JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A LITERATURE SURVEY ON WIDE USAGE OF ADVANCED ENCRYPTION STANDARD ALGORITHM FOR PRIVACY AUTHENTICATION IN CLOUD COMPUTING

[1]G Kiranmai,[2] Dr. E.V.N. Jyothi
[1]Designation of PG Student, [2]Asociate Professor
[1]Department of CSE,
[1]RISE Krishna Sai Prakasam Group of Institutions, Ongole, AP

Abstract : **The aim of this study is to identify the importance and wide usage of Advanced Encryption standard algorithm to enhance the utilities of applications in cloud computing. Here we conduct a literature survey on data encryption to use the privacy applications of cloud to encrypt or decrypt the data in database. Cloud computing offers various types of services to users. In the recent decade, there has been increase in the use of storage from the service providing organizations. In order to safeguard the data saved in the cloud, this paper addresses the AES encryption mechanism, which is a contemporary secure cloud protection and safety technology employed in the cloud platform. This paper explains study of enhancement technology for confidential data authentication with a Secure Framework and appliance in the cloud computing for better usage.**

***IndexTerms* -** Security, Advanced Encryption Algorithm, Encryption, Specific factors, Cloud computing.

I. INTRODUCTION

Cloud computing has emerged as an important paradigm that has impressively attracted in both industry and academia. Cloud computing offers number of services to its users who use of hardware and software resources via internet without the need of large database and maintenance fee. Cloud computing existed under names like outsourcing and Server hosting through wireless communication. Day to day usage of cloud computing attracted attackers to unlock the security in the cloud. Privacy through authentication is noticed as the need of the customers to protect their data. To achieve this authentication in cloud computing we have existed technologies.

It has been noted that cloud computing is employed in numerous architectures, services that incorporate other technologies, and software design methodologies. Platform as a service (PaaS), software as a service (SaaS), and infrastructure as a service (IaaS) are examples of cloud service paradigms. Four cloud platform deployment strategies are necessary for public, private, community, and hybrid system architecture solutions. Flexibility, accessibility, and capacity are benefits of cloud computing when compared to conventional online computing or storage methods. Computational clouds do, however, raise a variety of security risks, such as (i) privacy and security issues with cloud service providers and (ii) security issues pertaining to customers..

Many people use the cloud every day without knowing how to secure the data for communication and storage purposes. Cloud computing security is one of the challenges to the users of cloud computing with large technologies to protect the data from the attackers. These attacks are like sending fault messages, viruses, spam, spoofing etc. To overcome these unauthorized access from the attackers we has the existing technology called as Data Encryption algorithm. In this the key length used by the DES algorithm is 64 bits, and the effective key length is 56 bits. Because the key is small, it cannot provide enough security. Before the process every 8 bit of key is kicked out to produce a 56-bit key. DES operation involves a series of rounds with key transformation, permutation, and substitution, and finally producing cipher text from plain text. This is used for encryption and decryption. The Encryption process of plain block text is, as initial permutation on plain text it separates as two LEFT and RIGHT plain text and be subjected to 16 rounds of the encryption process. In the end these two, LEFT and RIGHT cipher text are rejoined to produce a 64-bit cipher text. Even though it has played a significant role in data security, due to vulnerabilities, its popularity has declined.

As the further step, AES algorithm is designed. In this paper we discuss various frame works for enhancing the authentication technology in AES algorithm. This article spell out specific factors for wide usage of Advanced Encryption standard algorithm, and its enhancement from data encryption to Advanced encryption standard and conclusion on extensive usage of the algorithm based on few review papers.

This review, discuss literature survey about AES algorithm in session1 for privacy authentication, methodology and working process in section2, section 3 describes about result and section 4 discuss the conclusion.

II. Literature Review

AES was modified in a number of ways to increase security and performance speed by adding some complexity to the algorithms. These adjustments are made to various hardware and software architectures. However, because of some security limitations and issues with cloud computing, preview framework security is never completely guaranteed. Cryptography algorithms are used to offer security to data that is kept on the cloud. There are large encryption algorithms used in cloud computing security frameworks. A few of these are showcased below.

In addition to emphasizing encryption and decryption techniques that let cloud users feel secure about their data, the authors of this research suggested a new architecture that guarantees data security and integrity. The enhanced security and performance were discussed in the suggested solution. Real-time system monitoring, virus identification, and the operation of the forensic virtual machine have all been integrated in their solution. The authors of this research proposed a framework in which the goal is to store data across many clouds. The provided framework is based on encryption using both RSA and 3DES. Conversely, this approach lacks privacy, efficiency, and middleware overload through many functions . The authors examined multilayer licensing framework approval in this paper.

The dismissal of logical purposes in the MixColumn conversion of AES resulted in the complexity detects. In the updated AES, these sensible duties were eliminated. Following that, using the improved AES resulted in a reduction of 13.6% in LUTs, 10.93% in share discount, and 1.19% in interruption eating. The limited dispersal rate reached by the cautious AES at the first nonentity, as well as significant agenda sequences, are also mentioned in previous papers. Five variables were carefully studied in this research: show distance, pixel-by-pixel assessment, radiance histogram, file size, and graphic study. The file scopes showed discrepancies in the regular worth of the fraction variations, which varied from −23.85% for the unique to the encrypted duplicate to −1.45% for the inventive.

Cloud computing envisions an alternative method of accessing cloud data into the real world. For privacy, authenticity, and contact controller, 128 bit AES encryption is recycled. The two most popular weight balancer techniques, namely Round-Robin and Supper Present Implementation Freight, also known as Active Monitoring Load Balancer, have been contrasted with load balancing using My Load Balancer optimization method in upcoming work. The Cloud Analyst Toolkit is created using all of these virtual methodologies based on Java. To support the comparative analysis, graph processes have been recycled.

III. Methodology

Advanced Encryption Standard (AES) algorithm is one of the security service used in cloud computing for securing sensitive data. It is a symmetric key algorithm. In this system a private key is generated by using bilinear pairing with hashing technique. It is used for both encryption and decryption. AES has several key lengths, with 128-bit being most common. This gives its structure and security greater flexibility. It carries out the parallel operations of substitution and permutation. Rather than using bits for all of its calculations, AES uses bytes. AES encrypts and decrypts data using a state array, whose rows are utilized for permutation, single byte replacement, column-wise mixing, and round key addition; however, the execution sequence is not exactly as stated. As a result, AES interprets a plaintext block's 128 bits as 16 bytes. It has four steps like sub bytes, shift rows, Mix columns and Add round key. The number of rounds will based on the cipher key size. Many people known for its efficiency and security, making it the standard choice for many encryption and decryption applications.

Specific Aspects to improvement in Encryption:

- For modern data encryption ceaseless developing and acquire stronger encryption algorithms that are repellent to cryptographic attacks.
- Enhancing key management practices to ensure secure generation, strong, distribution, and revocation of encryption keys.
- Researching and implementing encryption techniques that are resistant to quantum computing attacks, which have the potential to break current encryption methods.
- Developing and deploying cryptographic algorithms that are secure against both classical and quantum computing threats.
- Optimizing encryption algorithms and protocols to minimize computational overhead and latency, especially in resource – constrained environments like IOT devices.
- Integrating robust authentication mechanisms with encryption to ensure the integrity and authenticity of data exchanged between parties.
- Regularly monitoring and updating encryption systems to address emerging threats and vulnerabilities.

IV. Working Procedure

General use of AES algorithm is for encryption and decryption of the data. Now a days AES algorithm is most effective and symmetric block algorithm and is universally accepted. Rather than bits it execute all its computations on bytes. It generates a secret key to transform, the plain text to cipher text and cipher text to plain text called encryption and decryption. Figure 1 explains the basic process of encryption and decryption.

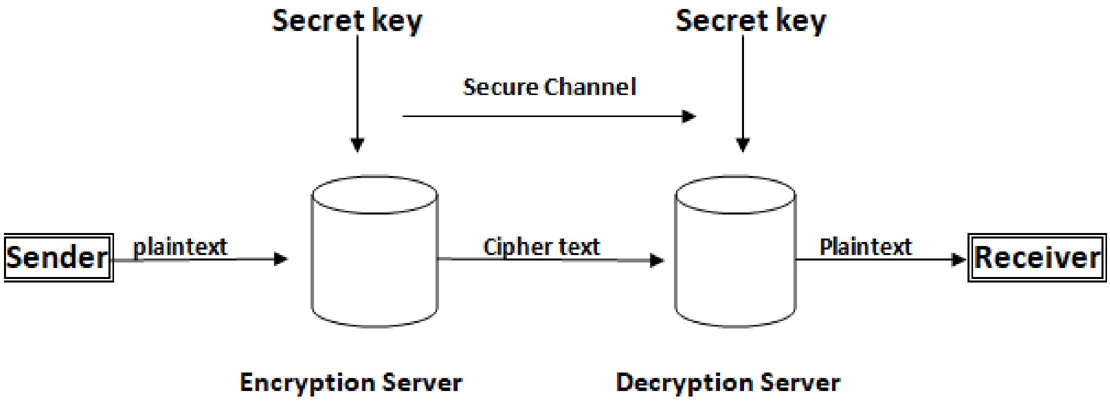
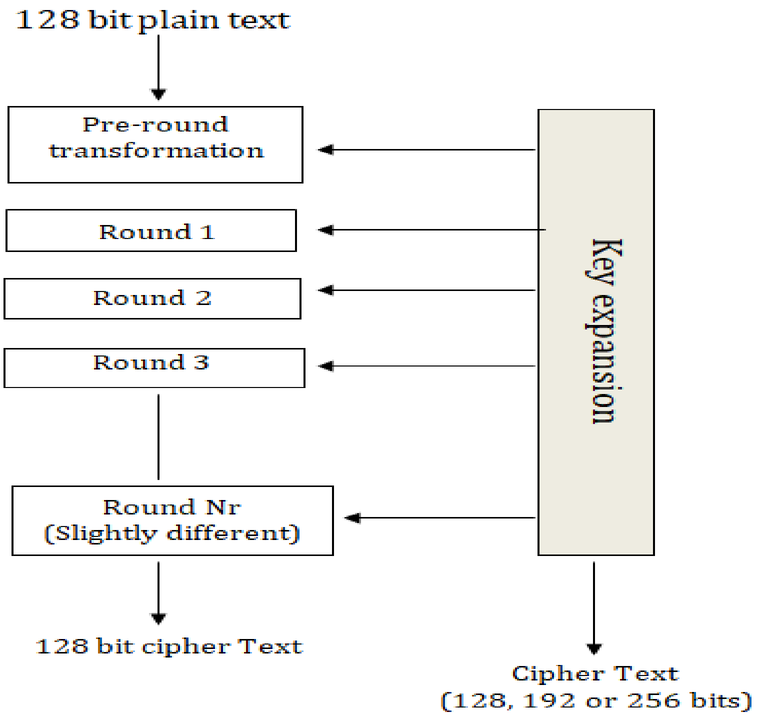


Figure 1: Basic Structure of AES algorithm

AES is an iterative rather than cipher. AES comprises a series of linked operations which involve replacing inputs by specific outputs and others involve shuffling bits around. AES encryption process mainly works on 4 by 4 matrix. AES Process mainly starts with AddRound key. Figure 2 explains the frame work of AES algorithm, it has N number of rounds depend upon the key size. Here, key size either 128, 192, 256 bits and rounds are 10, 12, 14 respectively.



R	Key size
10	128
12	192
14	256

Relationship between Number of rounds® and Cipher key size

Figure 2: Frame work of AES algorithm

It has four steps in its operation:

1. *SubByte*: In this each byte is replaced by a lookup table through 1 by 1 matrix. This stage is depends on non-linear S-box to substitute a byte in the state to another byte.
2. *Shift rows*: Next step is shift rows, the main idea behind this step is to shift bytes to left. Hence, the bytes of row number zero remains and does not carry out any permutation.
3. *MixColumn*: In mixColumns multiplication is carried out and each byte of one row in matrix transformation must multiply by each column of the state. Final result of multiplication used with XOR to produce a new four bytes for the next step. Here the size of original size is 4 by 4 only.
4. *AddRoundKey*: it has the ability to secure the encrypting data. It build relationship connecting the key and cipher text. In this the main key is used to extract the subkey in each round by using Rjindael's key schedule. The subkey is added by merge each byte of the state with the consistent byte of the subkey using bitwise XOR.

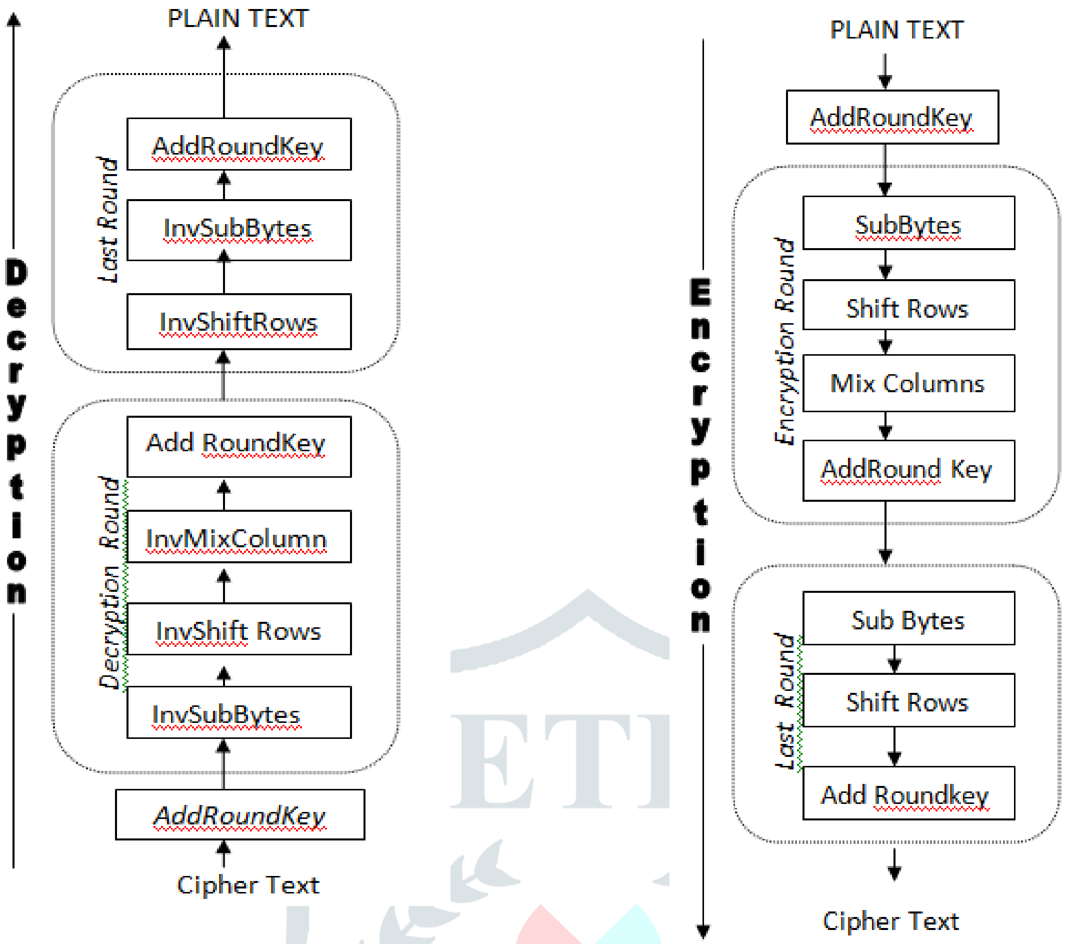


Figure 3: Encryption and Decryption procedure of AES algorithm

V. Result

In this paper we have seen that AES algorithm is used for privacy authentication and efficient than Data Encryption algorithm. With this algorithm privacy authentication is more secure and against the caricature attacks. Here we don't have to register again and again in the cloud, then we can able to use the services with less time consuming. It is clear that, we can enhance text for authentication and better frame work for much secure. The following table shows the security specifications of AES algorithm. I noticed that, when comparing the DES algorithm and AES algorithm, in DES algorithm there is no possibility for Mutual authentication. But in AES algorithm we have Mutual authentication.

TABLE 1
SECURITY SPECIFICATIONS IN AES ALGORITHM

Mutual authentication	YES
User anonymity	YES
Untrace ability	YES
Key establishment	YES
Known session key security	YES
Perfect forward secrecy	YES
No verifier table	YES
No clock synchronization	YES
Resistance of known attacks	YES

VI. Conclusion

AES is extended custom configurable encryption is the foundation of the work. AES algorithm is the improvement to the DES algorithm. AES has the potential to protect exposed data from assaulters and to damage the encrypt data as compared to the Existed data encryption algorithm. Here, we observe that DES is a block cipher with a 56-bit key length. But in AES has the propensity to deal with three different key lengths such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. This algorithm's advantage is that it encourages cloud storage frame works a vertebrae structure to boost security. Although, this proposed system is useful only for text files. It does not works with image, audio and video files. As a result, the AES algorithm is a very safe encryption method. Additionally, data can be shielded against upcoming assaults like smash attacks. While other symmetric encryption algorithms have flaws and differ in performance and storage capacity, the AES encryption algorithm has minimal storage requirements, great performance, and no limitations. AES encryption is used regularly by federal government departments as well as non-government entities, commercial firms, and organizations, to secure sensitive data.

References

[1] M. Satyanarayanan, "Fundamental challenges in mobile computing," in Proc. 15th Annu. ACM Symp. Princ. Distrib. Comput., 1996, pp. 1–7.

[2] A. Lin and N.-C. Chen, "Cloud computing as an innovation: Percepetion, attitude, and adoption," Int. J. Inf. Manag., vol. 32, no. 6, pp. 533–540, 2012.

[3] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340–352, Feb. 2016.

[4] M.Armbrustetal.,"Aviewofcloudcomputing,"Comm un.ACM,vol.53, no. 4, pp. 50–58, 2010.

[5] M. Edjie, D. L. Reyes, M. Ariel, Sison, and Dr.R. P. Medina, "Modified AES cipher round and key schedule," Indonesian Journal of Electrical Engineering and Informatics (IJEEI), vol. 7, no. 1, March 2019.

[6] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[7] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981. [8] E.-J. Yoon, K.-Y. Yoo, C. Kim, Y.-S. Hong, M. Jo, and H.-H. Chen, "A secure and efficient sip authentication scheme for converged VOIP

[8] M. Marwan, A. Kartit, and H. Ouahmane, "A framework to secure medical image storage in cloud computing environment," Journal of Electronic Commerce in Organizations, vol. 16, no. 1, pp. 1–16, 2018.

[9] P. Sirohi and A. Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy and trust," in Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), pp. 4-5, Dehradun, India, September 2015.

[10] K. Subramanian, F. L. John, and F. L. John, "Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system," International Journal of Advanced and Applied Sciences, vol. 5, no. 1, pp. 15–23, 2018.

[11] V. Surya, S. Ranichandra, and R. Ranjani, "Secure cloud storage using AES encryption," International Journal of Innovative Research in Computer and Communication Engineering, vol. 6, no. 6, 2018.

[12] A. Nair and S. S. SantoshAnand, "A performance booster for load balancing in cloud computing with my load balancer technique," International Journal of Recent Technology and Engineering, vol. 8, no. 1, 2019.

[13] Ijaz Ahmad Awan, Security and Communication Networks Volume 2020, Article ID 8863345, 16 pages https://doi.org/10.1155/2020/8863345 , Academic Editor: Umar M. Khokhar

[14] Kundlik Waybhase "Data Security using Advanced Encryption Standard(AES)" ISSN: 2278-0181 IJERTV11IS060338, Published by : www.ijert.org Vol. 11 Issue 06, June-2022.

[15] Smitha Nisha Mendonca, Data Security in Cloud using AES, (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV7IS010104 Published by : www.ijert.org Vol. 7 Issue 01, January-2018.

[16] 'Applications of advanced encryption standard algorithm' [website] date: 30-05-2024 and time: 12:00pm from google.