iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69587

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Advanced Encryption Standard (AES): A Comprehensive Analysis and Application

Onkar Kailas Mane[1], Mr. Himanshu Tarale[2], Miss. Sharayu Konde[3]
[1, 2]*Research Scholar, Dr.Vishwanath Karad MIT World Peace University INDIA*
[3]*Research Scholar, Modern college of Engineering, Pune, INDIA*

Abstract-In this paper we have discussed aboutAES, the Advanced Encryption Standard, is a pivotal cryptographic algorithm making sure data confidentiality in cutting-edge computing. This paper elucidates AES's technical intricacies, evaluates its security robustness towards numerous assaults, and delineates its vast programs throughout diverse domain names. Through comprehensive analysis and exam, this research objectives to underscore AES's importance in safeguarding sensitive facts, facilitating secure communique, and fortifying information protection frameworks in present day digital landscape.
Keywords: AES, Encryption, Decryption

I. INTRODUCTION

A. Brief History and Development of AES

The Advanced Encryption Standard (AES) emerged from a competitive selection procedure initiated by means of the National Institute of Standards and Technology (NIST) to replace the growing older Data Encryption Standard (DES). After an exhaustive evaluation of candidate algorithms, Rijndael, proposed through Daemen and Rijmen, changed into selected because the AES widespread in 2001 [1]. This rigorous selection process ensured that AES turned into both secure and efficient, paving the manner for its full-size adoption as an international encryption popular.

B. Importance and Relevance of Encryption in Modern Computing

Encryption serves as a cornerstone of present-day computing, making sure the confidentiality, integrity, and authenticity of virtual statistics. With the proliferation of digital transactions, communications, and information garage, the want for robust encryption mechanisms has in no way been greater important. Encryption algorithms like AES play a pivotal role in safeguarding sensitive information from unauthorized get right of entry to, interception, and tampering. They shape the backbone of steady verbal exchange protocols, information storage structures, and cryptographic frameworks throughout numerous industries, together with finance, healthcare, and e-trade.

C. Overview of Symmetric Encryption and the Role of AES

Symmetric encryption, characterized via the usage of an unmarried shared key for both encryption and decryption, is an essential cryptographic approach hired in securing digital communications and records. AES, a symmetric encryption set of rules, operates on fixed-length blocks of information, and employs a chain of substitution-permutation operations to convert plaintext into ciphertext and vice versa. Renowned for its performance, security, and flexibility, AES has end up the gold preferred for symmetric encryption and is widely hired in various applications, ranging from secure conversation protocols to disk encryption mechanisms.

II. FUNDAMENTALS OF AES ENCRYPTION

A. Core Principles of AES Algorithm

The AES set of rules operates on constant-length blocks of facts, generally 128 bits, and consists of numerous middle concepts to make certain its protection and performance. These principles consist of substitution, permutation, and key blending operations achieved over more than one rounds. SubBytes and ShiftRows operations introduce non-linearity and diffusion, even as MixColumns and AddRoundKey operations in addition obfuscate the records and comprise the key into the encryption system [2].

B. Block Cipher Operation Modes

Block cipher operation modes dictate how a block cipher, which includes AES, encrypts plaintext data large than its block size.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Common modes encompass Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), and Galois/Counter Mode (GCM). Each mode gives distinct benefits and is desirable to exceptional use instances. For instance, CBC mode introduces a chaining mechanism to mitigate patterns inside the ciphertext, whilst CTR mode permits parallel encryption and decryption [4].

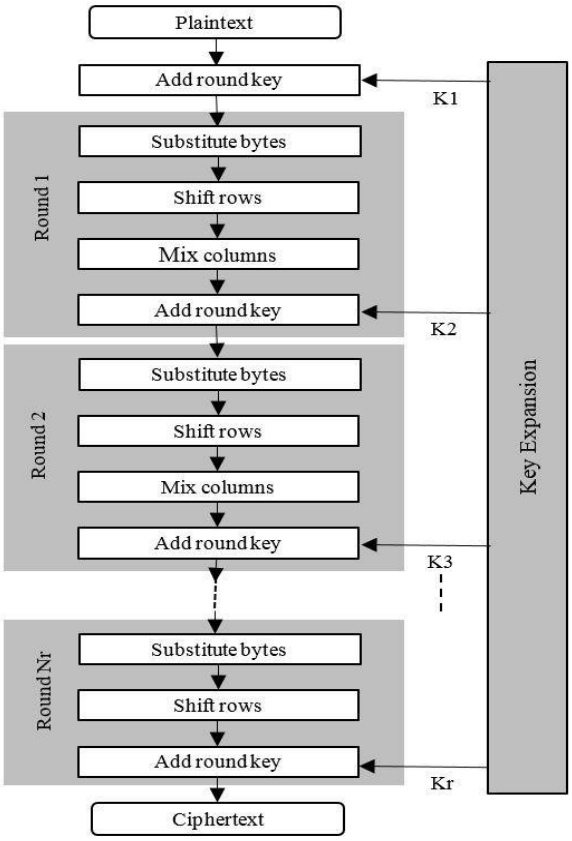


Figure 1. AES Algorithm Structure

III. TECHNICAL DETAILS OF AES ALGORITHM

A. Structure of AES Algorithm

The AES set of rules operates through a sequence of rounds, each which includes several transformation stages applied to the input statistics. These transformation degrees encompass SubBytes, ShiftRows, MixColumns, and AddRoundKey. SubBytes entails substituting every byte of the enter with a corresponding byte from a fixed S-box. ShiftRows shifts the rows of the kingdom array cyclically to the left. MixColumns mixes the columns of the kingdom array, while AddRoundKey XORs the country with the spherical key [2].

B. Key Sizes and Key Expansion Process

AES helps 3 key sizes: 128, 192, and 256 bits, corresponding to 10, 12, and 14 rounds, respectively. The key expansion process generates round keys from the given initial encryption key. It involves repeatedly applying a key timetable algorithm to transform the initial key into a chain of spherical keys. Each spherical key is derived from the previous round key through a mixture of byte substitution, rotation, and XOR operations [3].

C. Security Properties and Strength of AES

AES famous several safety houses that make contributions to its electricity as an encryption algorithm. These residences consist of confusion, diffusion, resistance to differential and linear cryptanalysis, and avalanche impact. Confusion guarantees that a small change in the enter key or plaintext consequences in a great trade in the ciphertext. Diffusion guarantees that modifications in one part of the plaintext affect a couple of parts of the ciphertext. AES's resistance to differential and linear cryptanalysis ensures that it is rather secure towards those forms of assaults [4].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

IV. AES ENCRYPTION PROCESS

A. Key Expansion:

AES uses a key schedule to expand the original key into a set of round keys. The key expansion process varies depending on the key size (128-bit, 192-bit, or 256-bit) and involves various operations such as key mixing, rotation, and substitution. Each round key is derived from the previous one, ensuring that each round has a unique key.

The initial key is expanded to generate a set of round keys. Each round key is 128 bits long. The key expansion process produces a total of 11 round keys for AES-128.

B. Initial Round Key Addition:

In this step, each byte of the plaintext block is XORed with a corresponding byte from the round key. This step introduces randomness into the encryption process by combining the plaintext with the encryption key.

Example:

PlaintextBlock: 0x3243f6a8885a308d313198a2e0370734

Round 0 Key: 0x2b7e151628aed2a6abf7158809cf4f3c

Each byte of the plaintext block is XORed with the corresponding byte from the round key.

C. SubBytes:

In the SubBytes step, each byte of the state array is replaced with a corresponding byte from the S-box, a fixed substitution table. This step introduces confusion by substituting bytes with non-linear transformations.

To perform the SubBytes step, you need to:

Prepare the S-box: The S-box is a 16x16 matrix containing substitution values for each byte. It is predefined and remains constant throughout the encryption process.

Substitute each byte of the state array with the corresponding byte from the S-box: For each byte in the state array, locate its row and column in the S-box and replace it with the byte value found at that position.

Here's a simplified explanation of how to perform the SubBytes step with an example:

Example:

Consider the following state array before SubBytes:

Perform SubBytes:

88	32	8D	E0
5A	39	E1	37
F6	34	98	6C
A8	47	23	43

For each byte in the state array, locate its row and column in the S-box and replace it with the byte value found at that position.

Byte 88: Row 8, Column 8. Substitute with S-box value 0x8D.

Byte 32: Row 3, Column 2. Substitute with S-box value 0x5B.

Byte 8D: Row 8, Column D. Substitute with S-box value 0xD4.

Byte E0: Row E, Column 0. Substitute with S-box value 0x45.

And so on for the remaining bytes in the state array.

After SubBytes State Array:

In this way, each byte in the state array is substituted with a corresponding byte from the S-box, completing the SubBytes step of the AES encryption process.

8D	5B	D4	45
5A	6E	5A	52
59	C3	B9	29
3A	60	E8	0C

D. ShiftRows:

In the ShiftRows step, the bytes in each row of the state array are cyclically shifted to the left. This step provides diffusion by spreading the influence of each byte throughout the state array.

Here's a simplified explanation of how to perform the ShiftRows step with an example:

Consider the previous state array before ShiftRows.

Perform ShiftRows:

For each row in the state array, perform the following shifting operations:

Row 1: No shift (remains unchanged).

Row 2: Shift one position to the left.

Row 3: Shift two positions to the left.

Row 4: Shift three positions to the left.

After ShiftRowsState Array:

8D	5B	D4	45
6E	5A	52	5A
B9	29	59	C3
0C	3A	60	E8

In this way, each row of the state array is cyclically shifted to the left, completing the ShiftRows step of the AES encryption process.

E. Mix Columns:

The MixColumns step operates on each column of the state array using a matrix multiplication operation. This step provides diffusion by mixing the bytes within each column.

To perform the MixColumns step, you need to:

1) Define a fixed matrix called the MixColumns matrix.

2) Multiply each column of the state array by the MixColumns matrix.

Example:

Consider the Previous state array before MixColumns and Perform MixColumns.

For each column in the state array, perform the following matrix multiplication operation:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

✖

8D
6E
B9
0C

=

04
66
81
E5

Each byte in a column is multiplied by the corresponding element in the MixColumns matrix, and the results are XORed together to obtain the new value for that byte in the column.

After MixColumnsState Array:

04	66	81	E5
27	49	36	A6
6E	98	59	6F
81	D2	77	15

In this way, each column of the state array is transformed using the MixColumns matrix, completing the MixColumns step of the AES encryption process.

F. Add Round Key

Each byte of the state array is XORed with a corresponding byte from the obtained round key. This operation adds additional randomness and security to the encryption process.

To perform the AddRoundKey step, you need to:

1) Retrieve the appropriate round key for the current round of encryption.

2) XOR each byte of the state array with the corresponding byte from the round key.

Example:

Consider the previous state array after the MixColumns step.

And consider the round key for the current round:

2B	7E	15	16
28	AE	D2	A6
AB	F7	15	88
09	CF	4F	3C

Perform AddRoundKey:

For each byte in the state array, XOR it with the corresponding byte from the round key.

State Array:

04^2B=2F| 66^7E=18 | 81^15=94 | E5^16=F3

27^28=0F| 49^AE=E7 | 36^D2=E4 |A6^A6=00

6E^AB=C5 | 98^F7=6F| 59^15=4C| 6F^88=E7

81^09=88 |D2^CF=1D| 77^4F=38 | 15^3C=29

After AddRoundKeyState Array:

2F	18	94	F3
0F	E7	E4	00
C5	6F	4C	E7
88	1D	38	29

In this way, each byte of the state array is XORed with the corresponding byte from the round key, completing the AddRoundKey step of the AES encryption process.

G. Final Round:

The final round excludes the MixColumns step.

After the final round, the state array represents the encrypted ciphertext.

V. AES DECRYPTION PROCESS

The AES decryption process is the reverse of the encryption process and involves similar steps but in reverse order. The steps involved in AES decryption are as follows:

1) *Key Expansion:* Generate round keys from the original decryption key using the key expansion algorithm.

2) *Initial Round Key Addition:* Add the final round key to the ciphertext.

3) *Inverse ShiftRows:* Perform the inverse of the ShiftRows operation by shifting the bytes in each row of the state array to the right.

4) *Inverse SubBytes:* Perform the inverse of the SubBytes operation by substituting each byte of the state array with a corresponding byte from the inverse S-box.

5) *Rounds of Inverse MixColumns and AddRoundKey:* Repeat a series of rounds that involve the following operations:

- *Inverse MixColumns:* Transform each column of the state array using a matrix multiplication operation with the inverse MixColumns matrix.
- *AddRoundKey:* XOR each byte of the state array with a corresponding byte from the respective round key.

6) *Final Round:* Perform a final round that involves the following operations:

- Inverse ShiftRows
- Inverse SubBytes
- *Final Round Key Addition:* Add the initial round key to the state array.

7) Output: The resulting state array after the final round represents the decrypted plaintext.

It's important to note that the inverse operations of SubBytes, ShiftRows, and MixColumns are used in decryption to reverse the effects of their respective encryption operations. Additionally, the round keys used in decryption are derived from the original encryption key but in reverse order.

These steps collectively reverse the encryption process and yield the original plaintext from the ciphertext.

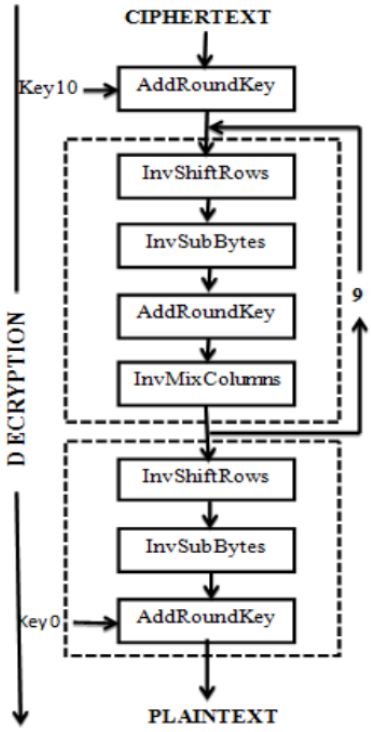


Figure 2. AES Decryption Process

VI. SECURITY ANALYSIS OF AES

A. Evaluation of AES Security Against Various Attacks

AES has passed through giant scrutiny and evaluation to assess its safety against diverse cryptographic assaults. Researchers have analyzed AES's resistance to differential and linear cryptanalysis, in addition to its susceptibility to related-key attacks, algebraic attacks, and facet-channel assaults. Numerous research has verified AES's resilience in opposition to known attacks, highlighting its robustness and suitability for steady information encryption in sensible applications [2]. However, ongoing research maintains to discover ability vulnerabilities and refine cryptographic techniques for stronger security.

B. AES as a Standardized and Widely Accepted Encryption Algorithm.

AES has carried out substantial adoption as a standardized encryption algorithm across numerous industries and programs. Its selection because the Advanced Encryption Standard through NIST in 2001 cemented its repute as a trusted and widely regularly occurring cryptographic set of rules. AES is integrated into numerous cryptographic libraries, protection protocols, and hardware implementations, underscoring its importance in safeguarding sensitive statistics in modern computing environments. Its standardized nature promotes interoperability and guarantees compatibility throughout unique systems, further solidifying its function as a cornerstone of current cryptography [1].

VII. APPLICATIONS OF AES

A. Real-World Applications of AES

AES encryption reveals giant use in diverse real-global programs across exclusive sectors. Some outstanding programs encompass:

1) Secure Communication Protocols: AES is applied in secure communique protocols which include TLS/SSL, SSH, and IPsec to encrypt information exchanged among customers and servers, making sure confidentiality and integrity [5].

2) *Data Storage Encryption:* AES is employed in disk encryption software program like BitLocker and FileVault to encrypt saved facts on hard drives and different garage gadgets, defensive it from unauthorized get entry to [6].
3) *Mobile Device Security:* AES is incorporated into cell operating structures like iOS and Android to encrypt person statistics, making sure the security of private facts saved on smartphones and tablets [7].
4) *Cloud Computing:* AES encryption is used to secure statistics saved in cloud computing environments, safeguarding touchy records from unauthorized get admission to or information breaches [8].
5) *Digital Rights Management (DRM):* AES is utilized in DRM structures to defend digital content which includes movies, music, and e-books from piracy by way of encrypting the content during transmission and garage [9].

B. Comparison with Other Encryption Algorithms

AES is as compared with other encryption algorithms based totally on different factors consisting of protection, performance, and applicability. While AES is extensively seemed as an enormously secure and efficient encryption algorithm, it's miles as compared with different algorithms along with DES, Triple DES, RSA, and Blowfish.

1) *Security:* AES is understood for its sturdy protection residences and resistance towards known cryptographic assaults, making it a favored desire for many applications in comparison to older algorithms like DES and Triple DES [3].
2) *Efficiency:* AES is designed for efficient implementation in both software program and hardware, offering excessive performance and occasional computational overhead as compared to some other encryption algorithms [4].
3) *Applicability:* AES is broadly supported and standardized, making it appropriate for a large range of programs across distinct platforms and environments. It outperforms a few other algorithms in terms of interoperability and compatibility [1].

VIII. CHALLENGES AND FUTURE DEVELOPMENTS

A. Limitations and Challenges Faced via AES

Despite its giant adoption and demonstrated protection, AES faces certain limitations and demanding situations:

1) *Quantum Computing Threats:* The upward push of quantum computing poses a potential danger to AES's security, as quantum computers may also render traditional encryption algorithms prone to attacks. AES-256, with its larger key length, gives multiplied resistance to quantum attacks as compared to AES-128 and AES-192 [10].
2) *Side-Channel Attacks:* AES implementations may be prone to aspect-channel attacks, in which an attacker exploits records leaked through the physical implementation of the algorithm, inclusive of timing, energy consumption, or electromagnetic radiation [11].
3) *Key Management:* AES's safety closely is based on the electricity of its encryption keys. Effective key management practices, which include key technology, distribution, and garage, are vital to keeping the safety of AES-encrypted facts [12].

B. Ongoing Research and Future Directions in AES Security

Researchers retain to explore avenues to enhance AES's safety and deal with emerging threats:

1) *Post-Quantum Cryptography:* Research in post-quantum cryptography aims to develop encryption algorithms resilient to attacks from quantum computers. Post-quantum options to AES, such as lattice-primarily based cryptography or multivariate polynomial cryptography, are below investigation [13].
2) *Lightweight Cryptography:* With the proliferation of IoT devices and useful resource-restricted environments, there's a developing call for for light-weight encryption algorithms appropriate for restricted systems. Research in lightweight cryptography focuses on growing green and stable encryption algorithms tailor-made to low-power devices [14].
3) *Homomorphic Encryption:* Homomorphic encryption permits computations to be carried out on encrypted records without decrypting it first. Future developments in homomorphic encryption may offer new opportunities for stable statistics processing and privacy-maintaining computation at the same time as the usage of AES as the underlying encryption scheme [15].

IX. CONCLUSION

A. Summary of Key Points Discussed

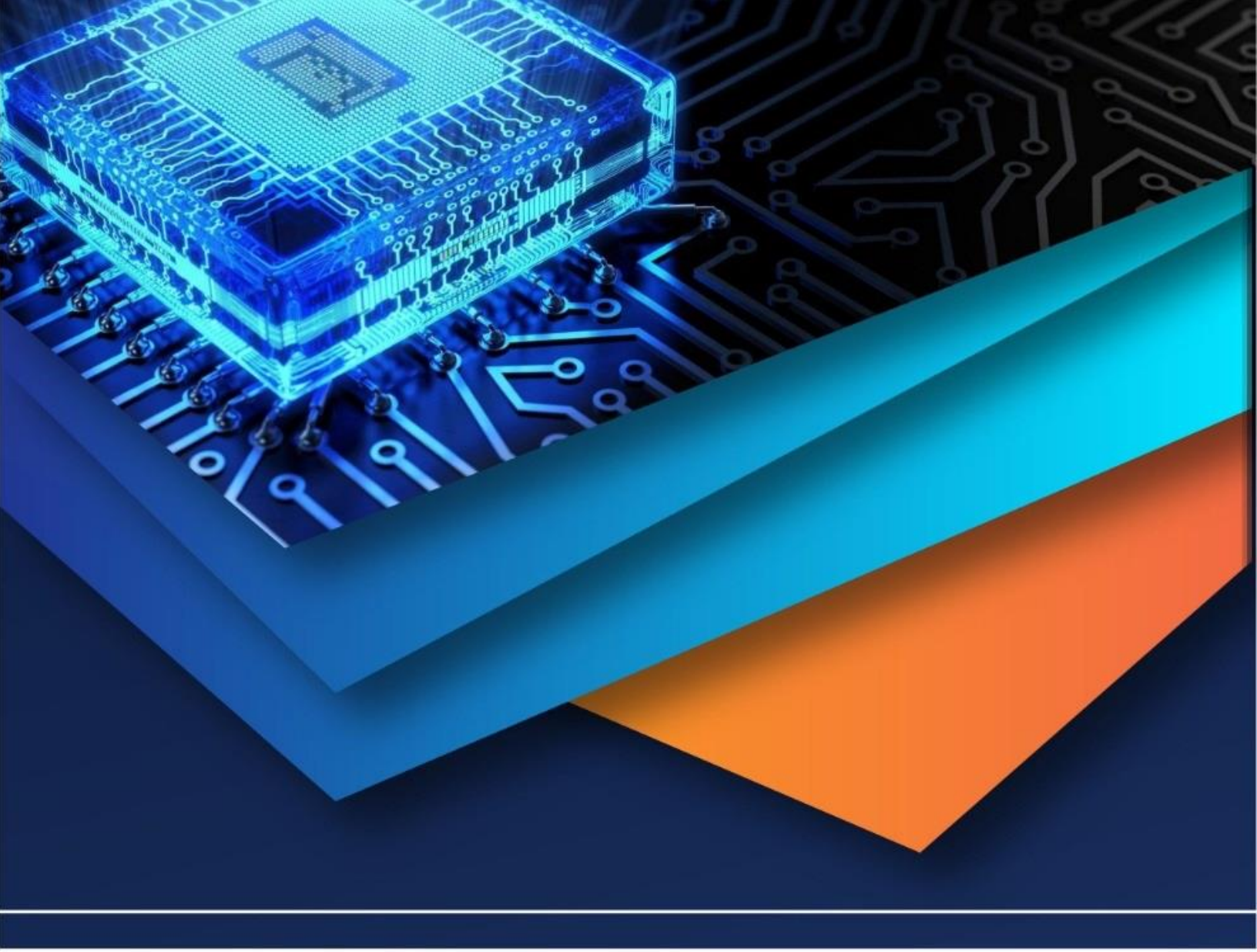
Throughout this paper, we've delved into numerous aspects of AES encryption, including its historical improvement, technical info, actual-global packages, protection evaluation, and destiny demanding situations. We explored the core standards of AES, its block cipher operation modes, and the significance of key sizes and key expansion procedures. Additionally, we discussed the significance of AES in making sure facts confidentiality and integrity throughout diverse domains.

B. Importance of AES in Data Confidentiality and Integrity

AES encryption performs an important role in safeguarding sensitive records and ensuring the confidentiality and integrity of facts in modern computing environments. Its adoption in steady verbal exchange protocols, records storage encryption, cell device security, and cloud computing display its importance in defensive valuable property from unauthorized get entry to and cyber threats.

REFERENCES

[1] National Institute of Standards and Technology (NIST), "FIPS PUB 197: Advanced Encryption Standard (AES)," November 2001.
[2] . Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," Springer, 2002.
[3] W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson, 2016.
[4] N. Ferguson, B. Schneier, and T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications," Wiley, 2010.
[5] D. Ristic, "Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications," Feisty Duck, 2017.
[6] A. Leonhardi, "Pro FileVault 2: Unlocking the Potential of Full Disk Encryption," Apress, 2012.
[7] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," ACM Transactions on Computer Systems (TOCS), vol. 32, no. 2, pp. 5:1–5:29, 2014.
[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 201
[9] M. H. R. K. Pillai, "Digital Rights Management: Technologies, Issues, Challenges and Systems," Springer Science & Business Media, 2008.
[10] M. Mosca, "Quantum attacks on classical cryptographic algorithms," in Post-Quantum Cryptography, Springer, 2009.
[11] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology—CRYPTO '99, Springer, 1999.
[12] C. Adams and S. Lloyd, "Understanding PKI: Concepts, Standards, and Deployment Considerations," 2nd ed., Addison-Wesley, 2003.
[13] D. J. Bernstein, "Introduction to post-quantum cryptography," Post-Quantum Cryptography, Springer, 2009.
[14] T. Güneysu and M. Paar, "Efficient hardware implementations of lightweight cryptography," in International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2007.
[15] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proceedings of the 41st annual ACM symposium on Theory of computing, 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY