranged in 4 rows and 4 columns [16].

i) Substitution Byte: Works in any state. it can replace the standard S-Box shown in Figure 5. Example: Replace b14 with S-Box instead of a14. It consists of a total of 256 numbers in the table. LUTs is use for substitution and there are different ways to calculate S-Box values. LUT offers less hardware wear and tear, reduces latency and processing time as shown in figure 8.

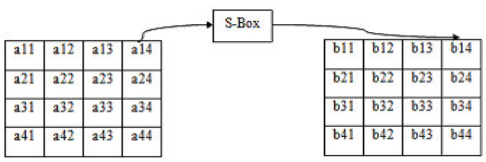

Fig 8: Substitute byte operations [12] [17].

ii) Shift rows operation: On matrix rows, operation will be performed. Here first row kept same, 2nd, 3rd and 4th row shifted cyclically left by 1 byte, 2 byte and 3 byte given in Figure 9.

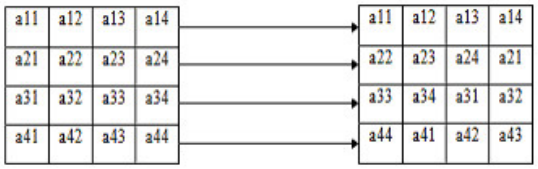

Fig 9: Shift rows operation on states [12] [17].

iii) Mix column operation: Current state matrix and standard matrix obtained from polynomial multiplied and evaluated in figure 10. Multiplication can be done on matrix of shift row output.

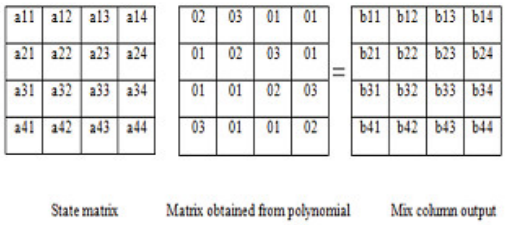

Fig 10: Mix column operations [12] [17].

iv) Add round key: XOR operation performed on each state of matrix. Hence, each byte of round key and current state matrix is XORed.

Add round key = State matrix $\oplus$ Round key

1

Key expansion operation: key expansion consists an array of 176-byte (44 words) key, called as expanded key which serves as the expansion combination of four bytes (word) as shown in figure 11.

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

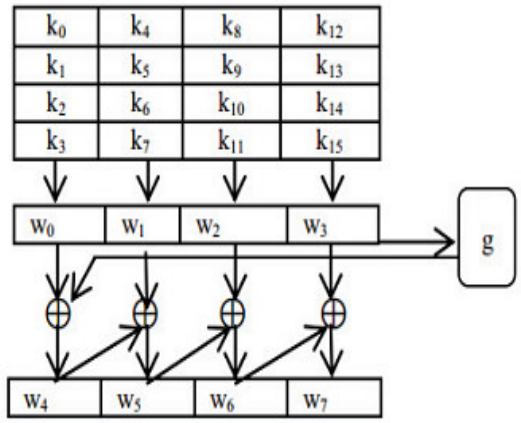

Fig 11: Key expanding algorithms [12] [17].

However, AES cryptanalysis has not stopped and many researchers are looking for new approaches that will allow us to achieve competitive performance [18]. The hardware implementation of AES encryption is very important for accelerating system performance, but it also raises concerns about protecting AES from side-channel attacks (SCA) [19].

The cipher values of the cipher algorithm are randomized using different diffusion elements like addition, rotation, transposition, etc. Such processes on the diffusion elements are repeated several times or in several cycles in order to achieve a sufficient degree of diffusion [20]. Among the biggest disadvantages of the AES algorithm is the fact that cyber-attacks are constantly evolving; Therefore, security specialists in the lab must be busy devising new plans to stop the attackers [21] [22]. Although AES is safe, there is still room for improvement, particularly in its diffusion properties, as it has been observed that the rate of diffusion is initially quite slow [23].

3.0 Enhanced AES Algorithm

[24] introduced a dynamic algorithm that defines the exact steps used to encrypt or decrypt payloads at runtime. This was achieved by entering AES parameters instead of reusing fixed and default values. The resulting encryption works very similar to AES. However, how exactly the rounds function works depends on a few bytes of the encryption key. Further analysis is required to assess the actual benefits of adopting these changes. In addition, extensive implementation of this technique is required to properly analyse the performance costs of these changes.

[25] showcase an AES implementation that utilizes a low-power shift register combined with ADOC and RTPG triggering techniques, enhancing the AES design's performance. The selection of a shift register architecture among various options is due to its advantages in terms of lower power usage and reduced size relative to alternative architectures. The overall configuration of the system is depicted in Figure 12.

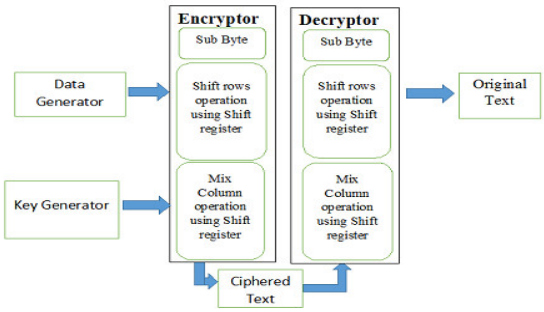

Fig 12: Improved AES block diagram [25]

The proposed AES design shows 29.32 percent improvement in power consumption over register renaming based AES design. However, using shift register in AES can easily result in low parallelism and clock dependency [25].

[26] implemented AES-128 with parity-based error detection techniques and nested parity generation, which requires no additional hardware due to the AES algorithm's vulnerability to spurious attacks. Parity-based error detection incorporates an additional bit, known as the parity bit, into the data that is either transmitted or stored. This method employs either even or odd parity. Odd parity is defined when the count of '1' bits in the data is odd, while even parity occurs when this count is even. While the conventional method of generating parity can identify stuck-at errors, it is ineffective for detecting transposition errors. To address this issue, parity is verified both at the end of each round and at the beginning of the next. A change in parity between these checks indicates an error. This technique of error detection is applied at various stages within the AES encryption process to identify errors. This approach was implemented using Modelsim AES simulations with and without error detection. However, the detected error was not fixed automatically, it was fixed manually.

[27] introducd a polymorphic variant of the AdvancedfEncryption Standard. With P-AES, the values of the AES parameters change with each new key. Exact values are only available to authorized communication partners at runtime. To achieve these goals, the fundamental transformations of AES, SubBytes, ShiftRows and Mix Columns in the proposed P-AES were crucial.The proposed P-AES can support 16, 24 or 32 byte keys. However, for consistency, the key length is assumed to be 32 bytes based on the following equation.

$$key = [byte_0|byte_1|byte_2|$$
$$\ldots.byte_{28}|byte_{29}|byte_{30}|byte_{31}|] \quad (2)$$

In addition, P-AES encryption uses a uniform level of ambiguity to prevent a potential attacker from discovering the exact details of how the encryption works. The avalanche criterion was tested and the P-AES values for the main avalanche and the manifest avalanche were 0.495 and 0.504, respectively. Since P-AES is a new technique, it may face challenges in adoption and implementation.

[28] explore different strategies to enhance the hardware efficiency of the AES algorithm's Rijndael S-box, focusing on reducing delay and minimizing the count of logic elements within the Altera Cyclone IV FPGA framework. This investigation utilized the Intel Quartus II software alongside the Verilog Hardware Description Language (Verilog HDL) for implementation. The computation of the Rijndael S-box was conducted through the affine transformation method in the Galois Field (GF)(2^8), employing the input vector signal "X" in the process.

$$GF(2^8) = \frac{GF(2)[X]}{(x^8+x^4+x^2+x+1)} \quad (4)$$

The algorithm utilizes the polynomial represented by the binary string "100011011" for Boolean addition operations. Three design strategies were explored: parallelization of the S-Box, generating smaller Lookup Tables (LUTs) from the standard Substitution Box, and implementation using Verilog HDL in Quartus. The initial setup resulted in an average delay of 11.41 nanoseconds and utilized 208 Logic Elements (LEs). The first design iteration increased the average delay by 0.11 ns for Design 1 and 0.52 ns for Design 2. However, Design 3 exhibited superior efficiency compared to the original LUT; it managed to produce the correct output 1.08 ns quicker and consumed 31.3% fewer LEs. However, design 3 uses Shannon's expansion theorem which does not inherently provide a structured or hierarchical representation of the multiplexer circuit and making it harder to optimize the circuit.

[29] introduced AES that was modified using a dynamic SBox that depends on the key and compares the snowball effect of base AES with our proposed algorithm. The proposed algorithm consists of the same tricks used in

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

simple AES. In this case, the key-dependent SBox is generated by performing operations on the underlying SBox and therefore does not violate the underlying AES design, but rather enhances the security of the underlying AES. In this approach, the dependent key is generated by computing an individual dynamic SBOX for encryption and decryption after generating a standard AES SBOX. The developed algorithm can be used where security has top priority. However, implementation of the method was limited to smaller samples, and the algorithm was not extended to AES-192 and AES-256 for better implementation and analysis.

[30] introduced an efficient Differential Power Analysis (DPA) technique tailored for the Advanced Encryption Standard (AES), aimed at decreasing the susceptibility to secondary attacks and lowering the overall cost of attacks. This DPA method's goal is to capture various energy traces produced by the cryptographic device during the encryption or decryption of data, and to deduce the device's secret key from these traces. The DPA methodology unfolds in four main phases: identifying an intermediate value within the cryptographic algorithm, recording the power traces, computing the intermediate value, and associating these intermediate values with corresponding energy consumption metrics. During the experimentation phase, a correlation coefficient was employed to ascertain the relationship between the hypothesized power consumption figures and the actual power waveforms, as delineated in equation (5).

$$r_{i,j} = \frac{\sum_{n=1}^{N}(h_{n,1}-\overline{h_1}).(s_{n,j}-\overline{s_j})}{\sqrt{\sum_{n=1}^{N}(h_{n,1}-\overline{h_1})^2.\sum_{n=1}^{N}(s_{n,j}-\overline{s_j})^2}} \quad 5$$

where $r_{i,j}$ is the element of the $i-th$ row and $j-th$ column of the matrix $R(i = 1,2 \ldots j = 1,2 \ldots .T)$ represent the correlation coefficient of $i-th$ column vector of H and $j-th$ column vector of $S, h_{n,1}$ and $s_{n,j}$, $\bar{h}$ and $\bar{s}$ represent the average value of $h_{n,1}$ and $s_{n,j}$.Finally, two attacking experiments base on analytical method for AES are performed. Experimental results proved that the key of the AES can be cracked and DPA methods were effective. However, the information system security was not protected in the DPA approach.

[31] conducted a comparative study of two encryption algorithms, namely Advanced Encryption Standard (AES) and Rivest Shamir Algorithm (RSA). Their goal was to determine which algorithm was the most reliable based on factors such as encryption time, decryption time, key length, and encryption length. The Rivest Shamir algorithm requires keys with at least 1024 bits for good security, while 2048 bits provide the best security. RSA is used to encrypt data to ensure that only authorized users can access it. Research has shown that AES is more efficient because it offers faster encryption and decryption times and requires shorter ciphers and keys than RSA. In contrast, RSA takes more time to encrypt and decrypt and requires longer ciphers and keys.

Ashqi and Haval, 2023 presented a new approach to image encryption using the AES algorithm and Henon card. First, the raw image is encrypted using the AES algorithm. A random key was then generated using the Hénon card, which was needed for the second encryption step, which was carried out using the XOR operation. In this method, users attempt to load an encrypted file as input to the application and are prompted to enter the generated password for decryption. Without the correct password, the data remains inaccessible. The decryption process mirrors the encryption algorithm, allowing the processes to be easily reversed. Research suggests that this technique effectively solves problems of traditional encryption methods, although its application is currently limited to image encryption.

[32] used the advanced AES-128 (Advanced Encryption Standard) algorithm to encrypt messages and the LSB (Least Significant Bit)

algorithm to embed the ciphertext into the image. In particular, they improved the key scheduling process by including unique identifiers for sending and receiving requests. Therefore, even if a single message security algorithm was used without the addition of a public key algorithm, the message was indirectly protected by two keys. These keys included security in the form of a public key derived from the sending and receiving application identifiers and a private key derived from the entered message key. The results of the study showed that eavesdroppers had difficulty detecting the presence of ciphertext. Furthermore, even if the eavesdroppers were able to obtain the ciphertext and encryption key, the message would have remained unintelligible on their mobile devices due to the changing application identifiers associated with the message. However, the authors recommended exploring better algorithms for future applications, particularly those that improve the process of embedding ciphertext into images.[33] proposed increasing text security by combining the AES cryptographic algorithm with LUC. This combination of two cryptographic algorithms was proposed to achieve a higher level of security. AES, which is known for its efficiency and low computational cost, was chosen as the preferred symmetric algorithm. On the other hand, the LUC algorithm derived from RSA was used as an asymmetric algorithm, which has the advantages of higher security and processing speed. Specifically, AES-128 was used, which uses 10 rounds in the encryption and decryption processes, using the LUC algorithm to protect the AES key. The study demonstrated the successful integration of AES and LUC algorithms. However, it was found that using these combined algorithms increased the computing time required for encryption and decryption operations.

[34] presented a revised architecture for Internet of Things (IoT) aimed at enhancing cross-media energy management applications. This novel framework merges two distinct management methodologies: a distributed approach and an integrated approach. According to their model, power generation units at the first layer autonomously control their supply and demand metrics through distributed management. Subsequently, at a secondary level, each unit acts as an agent in a broader competitive marketplace to achieve an optimal operational status. Furthermore, this approach incorporates a protocol for generating data blockchains based on the Advanced Encryption Standard (AES) within the IoT infrastructure, which is then synchronized with cloud technology. computing model inspired by the PSO algorithm, creating an integrated approach to data management, energy and Data security. The results of this approach suggest a significant reduction in the volume of data transactions and therefore the time required to reach a final consensus, while achieving the desired results.[35], analysed the AES encryption standard and its security aspects. Security analysis is important to evaluate the usability and stability of an algorithm. This assesses whether potential attackers, even if they understand the structure and processes of the algorithm, are still unable to decrypt the key. In this context, attackers should spend more time on important attacks rather than exhaustive methods of dealing with this algorithm. When conducting -AES security analysis, it is important to consider the algorithm's resilience to several key attacks. The research results showed that traditional AES shows resistance to brute force attacks when analyzed in terms of temporal security. AES with a key length of 128 bits and more is also resistant to quadratic attacks. However, the study concludes by highlighting the need to improve the AES algorithm, as suggested in other studies, to increase both performance and security.

[36] introduced an advanced implementation of the encryption standard in a Field Programmable Gate Array (FPGA) with minimal resource consumption. Experimental

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

results show a hardware structure with high bandwidth and area efficiency. To increase productivity and minimize resource allocation, a parallel design and data transfer mechanism with an optimized S-Box are introduced. In the proposed method, each cycle was treated as a pipeline phase by dividing the critical path into multiple blocks using appropriate registers. In addition, S-box optimization was proposed using a residual bootstrapping system instead of the Galois box method, resulting in a reduction of 12.42% in lookup tables (LUTs) compared to previous approaches. This optimization not only reduced the LUT, but also minimized memory consumption and required minimal latency. However, it should be noted that this method has not been extended to the implementation of application-specific integrated circuit (ASIC).

[37], a three-tier hybrid cloud storage security model that leverages the Advanced Encryption Standard (AES) was proposed to address security issues. In the first phase, the data was encrypted using the AES algorithm, using a key shared between the user and the cloud server. In the second phase, a data integrity checking algorithm was applied to ensure that the archived data remained unchanged. Finally, a transmission security layer is applied to protect the data transmission between the user and the cloud server. During the encryption process, the data was encrypted using AES with a 16-bit key and then embedded into the cover image in step of the steganography. The general architecture of the method is shown in Figure 13.

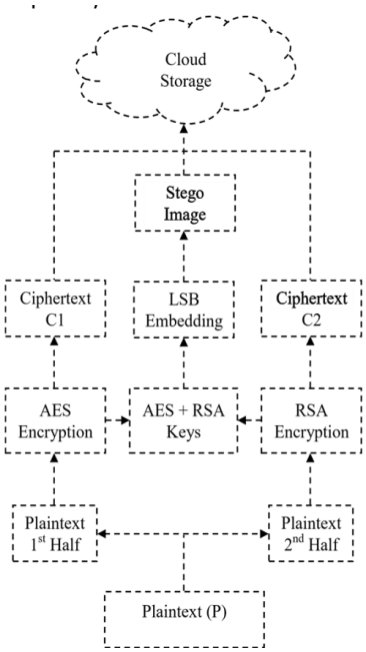

Fig 13: visualizing the Architecture of the proposed Hybrid model

Combining the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) and Least Significant Bit (LSB) techniques creates a hybrid model that is suitable for both cryptography and steganography purposes. The results show that although the decryption process takes longer than encryption, the delay is minimal. Users don't have to wait long; Your data will be encrypted or decrypted within seconds. Furthermore, this research can be extended to include hybrid data transfer techniques and steganography to improve overall data security.

[38], an improved version of the Advanced Encryption Standard (AES) algorithm called Optimized Advanced Encryption Standard (OAES) was proposed. The OAES algorithm uses a sine map and a random number to generate a new key, which increases the complexity of the generated key. Additionally, a multiplication operation is applied to the original text, creating a 4x4 random matrix before five passes of the encoding cycles. Instead of a fixed S-Box, a Random Replacement Box (S-Box) is

used.Extensive tests were conducted, showing that even with the same password and input text, different encoded texts were produced each time. This dynamic change in the encoded text indicates that the proposed algorithm is highly resistant to attacks.

[39] enhanced AES performance by incorporating extra encoding, decoding, compression, and expansion layers to reduce processing times. This research juxtaposed the encryption durations of traditional AES against an enhanced AES setup, conducting tests across various file formats such as a 2500KB JPG, 5MB MP3, and 10MB MP4, averaging the outcomes over three trials. Findings revealed that the refined AES approach, while more efficient, demands greater memory usage than its standard counterpart, particularly in the decryption phase.

[40], provides modification for modifications AES algorithm, specifically focusing on improvements in S-box and mix columns operations. The basic AES algorithm faced limitations where the S-box and polynomial matrix were generated every time the algorithm initialized, leading to increased execution time as input data size grew. The modified AES operates differently by generating the same S-box and inverse S-box every time the algorithm is initialized. The S-box is constructed by finding inverses of all elements in GF (28) and applying affine transformations. The modified AES version utilized a fixed S-box and inverse S-box in the form of a 16x16 matrix. Testing on ANDROID devices showed a 70% improvement on average in the efficiency of AES for encrypting and decrypting text, audio, and image files. However, the method requires larger memory due to storing predefined S-boxes and polynomial matrices in arrays.

[41] presented an efficient and compact key expansion scheme implemented on the AES (Advanced Encryption Standard) to secure backup files in the system. Additionally, John (2023) introduces MAES, a lightweight version of AES designed to meet specific demands. MAES features a novel 1-dimensional Substitution Box derived from a unique equation for constructing a square matrix during the affine transformation phase. MAES employs a multiplicative inverse table for arithmetic operations and an affine transformation process involving 4x4 square matrix multiplication and 4x1 constant column matrix addition. Implemented in nes C language supported in Tiny OS 2.1.2, MAES demonstrated improved efficiency in Resource Constraint Environments (RCEs). Analysis revealed that MAES consumes less energy than AES, with an efficiency rate of around 18.35% in terms of packet transmission, making it a preferable choice for RCEs compared to AES.

[42], introduced a new hybrid encryption algorithm called EMAES, which combines the performance of MAES (Modified Advanced Encryption Standard) and the security of ECC (Elliptic Curve Cryptography). EMAES increases AES performance over MAES and ensures greater security over ECC. The EMAES decryption process mirrors the encryption process. The recipient generates a public key and a private key and a shared key using the sender's private key and public key. This shared key is then used in the MAES algorithm as a secure key to decrypt the encrypted data. EMAES offers the advantages of AES, higher speed with MAES and more security with ECC. The algorithm has been implemented and tested in MATLAB and an Android chat application, although it has not been evaluated on an FPGA, multiple devices over the Internet, or in a cloud computing environment. [43] proposed a hybrid modeling approach involving a combination of several symmetric block ciphers and stream ciphers, mainly AES-GCM, Chacha20 Poly-1305, Multi

El-Amin University Journal of Computing (EAUJC).
Vol. 1, Issue 1, April, 2024

Journal Homepage: https://www.eaujc.el-aminuniversity.edu.ng

Fernet and Ferne. This method transfers the user-supplied Fernet key and decrypts the encrypted key store, resulting in separate keys for AES-GCM, Chacha20 Poly1305 and Multi Fernet. Each encrypted segment is decrypted with the corresponding AES-GCM, Chacha20 Poly1305 and Multi Fernet decryption keys, which are applied in a circular manner depending on the encryption method used. However, the developed model has not been implemented in a real-time environment to encrypt data in transit and storage.

[44] introduced improvements to the chaos theory-based Advanced Encryption Standard (AES) mathematical model for encryption and decryption. The AES key was derived using logistic mapping and Chebyshev mapping, and random words were introduced to increase the randomness of the key. The study used two chaos mappings to generate optimal random sequences, and bitwise XOR was applied to these sequences to generate a chaotic key stream that served as the starting key for AES. This improved mathematical model used two-dimensional chaotic mappings to generate the key flow. The model was developed and subjected to rigorous safety testing and passed the NIST test with flying colours. In particular, the improved model proved to be very efficient, performing encryption and decryption operations in just a third of the time compared to AES. These results highlight the effectiveness and reliability of an improved mathematical model for data encryption and decryption in communication networks.

4.0 Quantity of Articles in terms of Record

The study time line in terms of the articles reviewed from different sources are given in figure 14, table 1 and figure 15 respectively.

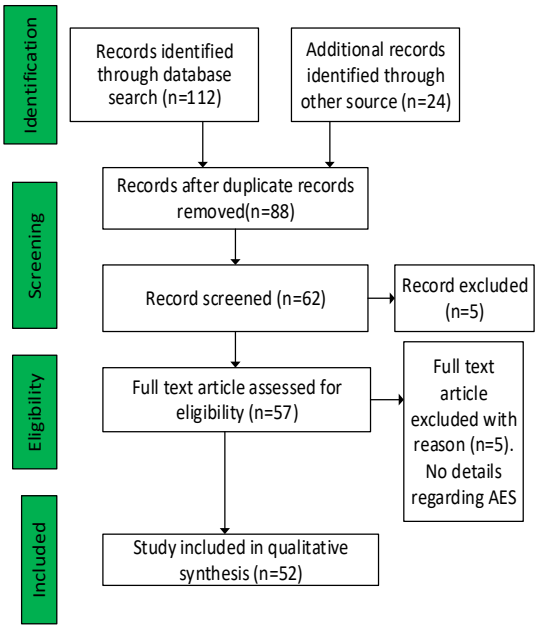

Figure 14: Reviewed flow with PRISMA

Table 2: Time line of reviewed articles

Years of Publication	Quantity Reviewed	Percentage (%)
2017	3	7
2018	8	17
2019	10	21
2020	9	19
2021	7	15
2022	2	4
2023	8	17
Total	47	100

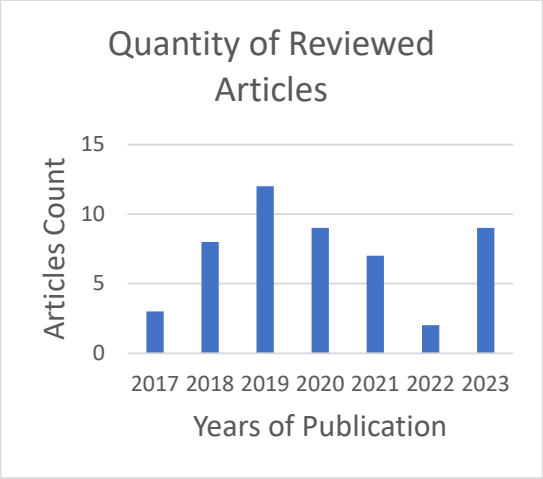

Fig 15: Reviewed trend from 2017-2023

5.0 Needs for Dynamic Randomized AES

The Dynamic Randomized AES will combat advanced cryptographic attacks that will exploit vulnerabilities in static key-based encryption systems. It incorporates dynamic randomization to introduce additional complexity and unpredictability, making cryptanalysis and brute-force attacks more difficult for hackers. By regularly changing encryption parameters like the key or initialization vector, the system becomes more resilient to long-term compromises and data breaches. Dynamic Randomized AES will effectively eliminate new threats and adapts to changing attack techniques that will ensure the encryption system remains secure from persistent attackers. The motivation for implementing this approach, is to increase the security of confidential information and protect it from unauthorized access.

6.0 Conclusion

The existing techniques provides a crucial role in ensuring the security and effectiveness of the Advanced Encryption Standard (AES). By subjecting AES to rigorous analysis, including cryptanalysis and side-channel attacks, the vulnerabilities and weaknesses can be identified and addressed, contributing to its overall robustness. Furthermore, the need for a dynamic random Advanced Encryption Standard arises from the desire to enhance the security of AES by incorporating randomization into the encryption process. Dynamic randomization of AES parameters such as key and initialization vector will provide an additional layer of protection against cryptographic attacks and increase the resilience of the cryptographic system. By integrating dynamism and randomization into AES, organizations can enhance the security posture of their systems and mitigate the risk of data breaches, intellectual property theft, and unauthorized access to sensitive information. The dynamism will be characterized by constant change while the randomization will provide a random number to make decisions during the execution process of the algorithm.

7.0 References

[1] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," in The Oxford Handbook of Cyberpsychology, 2019, pp. 662–690. [Online]. Available: https://doi.org/10.1093/oxfordhb/9780198812746.013.35

[2] Aloraini and M. Hammoudeh, "A survey on data confidentiality and privacy in cloud computing," in ACM International Conference Proceeding Series, Part F1305, 2017. [Online]. Available: https://doi.org/10.1145/3102304.3102314

[3] R. Singh Deora, & Dhaval M. Chudasama, "Brief Study of Cybercrime on an Internet," Journal of Communication Engineering & Systems, vol. 11, no. 1, pp. 1–6, 2021. [Online]. Available: https://www.researchgate.net/publication/352121472

[4] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176–8186, 2021. [Online]. Available: https://doi.org/10.1016/j.egyr.2021.08.126

[5] M. D. Babakerkhell and H. Slimanzai, "Internet Crimes- it's Analysis and Prevention Approaches," Asian Journal of Research in Computer

Science, pp. 41–48, 2021. [Online]. Available: https://doi.org/10.9734/ajrcos/2021/v11i130255

[6] M. Shamiulla, "Role of artificial intelligence in cyber security," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, pp. 4628–4630, 2019. [Online]. Available: https://doi.org/10.35940/ijitee.A6115.119119

[7] S. A. Ahmad, "Computing: A Review," in 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019, pp. 1–6.

[8] M. M. Mohd Nadzri, A. Ahmad, and A. Amira, "Implementation of Advanced Encryption Standard (AES) for Wireless Image Transmission using LabVIEW," in 2018 IEEE 16th Student Conference on Research and Development, SCOReD 2018, 2018, pp. 1–4. [Online]. Available: https://doi.org/10.1109/SCORED.2018.8710984

[9] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp. 442–448, 2017. [Online]. Available: https://doi.org/10.14569/ijacsa.2017.080659

[10] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," International Journal of Communication Networks and Information Security, vol. 12, no. 2, pp. 256–272, 2020.

[11] N. Mathur, G. Mitwa, and P. Mathur, "Overview Study of Advanced Encryption Standard (Aes) in Cryptology," International Research Journal of Modernization in Engineering Technology and Science, vol. 2, no. 10, pp. 176–180, 2020.

[12] V. H. Soumya, M. B. Neelagar, and K. V. Kumaraswamy, "Designing of AES Algorithm using Verilog," in 2018 4th International Conference for Convergence in Technology, I2CT 2018, 2018, pp. 1–5. [Online]. Available: https://doi.org/10.1109/I2CT42659.2018.9058322

[13] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," International Journal of Artificial Intelligence Research, vol. 4, no. 1, pp. 49–57, 2020. [Online]. Available: https://doi.org/10.29099/ijair.v4i1.154

[14] T. Ullah, B. Ali, and N. U. Arfeen, "Cyber Secure Framework for Energy Management System," International Research Journal of Modernization in Engineering Technology and Science, vol. 08, pp. 2582–5208, 2021. [Online]. Available: www.irjmets.com

[15] O. Hajihassani, S. K. Monfared, S. H. Khasteh, and S. Gorgin, "Fast AES Implementation: A High-Throughput Bitsliced Approach," IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 10, pp. 2211–2222, 2019. [Online]. Available: https://doi.org/10.1109/TPDS.2019.2911278

[16] N. Su, Y. Zhang, and M. Li, "Research on data encryption standard based on AES algorithm in internet of things environment," in Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019, 2019, pp. 2071–2075. [Online]. Available: https://doi.org/10.1109/ITNEC.2019.8729488

[17] G. Sravya et al., "The Ideal Block Ciphers-Correlation of AES and PRESENT in Cryptography," in Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, 2020, pp. 1107–1113. [Online]. Available: https://doi.org/10.1109/ICISS49785.2020.9315883

[18] Z. Lu and H. Mohamed, "A Complex Encryption System Design Implemented by AES," Journal of Information Security, vol. 12, no. 02, pp. 177–187, 2021. [Online]. Available: https://doi.org/10.4236/jis.2021.122009

[19] Q. Alasad, J. Yuan, and J. Lin, "Resilient AES against side-Channel attack using all-Spin logic," in Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI, 2018, pp. 57–62. [Online]. Available: https://doi.org/10.1145/3194554.3194595

[20] S. Bader and A. M. Sagheer, "Modification on AES-GCM to Increment Ciphertext Randomness," International Journal of Mathematical Sciences and Computing, vol. 4, no. 4, pp. 34–40, 2018. [Online]. Available: https://doi.org/10.5815/ijmsc.2018.04.03

[21] F. J. D, "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach," pp. 647–652, 2017.

[22] T. N. Dang and H. M. Vo, "Advanced AES algorithm using dynamic key in the internet of things system," in 2019 IEEE 4th International Conference on Computer and Communication Systems, ICCCS 2019, 2019, pp. 682–686. [Online]. Available: https://doi.org/10.1109/CCOMS.2019.8821647

[23] E. M. De Los Reyes, A. M. Sison, and R. P. Medina, "Modified AES cipher round and key schedule," Indonesian Journal of Electrical Engineering and Informatics, vol. 7, no. 1, pp. 28–35, 2019. [Online]. Available: https://doi.org/10.11591/ijeei.v7i1.652

[24] Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "Key-dependent Advanced Encryption Standard," in 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering, ICCCEEE 2018, 2018, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICCCEEE.2018.8515761

[25] Y. S. Sikarwar and N. S. Murty, "Low Power Implementation of Advanced Encryption Standard using Efficient Shift Registers in 45 nm Technology," in Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, pp. 26–30. [Online]. Available: https://doi.org/10.1109/CESYS.2018.8723879

[26] G. G. Dath, A. Chalil, and J. Joseph, "An Efficient Fault Detection Scheme for Advanced Encryption Standard," in Proceedings of the 3rd International Conference on Communication and Electronics Systems, ICCES 2018, 2018, pp. 99–103. [Online]. Available: https://doi.org/10.1109/CESYS.2018.8723989

[27] Altigani et al., "A Polymorphic Advanced Encryption Standard - A Novel Approach," IEEE Access, vol. 9, pp. 20191–20207, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3051556

A. Barrera, C. W. Cheng, and S. Kumar, "A fast implementation of the rijndael substitution box for cryptographic AES," in Proceedings - 2020 3rd

International Conference on Data Intelligence and Security, ICDIS 2020, 2020, pp. 20–25. [Online]. Available: https://doi.org/10.1109/ICDIS50059.2020.00009

[28] Y. S. Chauhan and T. N. Sasamal, *"Enhancing Security of AES Using Key Dependent Dynamic Sbox,"* in Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019, 2019, pp. 468–473. [Online]. Available: https://doi.org/10.1109/ICCES45898.2019.9002543

[29] Q. Hu, X. Fan, and Q. Zhang, "An effective differential power attack method for advanced encryption standard," in *Proceedings - 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019, 2019, pp. 58–61. [Online]. Available: https://doi.org/10.1109/CyberC.2019.00019*

A. Olutola and M. Olumuyiwa, "Comparative analysis of encryption algorithms," *Eur. J. Technol.,* vol. 7, no. 1, pp. 1-9, 2023.

[30] Top of Form

[31] P. Pujiono, E. H. Rachmawanto, and D. A. Nugroho, "The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images," Journal of Applied Intelligent System, vol. 8, no. 1, pp. 69–80, 2023. [Online]. Available: https://doi.org/10.33633/jais.v8i1.7324

[32] W. Ady Putra, S. Suyanto, and M. Zarlis, "Performance Analysis of The Combination of Advanced Encryption Standard Cryptography Algorithms with Luc for Text Security," *SinkrOn,* vol. 8, no. 2, pp. 890–897, 2023. [Online]. Available: https://doi.org/10.33395/sinkron.v8i2.12202

[33] M. Shahmanesh et al., "Towards a Coefficient Secure IoT Energy Framework within the Smart City: Advanced Encryption Standard," 2023.

[34] Z. Lu, "Analysis on AES encryption standard and safety," 128, February 2023. [Online]. Available: https://doi.org/10.1117/12.2662564

[35] S. Sanap and V. More, "An Ultra-High Throughput and Efficient Implementation of Advanced Encryption Standard," International Journal of Electrical and Electronic Engineering and Telecommunications, vol. 12, no. 1, pp. 46–52, 2023. [Online]. Available: https://doi.org/10.18178/ijeetc.12.1.46-52

[36] T. Solomon, Y. M. Malgwi, M. D. Eli, and C. Sermeje, "Afropolitan Journals A Triple Paase Hybrid Security Model for Cloud Storage Using Advanced Encryption Standard," vol. 11, no. 1, pp. 53–67, 2023.

[37] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Advanced approach for encryption using advanced encryption standard with chaotic map," *International Journal of Electrical and Computer Engineering,* vol. 13, no. 2, pp. 1708–1723, 2023. [Online]. Available: *https://doi.org/10.11591/ijece.v13i2.pp1708-1723*

[38] K. Assa-agyei, "Optimizing the Performance of the Advanced Encryption Standard Techniques for Secured Data Transmission," 185(21), pp. 31–36, 2023.

[39] R. Somaiya, "Design and implementation of MAES (modified Advanced Encryption Standard) algorithm in ANDROID for multimedia applications," pp. 1–13, 2023.

[40] S. K. John, "Advanced Encryption Standard Modified for Cryptographic Applications," *International Research*

Journal of Modernization in Engineering Technology and Science, vol. 05, no. 08, August-2023.

[41] R. Somaiya, A. Gonsai, and R. Tanna, "Implementation and evaluation of EMAES–A hybrid encryption algorithm for sharing multimedia files with more security and speed," *Int. J. Electr. Comput. Eng. Syst.,* vol. 14, no. 4, pp. 401-409, 2023.

[42] N. Mudegol, "Hybrid encryption using symmetric block and stream cipher," *Int. J. Eng. Manage. Res., vol*. 13, no. 1, pp. 35-39, 2023.

[43] N. Yang, "Establishing a mathematical model for encryption and decryption of communication network data," *Int. J. Mechatronics Appl. Mech., no. 13, pp. 70-75, 2023*