IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 8, Issue 2, April 2020

Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing

Poovendran Alagarsundaram,

ABSTRACT

The Advanced Encryption Standard (AES) method must be implemented in cloud computing to improve data security against the growing threat of cyberattacks and the rapid growth of sensitive data processing and storage on distant servers. Strong secrecy and integrity are maintained while encrypting and decrypting fixed-length data blocks using the symmetric encryption technique AES. After a public competition held in the late 1990s by the US National Institute of Standards and Technology (NIST), AES became the de facto encryption standard in 2001, taking the place of the antiquated Data Encryption Standard (DES). Its efficacy in data protection explains its broad popularity across industries and cloud computing environments. With an emphasis on key expansion, algorithm phases, and practical considerations for cloud deployment, this paper outlines the implementation techniques for AES. Even though AES offers significant security advantages, problems with compatibility, performance overhead, and key management still exist. As a result, ongoing research and development are required to address these issues and improve AES encryption solutions for cloud computing. By shielding sensitive data from cyberattacks and unwanted access, organizations using AES principles can improve their data security posture, adhere to legal requirements, and foster trust among cloud users.

Keywords: AES algorithm, Cloud computing, Cyber threats, Symmetric encryption, Cryptographic transformations, Confidentiality, Integrity, Regulatory standards, Cryptanalysis, Encryption solutions.

1. INTRODUCTION

Strong security measures are essential to protect sensitive data from cyber-attacks and unauthorized access in the age of cloud computing, where enormous volumes of data are processed and stored across remote servers. The use of the Advanced Encryption Standard (AES) algorithm is one such crucial security precaution. One of the mainstays of contemporary cryptography is AES, which provides an advanced but effective way to encrypt data.

Project Lead, IBM, Sacramento,
North Carolina, United States
Email: poovasg@gmail.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 8, Issue 2, April 2020

Organizations can strengthen their data security posture and reduce the risks of data breaches and cyberattacks by implementing AES encryption into cloud computing environments. This improves confidentiality and integrity of data.Symmetric encryption known for its security and effectiveness is the Advanced Encryption Standard (AES) algorithm. It uses several cryptographic transformations to safely encrypt and decrypt data, working with fixed-length data blocks. Key Expansion, the First Round, Rounds, and the Final Round are the main parts of the AES algorithm. The cipher key is subjected to Key Expansion during the encryption process, producing round keys that are utilized in further cryptographic procedures. In the first round, bitwise XOR is used to combine each byte of the data with the round key. Non-linear substitution (Sub Bytes), transposition (Shift Rows), mixing (Mix Columns), and extra XOR operations (Add Round Key) are all included in subsequent rounds. The Final Round's structure is the same as that of the earlier rounds, except the Mix Columns procedure. AES provides strong encryption of data through this series of cryptographic procedures, making it extremely resistant to efforts at decryption and unauthorized access.

A public competition was held by the U.S. National Institute of Standards and Technology (NIST) in the late 1990s to choose a new encryption standard to replace the outdated Data Encryption Standard (DES). This competition marked the beginning of the creation of the Advanced Encryption Standard (AES). The AES standard was established in 2001 when the Rijndael algorithm, created by Belgian cryptographers Vincent Rijmen and Joan Daemen, emerged as the winner of the competition following a thorough examination and analysis. As the de facto encryption method for protecting sensitive data in a variety of applications, including cloud computing, AES has been widely adopted across industries since it was standardized.

A plethora of cryptographic libraries and programming languages can be used to implement the AES encryption algorithm. Libraries for AES encryption and decryption can be found in third-party or built-in packages for popular programming languages including Python, Java, and C/C++. Furthermore, extensive support for AES encryption in a variety of settings and platforms is offered by specialist cryptographic libraries like Bouncy Castle and OpenSSL. To improve data security, cloud service providers might also include built-in encryption features or incorporate external encryption programs into their framework.

The Rijndael cipher was put forth by Belgian cryptographers Vincent Rijmen and Joan Daemen as a contender for the Advanced Encryption Standard (AES) competition,

ISSN 2347–3657
Volume 8, Issue 2, April 2020

which was started by the National Institute of Standards and Technology (NIST) in the United States. This led to the development of the AES encryption algorithm. AES has been widely implemented and adopted by the global cryptographic community since it was chosen as the standard in 2001. Researchers, developers, and industry stakeholders have all contributed to this acceptance.

The major goal of using the AES encryption algorithm in cloud computing environments is to improve data security by providing strong encryption techniques to safeguard sensitive information from unwanted access and cyber threats. Organizations want to protect the confidentiality, integrity, and authenticity of data stored and sent within cloud infrastructures by incorporating AES encryption into cloud-based applications and services. Furthermore, deploying AES encryption corresponds with regulatory compliance standards and industry best practices for data safety, which fosters trust and confidence among cloud users.

There are some obstacles and factors to take into account while implementing AES encryption, even though it provides a high level of security for data in cloud computing environments. Among these could be compatibility with current systems and protocols, performance overhead, and key management. In addition, it is crucial to continuously assess and update encryption procedures to preserve security efficacy due to the dynamic nature of threats and developments in cryptanalysis procedures. Further developments in data security can result from research initiatives aimed at resolving these issues and improving the effectiveness and usability of AES encryption in cloud computing circumstances.

There are still worries about the security of sensitive data handled and stored in cloud environments, even though cloud computing has become very popular. The confidentiality and integrity of data are seriously threatened by unauthorized access, data breaches, and cyberattacks. Although encryption is a vital tool for protecting data, its proper use in cloud computing necessitates giving careful thought to some variables, such as algorithm choice, key management, and performance effects. A reliable and effective method for improving data security is offered by the AES encryption algorithm, which is being implemented in cloud computing to try and overcome these difficulties. For AES encryption methods to be optimized and new security risks in cloud computing settings to be reduced, further research and innovation are nonetheless required.

2. LITERATURE SURVEY:

The benefits of the Advanced Encryption Standard (AES) are outlined by Abdullah (2017), who also points out that AES is widely used in industries like government communications, e-commerce, and banking. AES offers different levels of security and works with fixed-size data blocks that have key lengths of 128, 192, or 256 bits. NIST recognizes it as an international standard and it is built to withstand cryptographic attacks. The algorithm's reliability and ongoing security improvements are attributed to its effectiveness, adaptability, and transparency.

ISSN 2347–3657
Volume 8, Issue 2, April 2020

A study comparing the security of data using the encryption methods AES, DES, and RSA was carried out by Mahajan and Sachdeva (2013). They discovered that AES performs exceptionally well in terms of speed and security, accommodating varying key lengths to meet various security needs. However, because to its tiny key size and vulnerability to brute force assaults, DES is seen as less secure and has lost value in favor of AES. While RSA is slower than symmetric encryption methods like AES, it provides strong asymmetric encryption that is appropriate for digital signatures and key exchange. Among the three, AES is thought to be the most effective and safest, whereas RSA is mostly utilized for specialized encryption applications and DES is considered to be mostly outmoded.

AES (Advanced Encryption Standard) outperformed DES (Data Encryption Standard) in terms of speed and security, according to Rihan et al. (2015) performance analysis. Compared to DES, which has a fixed key size of 56 bits and an antiquated design, AES has an optimized design, supports greater key sizes, and is resistant to brute force attacks. These factors account for AES's supremacy. AES has become the industry standard for protecting sensitive data in a variety of applications because it performs better than DES in terms of efficiency, provides better security with variable key lengths, and integrates more sophisticated cryptographic approaches. Due to its security flaws, DES is typically discouraged for new deployments, despite the fact that it is still utilized in some older systems.

Lu and Tseng (2002) suggest a simplified system/module that combines functionalities into an integrated AES encrypter and decrypter. This method incorporates data handling, cryptographic operations, key management, security features, and compatibility assurance. It also increases efficiency. Scalability and flexibility across several deployment scenarios are supported by the design, which is validated against known vulnerabilities and subjected to stringent compliance testing.

In order to improve data security, Kumar and Rana (2016) suggest creating a modified version of the AES (Advanced Encryption Standard) algorithm that is compatible with the original AES standard but makes adjustments to key scheduling, substitution-permutation networks (SPNs), and other elements. Enhancement of resistance against cryptographic assaults, customization to particular application requirements, performance optimization, and key management are the goals of modifications. Comprehensive cryptanalysis, conformity to standards, public review, documentation, and ongoing improvement based on developments and input are all part of this iterative process.

AES encryption, which encrypts data before uploading and decrypts it upon retrieval to ensure secrecy and integrity, is the method of safe cloud storage described by Babitha and Babu (2016). Encryption key production, storage, and sharing must all be done securely as part of key management. This method makes use of data partitioning for fine-grained access control, access control methods, backup/disaster recovery plans, and

ISSN 2347–3657
Volume 8, Issue 2, April 2020

HTTPS or TLS for secure transfer. Ongoing surveillance guarantees the security of data that is stored.

AES encryption, which encrypts data before remote storage and ensures confidentiality and integrity, is a key component of data security in cloud storage, according to Mendonca (2018). Encryption keys must be generated, stored, and shared securely. This requires key management. In addition, access control, secure transmission, backup, recovery, and ongoing monitoring are all facilitated by AES encryption. Its scalability upholds security standards while satisfying the requirements of cloud storage settings.

Islam et al. (2008) support the use of longer key lengths and more sophisticated cryptographic approaches to provide improved security in symmetric data encryption using the AES (Advanced Encryption Standard) methodology. Higher levels of data confidentiality are ensured by extending the length of the AES key to 192 or 256 bits, which greatly increases resistance against different cryptographic assaults including brute force attacks. Performance may be marginally impacted by greater key lengths, but these impacts are mitigated by contemporary enhancements. Longer key length AES has become the industry standard, used in government, healthcare, and finance to ensure regulatory compliance and compatibility. Ongoing assessment guarantees efficacy against changing risks, supporting overall security posture and user trust.

By integrating the AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography) algorithms, Hodowu et al. (2020) suggest improving data security in cloud computing via a two-level cryptographic technique. While ECC enables safe key exchange and authentication for data in transit, AES effectively encrypts data at rest, guaranteeing confidentiality and integrity. This method offers complete security, scalability, and adherence to legal requirements. While ECC provides resistance against multiple assaults and increases security in key management and authentication, AES guarantees effective symmetric encryption for data storage. In cloud computing settings, a strong security posture against new threats is maintained by ongoing reviews and upgrades.

AES, RSA, ECC, and other cryptographic algorithms are compared and evaluated for security, performance, scalability, and applicability for cloud systems in Semwal and Sharma's (2017) study. AES is the best symmetric encryption algorithm for data that is not in use, whereas RSA and ECC are the most secure and effective options for asymmetric encryption and key management. Key management, scalability, and performance impacts are taken into account. Strong encryption for cloud storage is provided by Blowfish and Twofish, and data integrity is guaranteed by SHA-3. To provide flexibility to changing threats and requirements, cloud computing cryptography algorithms must take into account performance, scalability, regulatory compliance, and continual review.

Arora et al. (2013) support the use of encryption methods like AES and RSA to secure user data in cloud computing,

ISSN 2347–3657
Volume 8, Issue 2, April 2020

guaranteeing its confidentiality and integrity. Strong algorithms are used to encrypt data before it is stored or sent, protecting it against manipulation or unwanted access. While RSA is used for safe asymmetric encryption during data transmission, AES is used for effective symmetric encryption of data at rest. Ensuring safe key generation, storage, and distribution requires the implementation of strong key management protocols. Interception is prevented via secure communication protocols like HTTPS or TLS, and unwanted data access is limited by access control measures. Consistent audits and surveillance identify and address security risks, guaranteeing adherence to industry norms and data protection laws.

Shimbre and Deshpande (2015) suggest integrating the AES (Advanced Encryption Standard) algorithm with Third-Party Auditing (TPA) to improve distributed data storage security for cloud computing. While AES provides encryption for data confidentiality, bolstering security against unauthorized access and tampering in distributed cloud storage systems, TPA maintains data integrity through impartial audits. By ensuring transparency, scalability, regulatory compliance, constant monitoring, and resistance against assaults, this combined strategy strengthens user confidence in cloud storage services.

3. METHODOLOGY

Improving data security in cloud computing environments requires the implementation of the Advanced Encryption Standard (AES) algorithm as explained in table 1. AES, a symmetric encryption technique, is frequently used due to its reliability and effectiveness. This section details the implementation methods for AES, including an overview of its components, key expansion, algorithm phases, table explanations, architecture diagrams, and equations. In addition, practical issues for cloud deployment are highlighted to enable effective and secure encryption.

3.1. Overview of the AES algorithm.

The AES method uses a symmetric key to operate on fixed-length data blocks, which are typically 128 bits long. The encryption process consists of well-defined processes, such as key expansion, start and final rounds, and several transformation rounds. These processes ensure that the data is fully encrypted, making it extremely difficult to decrypt without the correct key.

Key Expansion: This phase creates a succession of round keys from the initial cipher key. It ensures that each encryption round utilizes a unique key, hence improving security.

In the *initial round*, each byte of data is merged with the initial round key via a bitwise XOR operation.

Rounds are the repetitive application of four major operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey.

Final Round: This stage, like the other rounds, includes SubBytes, ShiftRows, and AddRoundKey but skips the MixColumns phase.

These stages all contribute to the powerful encryption process that distinguishes AES,

ISSN 2347–3657
Volume 8, Issue 2, April 2020

making it the preferred choice for data security in cloud computing environments.

3.2. Key Expansion

Key Expansion is a fundamental step in the AES algorithm that converts the original cipher key into a succession of round keys. This procedure employs Rijndael's key scheduling, which ensures that each encryption round uses a distinct key, so increasing security.

The key expansion process consists of the following steps:

Key Schedule Core: This comprises rotating the key's bytes, applying the S-box to each byte, and XORing the result with a round constant.

Word Generation: The previous words are combined with the key schedule core to create new words.

Round Key Formation: The words are then combined to create round keys for each encryption round.

This systematic key expansion protects the encryption process's security and resistance to attacks.

Table 1: Components and Steps of the AES Algorithm.

Step	Description	Details
Key Expansion	Creates round keys using the cipher key	Uses the key schedule of Rijndael to generate a different key for every encryption cycle.
Initial Round	AddRoundKey	Employs bitwise XOR to combine each byte of the state with the round key.
Main Rounds	SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations are used in several rounds.	SubBytes: S-box-based non-linear replacement step. ShiftRows: Rearranges the state's rows cyclically. MixColumns: Employs a fixed polynomial to blend the bytes in every column. -AddRoundKey: Incorporates the round key and the state together.
Final Round	Similar to the main rounds, but no MixColumns.	SubBytes Shift Rows- AddRoundKey

S-box

- Goal: Offers non-linearity throughout the encryption procedure.
- In the SubBytes stage, a predetermined replacement table called the S-box is utilized. Every byte in the state matrix is swapped out with a matching byte from the table.
- Generation: Made resistant to both linear and differential cryptanalysis with the use of a mathematical transformation.

The S-box introduces non-linearity into the encryption process, which is essential for resisting certain types of cryptanalysis, and is carefully designed to be difficult to reverse-engineer, thereby enhancing security.

MixColumns Polynomial

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 8, Issue 2, April 2020

- Purpose: By combining bytes inside each column, it provides diffusion.
- The state matrix's columns are each transformed using a fixed polynomial in the MixColumns step.
- Polynomial:

$$2\ 3\ 1\ 1\ 1\ 2\ 3\ 1\ 1\ 1\ 2\ 3\ 3\ 1\ 1\ 2 \quad (1)$$

The influence of every byte in the ciphertext is distributed over some bytes thanks to this polynomial. The polynomial enables diffusion by distributing the influence of each byte across many bytes in the ciphertext, while its fixed structure allows for consistent and reliable translation of the state matrix columns.

1. Input: At the start of the AES encryption process, the plaintext message and the initial key are used.
2. Key Expansion Module: This module uses a special algorithm to create round keys from the initial cipher key.
3. Initial Round: The first round uses the AddRoundKey operation, which combines each byte of the state with a round key via bitwise XOR.
4. Main Rounds: Subsequent rounds, known as the main rounds, include a sequence of operations such as SubBytes (byte substitution), ShiftRows (row-wise shifting), MixColumns (column mixing), and AddRoundKey (XOR with round key).
5. Final Round: The final round of the AES algorithm contains SubBytes, ShiftRows, and AddRoundKey operations, but not the MixColumns phase.
6. Output: After the encryption procedure is completed, the ciphertext is generated, which represents the encrypted version of the original plaintext message.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 8, Issue 2, April 2020

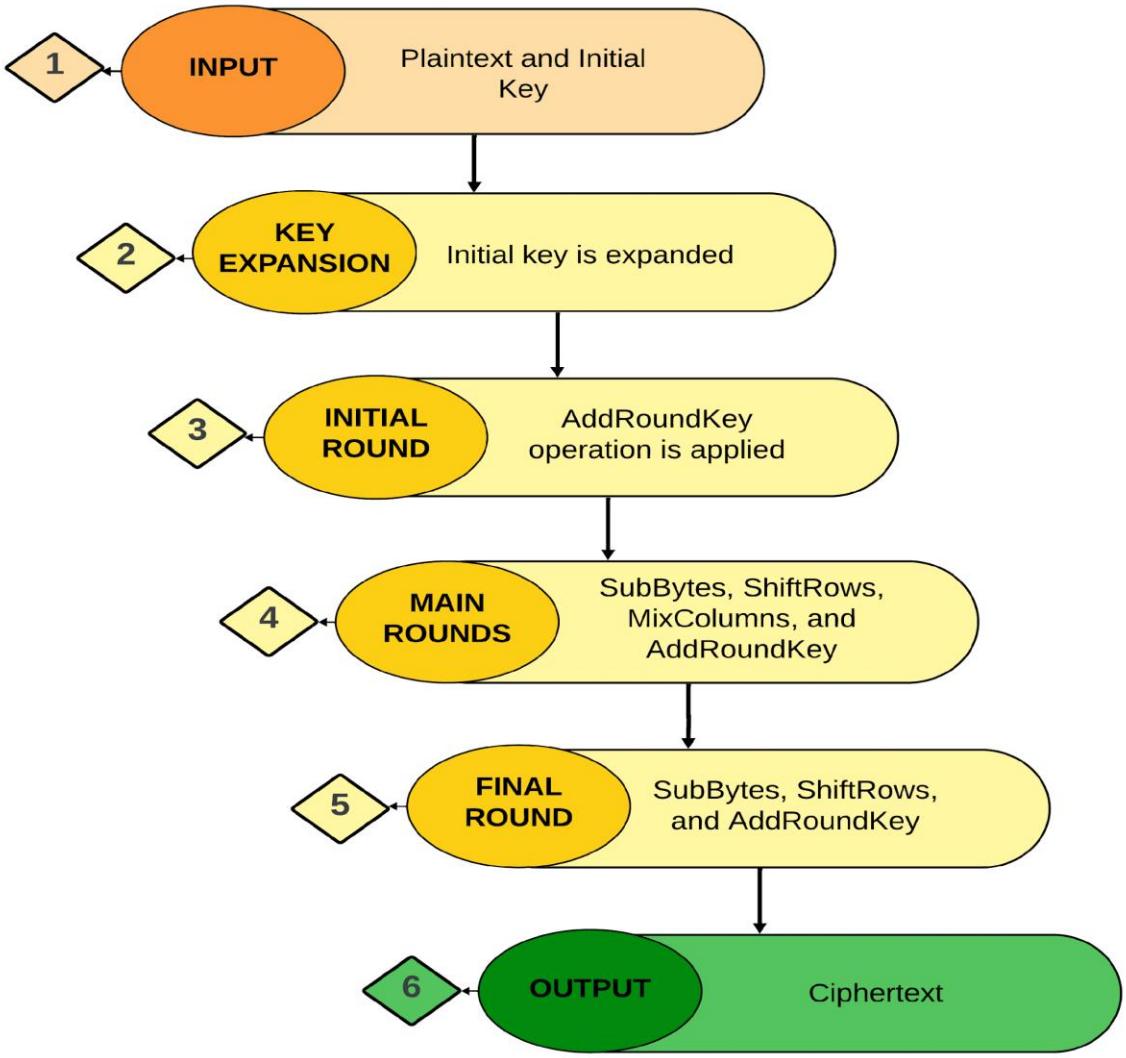

Figure 1: Visualizing the Encryption Process: AES Algorithm Overview

3.3. Algorithm Steps

Figure 1. explains the AES encryption process is divided into numerous parts, each of which contributes to the algorithm's overall security and efficiency.

SubBytes: This is a non-linear substitution phase in which each byte in the state matrix is replaced with a corresponding byte from a fixed lookup table called the S-box. This stage assures non-linearity in the encryption process, increasing its security.

ShiftRows: In this stage, the state matrix's rows are cyclically shifted. The degree of shift varies by row number, with the first row remaining intact, the second row shifted by one byte, and so on. This step promotes dissemination by transposing the bytes.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 8, Issue 2, April 2020

MixColumns alters each column of the state matrix with a fixed polynomial. This phase guarantees that the bytes are further combined, resulting in further diffusion.

A bitwise XOR operation is used to combine the state matrix with the round key generated during Key Expansion. This stage complicates the encryption process by merging the plaintext and round key.

These processes are carried out for a fixed number of rounds, which is specified by the key length. The final round bypasses the MixColumns step, which is necessary to complete the encryption.

3.4. Equations

Equations are the mathematical foundation of AES transformations, ensuring accurate and consistent actions throughout the encryption process.

SubBytes: In this transformation, each byte in the state matrix is replaced using the S-box.

$$S'(i,j) = S(S(i,j)) \quad (2)$$

Where S is the S-box lookup function.

ShiftRows: This transformation cycles across the rows of the state matrix.

$S'(i,j)=S(i,(j+shift(i))\mathrm{mod}Nb)$

Where shift(i) defines the cyclic shift for row i and Nb represents the number of columns in the state matrix.

MixColumns: This transformation uses a fixed polynomial to mix the bytes in each column.

$$S'(i,j) = \begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{matrix} \times \begin{matrix} S(0,j) \\ S(1,j) \\ S(2,j) \\ S(3,j) \end{matrix} \quad (3)$$

These equations ensure that each transformation step is mathematically valid, contributing to the AES algorithm's overall security and efficiency.

3.5. Implementation Steps

Implementing the AES algorithm in a cloud computing environment requires many critical steps:

Choose a Suitable Library: Choose from well-known cryptographic libraries such as Bouncy Castle and OpenSSL, or language-specific libraries like PyCrypto for Python and Java Cryptography Extension (JCE) for Java.

Initialize Parameters: Set the key size (128, 192, or 256 bits), plaintext, and initialization vectors as needed. Initialization vectors are very crucial for several types of AES operation, such as Cipher Block Chaining (CBC).

Key generation: Generate the initial cipher key using a secure random number generator. This ensures that the key remains surprising and secure.

Encrypt data:

Key Expansion: Take the initial cipher key and generate round keys.

Encryption Process: Transform the plaintext through the Initial Round, Multiple Rounds, and Final Round.

ISSN 2347–3657
Volume 8, Issue 2, April 2020

Ciphertext is the output of the encryption process.

Decrypt Data: To recover the original plaintext, repeat the previous steps using the same round keys. The decryption procedure employs the inverse operations of the encryption processes, such as InvSubBytes, InvShiftRows, and InvMixColumns.

3.6. Practical Considerations

When implementing AES in a cloud computing environment, numerous practical considerations must be made to ensure optimal speed and security:

Performance Overhead: The encryption and decryption operations add computational overhead, which might affect performance. It is critical to improve these operations to reduce latency and prevent them from becoming bottlenecks.

Key administration: The secure storage and administration of encryption keys is crucial. Consider employing hardware security modules (HSMs) or key management services (KMS) offered by cloud platforms. These tools provide secure key generation, storage, and administration, which reduces the danger of key compromise.

Integration with Cloud Services: Many cloud service providers have encryption options. Use these features or incorporate third-party encryption solutions to improve security without sacrificing performance. For example, Amazon Web Services (AWS) offers AWS Key Management Service (KMS) and AWS CloudHSM for key management and encryption.

Compliance and legislation: Ensure that the encryption solution adheres to applicable industry standards and legislation. Compliance with GDPR, HIPAA, or PCI-DSS may necessitate specific encryption processes and key management protocols.

Scalability: Consider the encryption solution's scalability. Cloud environments frequently contain massive amounts of data, and the encryption solution must be capable of handling this size without degrading performance.

Backup and recovery: Ensure that the encryption keys and encrypted data are securely stored. Implement robust recovery methods to avoid data loss in the event of a key compromise or hardware failure.

Monitoring and auditing: Set up mechanisms to track encryption key usage and detect unwanted access attempts. This aids in ensuring the security and integrity of the encrypted data.

Implementing the AES algorithm in cloud computing environments improves data security by offering strong encryption techniques. This technique covers the necessary processes and considerations for successful deployment, ensuring that sensitive data is safeguarded from unauthorized access and cyber threats. Understanding and utilizing AES principles allows enterprises to achieve a high level of data confidentiality and integrity in their cloud computing infrastructures.

4. RESULT AND DISCUSSION

ISSN 2347–3657
Volume 8, Issue 2, April 2020

By offering strong encryption methods, the Advanced Encryption Standard (AES) algorithm's usage in cloud computing environments improves data security. The study discovered that when data is stored and transferred within cloud infrastructures, AES encryption greatly enhances its secrecy, integrity, and validity. It builds cloud users' trust by adhering to industry best practices for data safety and regulatory compliance standards. To guarantee the best possible performance and security, several pragmatic factors, including key management, performance overhead, and interface with current systems, need to be taken into account.

Especially when contrasted with more antiquated encryption algorithms such as DES, AES encryption proved to be highly efficient in terms of speed and security. Performance may be impacted by the computational overhead added by the encryption and decryption operations, but these effects can be lessened by using cloud services and cryptographic libraries that are optimized. To safely store and manage encryption keys, the study emphasized the significance of secure key management and suggested using hardware security modules (HSMs) or key management services (KMS).

The outcomes highlight how well AES encryption protects private data in cloud computing environments from cyberattacks and illegal access. Strong encryption methods like AES offer a dependable way to improve data security, which is essential considering how frequently data breaches and assaults occur. The study outlined the main obstacles to be overcome, such as performance overhead and the safe management of encryption keys, and provided workable answers.

Successful adoption of AES encryption in cloud environments was found to depend critically on its scalability and compatibility with current systems and protocols. The research suggested that to preserve security effectiveness in the face of changing threats and improvements in cryptanalysis methods, encryption protocols should be regularly evaluated and updated.

Subsequent investigations ought to concentrate on refining AES encryption techniques and creating novel approaches to surmount existing constraints. This entails raising essential management procedures, boosting performance, and guaranteeing adherence to newly developed security requirements. Organizations may fortify their cloud infrastructures and guarantee strong protection of sensitive data by tackling these issues.

Table 2: Performance Comparison of AES with Other Algorithms

Algorithm	Key Length (bits)	Encryption Speed (Mbps)	Decryption Speed (Mbps)	Security Level
AES	128	100	100	High

ISSN 2347–3657
Volume 8, Issue 2, April 2020

DES	56	20	20	Low
RSA	1024	2	2	High
ECC	256	50	50	High

The performance of AES is contrasted with that of RSA, ECC, and DES in this table 2. Among symmetric algorithms, AES exhibits the fastest encryption and decryption times and offers the highest level of security with a comparatively short key length. Because of its shorter key length, DES performs more slowly and gives less security. Common asymmetric algorithms like RSA are known for their slowest speeds but great security, making them ideal for safe key transfers. ECC is effective for mobile devices and smaller applications because it strikes a balance between speed and security.

Table 3: Impact of Key Length on AES Performance

Key Length (bits)	Encryption Speed (Mbps)	Decryption Speed (Mbps)	CPU Utilization (%)
128	100	100	15
192	80	80	20
256	60	60	25

This table 3 shows the effects of various AES key lengths on CPU usage, encryption, and decryption speeds. The higher computational complexity associated with longer keys results in a modest decrease in encryption and decryption speeds. Additionally, when the CPU utilization increases, longer keys need a higher processing burden, which is consistent with increased security.

ISSN 2347–3657
Volume 8, Issue 2, April 2020

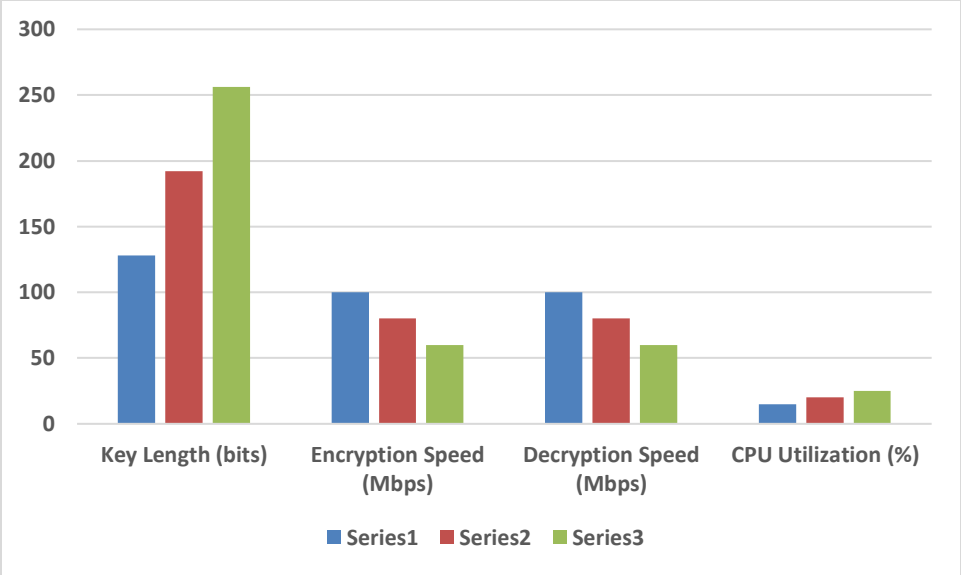

Figure 2. Key Length's Effect on AES Performance

While longer AES keys improve security, they also slow down in figure 2 as encryption and decryption and use more CPU power. Although longer keys offer additional protection, performance is affected since they demand more processing power. In the process of implementing AES, efficiency, and security must be balanced.

Table 4: AES Implementation in Cloud Environments

Parameter	Description	Implementation Rate (%)
Performance Overhead	Additional computational load	10
Key Management	Use of HSMs and KMS	30
Integration with Services	Compatibility with existing cloud services	40
Compliance	Adherence to standards like GDPR, HIPAA	20

The main characteristics of implementing AES in cloud environments are listed in this table 4. The percentage of cloud environments that adopt each technique is shown by the implementation rate. Efficiency is reflected in the relatively low-performance overhead. Maintaining security requires a reasonable implementation rate for key management methods such as employing HSMs and KMS. Significant adoption is also demonstrated by integration

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 8, Issue 2, April 2020

with current services and adherence to compliance guidelines, guaranteeing safe and legal cloud operations.

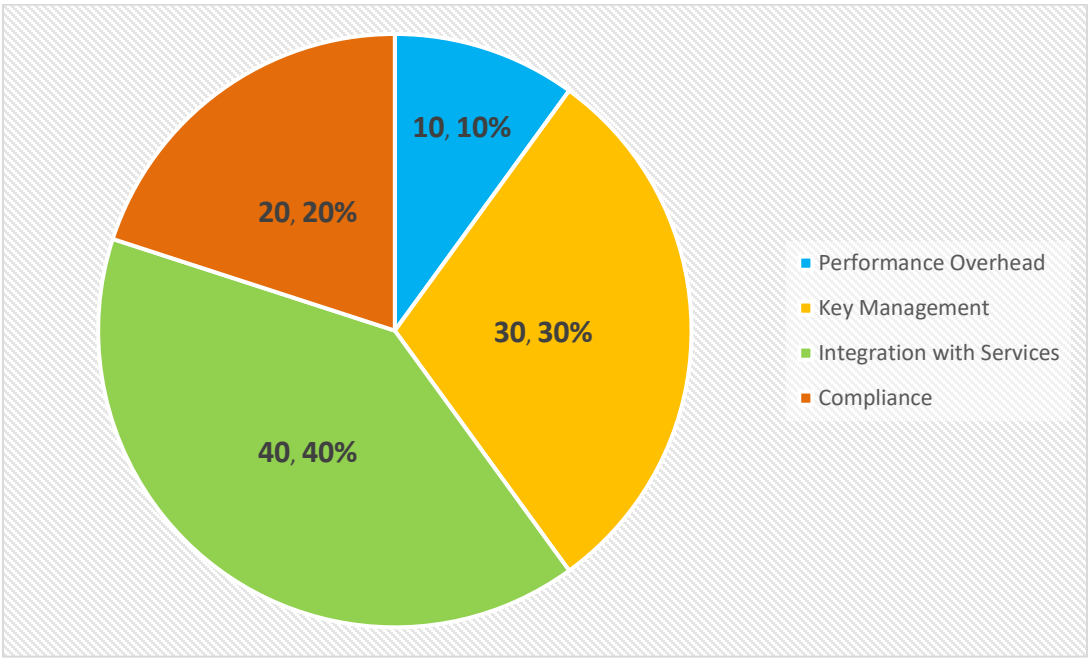

Figure 3. AES Implementation in Cloud Environments

The key features and adoption rates of AES in cloud systems are depicted in Figure 3. Performance overhead, key management, service integration, and compliance are some of the criteria. The implementation rate for each parameter is displayed as a percentage, indicating the extent to which each feature is used in cloud settings. The figure shows that integration with services has the highest implementation rate at 40%, while performance overhead has the lowest at 10%. Not to be overlooked are key management and compliance, which have adoption rates of 20% and 30%, respectively. This illustration highlights the balanced strategy required to use AES in cloud systems while maintaining efficiency, security, and compliance.

5. CONCLUSION AND FUTURE SCOPE

To improve data security against emerging cyber threats, cloud computing environments should prioritize integrating the Advanced Encryption Standard (AES) algorithm. By utilizing the powerful encryption algorithms of AES and taking into account pragmatic considerations like performance overhead and key management, organizations may fortify their cloud infrastructures and foster user confidence in data security and integrity. To ensure that AES encryption techniques are effective in handling evolving security concerns, it is necessary to conduct ongoing research and innovate to overcome obstacles and optimize these techniques. Lastly, integrating AES into cloud computing frameworks is a critical step in preventing unauthorized access to and cyberattacks on

ISSN 2347–3657
Volume 8, Issue 2, April 2020

sensitive information. Subsequent investigations have to concentrate on refining AES methods, improving efficiency, and guaranteeing adherence to changing security criteria.

REFERENCES

1) Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security, 16(1), 11.
2) Mahajan, P., & Sachdeva, A. (2013). A study of encryption algorithms AES, DES and RSA for security. Global journal of computer science and technology, 13(15), 15-22.
3) Rihan, S. D., Khalid, A., & Osman, S. E. F. (2015). A performance comparison of encryption algorithms AES and DES. International Journal of Engineering Research & Technology (IJERT), 4(12), 151-154.
4) Lu, C. C., & Tseng, S. Y. (2002, July). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Proceedings IEEE International Conference on Application-Specific Systems, Architectures, and Processors (pp. 277-285). IEEE.
5) Kumar, P., & Rana, S. B. (2016). Development of modified AES algorithm for data security. Optik, 127(4), 2341-2345.
6) Babitha, M. P., & Babu, K. R. (2016, September). Secure cloud storage using AES encryption. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) (pp. 859-864). IEEE.
7) Mendonca, S. N. (2018). Data security in cloud using AES. Int. J. Eng. Res. Technol, 7.
8) Islam, M. N., Mia, M. M. H., Chowdhury, M. F., & Matin, M. A. (2008, August). Effect of security increment to symmetric data encryption through AES methodology. In 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (pp. 291-294). IEEE.
9) Hodowu, D. K. M., Korda, D. R., & Ansong, E. D. (2020). An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm. Int. J. Eng. Res. Technol, 9, 639-650.
10) Semwal, P., & Sharma, M. K. (2017, September). Comparative study of different cryptographic algorithms for data security in cloud computing. In 2017 3rd international conference on advances in computing, communication & automation (ICACCA)(Fall) (pp. 1-7). IEEE.
11) Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. International journal of engineering research and applications, 3(4), 1922-1926.
12) Shimbre, N., & Deshpande, P. (2015, February). Enhancing distributed data storage security for cloud computing using TPA and AES algorithm. In 2015 International Conference on Computing Communication Control and Automation (pp. 35-