International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 3, May-June 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

# Enhancing Data Security with the Upgraded AES Algorithm

SUPRIYA SINGH[1] , Prof. SATISH SONI[2],

[1]Scholar, Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India
[2]Professor & Head of Computer Science & Engineering Department, JNCT Rewa M.P. 486001 India

## ABSTRACT:

In this specialised world where data is transported by electronic means and kept on clouds, information security is a critical subject to take into account. There have been many other recommended configurations, but each has limitations unique to that situation. Here, a new security paradigm is presented in an effort to safeguard the cloud environment from diverse attacks originating from several malevolent hosts. Advanced Encryption Standard is an example of a cryptographic technique in which anyone having the key may read the message without any issues. The current technique uses keys with sizes of 128, 192, and 256 bits. Decoding the encoded text becomes more challenging as the key's size increases. As a result, the information and key sizes both approach 512 bits.

## 1. INTRODUCTION :

Numerous new network-related technologies are being incorporated as the Internet expands in order to enhance service quality. With capabilities like service and application virtualization, cloud computing is brought in this scenario to the distributed computing environment. The study finds that the network's overall latency and traffic volume are reduced by the deployment of dynamic code and remote data processing utilising cloud infrastructure. The issue for the feature-rich cloud technology, however, is the defence against numerous assaults.

## 1.1TYPES OF CLOUD

There are several distinct kinds of cloud infrastructures utilised to deliver effective services in the cloud environment. The component that the user uses to call cloud operations is known as the client, and cloud infrastructure is referred to as infrastructure that is located at a remote location from the home client. According to how it is used and maintained, there are three primary categories for cloud infrastructure.

**Public Cloud:** Third parties are in charge of maintaining public clouds. Utilising storage structures, server facilities, and infrastructures, the cloud classifies activities or jobs from various clients. The final customer won't be aware of which tasks are being carried out on the same network, disc, or server as their own work. Based on the starting conditions described in the cloud owner's profile, it may be static or dynamic.

**Private Cloud:** It is an on-demand framework managed by a single user who controls applications and decides where they run. This cloud maintains the network, disk and server. They can allow selected users access to the framework.

**Hybrid Cloud:** This cloud combines private and public cloud. Parts of the cloud are owned by industry and some are distributed in a controlled manner. Although targeting applications to diagonally different regions is difficult to define, it works at the level of demand and external control.

## 1.2 Cloud Attacks

Shadow IT is a wonderful thing until it constantly meets cloud security. Very often, users create applications and transfer data to the cloud without seeing all the security offers. The Cloud Security

  

Alliance consists of nine broad and serious cloud service security threats. Most of them are related in one way or another to the downside of Shadow IT. When it comes to cloud security, unfortunately, security holes have been found in the cloud environment that lead to attacks. The following are some known attacks in the cloud environment.

## 1.3 Denial of Service

Denial of service is a kind of attack used from olden days for online operations that still remain a major threat. There are millions of automated service requests exists, screening and detection of those attacks is essential before it affect the operations. Attackers also have improvised their infrastructure in a sophisticated manner, making it tough to detect the traffic. Sometimes the customer may experience denial of certain services; it is more like getting caught in rush hour traffic. The customer cannot reach the destination; all he can do is sit and watch. If any customer faces such attack in the cloud, it sometimes damages the service without shutting down, the cloud service will charge the customer for the employed resources during the attack. "If the service attacks are denied continuously, then it will make the customer very expensive to run the service and he will be forced at one point to go for it." The report said.

## 1.4 OBJECTIVE

The main objective of the paper is to design a security architecture that protects the cloud environment from various attacks. The objectives of the proposed architectural project include.

- Protection of cloud data against malicious attacks with an advanced cryptographic encryption standard.
- Cloud platform protection with a higher level of security and protection against unauthorized users.

## 2.LITERATURE SURVEY:

**1.Nalini Priya & Aswin Kumar (2013):** proposed a system to restrict the attack on data by using the exceptional cryptographic encryption techniques. The proposed algorithm AES-NI prevents the privacy of the sensitive data that are stored in the server.

**2.ashaswi Singh et al. (2011):** The Secured Cost-Effective Multi-Cloud Storage in Cloud Computing provides each user a better cloud data storage, considering both the consumer budget and available best quality of service given by CSP.

**3.Priyadharshini Patil et al. (2015):** studied the strength, weakness, cost and performance of various algorithms like DES, AES, RSA,3DES and Blowfish algorithms in order to show overall performance analysis algorithms in this today's internet era, with online transactions almost every second. In this work the author used only 128 bit key to encrypt the text message. But nowadays attackers using various novel approaches to reveal the original message. So, the algorithm may be vulnerable over the internet based transactions.

**4.Rohan Rayarikar et al. (2012):** presented encryption is of prime importance when confidential data is transmitted data is transmitted over the network. In this work there is a huge amount of confusion and diffusion of the data during encryption which makes it very difficult for an attacker to interpret the encryption pattern and the plain text form of the encrypted data.In the above algorithm they used AES 128 bit key length to encrypt the data. AES has its own advantages using this approach. But they used only128 bit key length to encrypt and decrypt the data. This could be leads to brute force attackers crack the data.

# 3. PROPOSED AES-X MODEL :

This chapter presents the proposed AES-X model, which protects the cloud platform against malicious attacks by encrypting the entire data. In addition, a key ring-based mechanism is described to improve the

  

efficiency of the method. Due to increasing algorithm parameters and complex algorithm, any system with only text size and position requires more chip and security. To improve the strength and efficiency of AES-X for secure communication, the key length is increased to 512 bits and thus the number of rounds. The number of laps is set at 22, which is a novelty of the approach.A modification using 512 bits for AES algorithm is proposed in this thesis. The purpose of this work is to show that AES 512 bit can be utilized whenever the system looks for a high-level security throughput by not changing overall design area comparing traditional techniques. The structure of the proposed AES algorithm is similar to original AES algorithm but with aslight modification that key size and plaintext size uses input of 512 bit whereas the original algorithm uses 128 bits. This impact is observed in the whole algorithm structure, and the same will be discussed in detail in this chapter. The AES algorithm comprise of 4 primary actions executed in each round, namely;

1) Byte substitution

2) Shifting rows

3) Mixing columns

4) Adding the round key

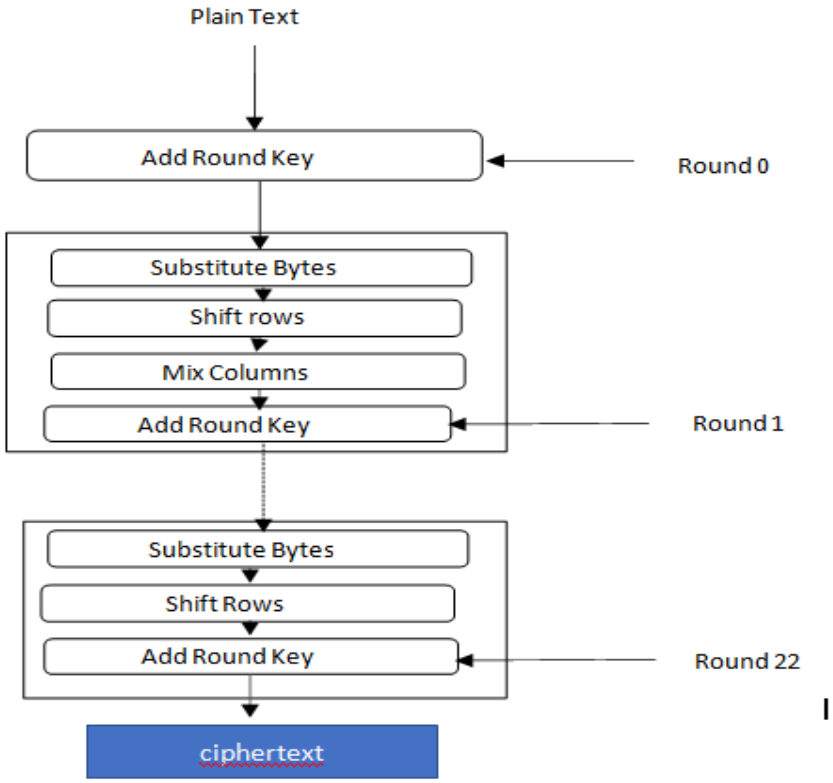


**Fig. 1 : AES 512 bits System**

## 4. APPLICATION OF PROPOSED SECURITYMODEL

This chapter illustrates the application of a security model with experimental results in eHealth environments to protect authentic medical record images from all false malicious claims by a malicious host. All the proposed security models were implemented and tested to prove their effectiveness in several perspectives

  

using medical data from the Microsoft Azure Cloud. Under National Data Protection Principle 4 of the Privacy Act 1988 (Cth), doctors/practitioners have a legal duty to ensure that various safeguards are in place to protect patients' health information. This applies to all patient records, whether electronic or paper, audio/video, x-rays and photographs, etc. Appropriate security measures are important when storing patient health data. Although national data protection principles provide guidance, it is up to the healthcare professional and the healthcare institution to ensure that data remains secure.

Few examples are:

- Safeguarding the computer system using password protectionby regularly changing the passwords
- Having backup facility for all data
- Maintaining lockable physical security for paper records
- Transferring data securely
- Monitoring and evaluating information systems for the data security.

## 5 CONCLUSION :

This chapter concludes by showing how the research objectives were achieved and provides a road map for future research. In this technical world, data is transmitted through electronic media and stored in clouds, where data security is the biggest concern. Although many solutions have been proposed, each has its own disadvantages for different environments. Here, a new security model is proposed to protect the cloud environment against attacks from multiple malicious hosts. One such encryption algorithm is the Advanced Encryption Standard algorithm, where anyone with the key can easily read the message. The current algorithm uses key sizes of 128, 192 and 256 bits. As the key size increases, decrypting the cipher becomes difficult. Therefore, the size of input and key is increased to 512 bits, which provides better security. The number of plaintext processing rounds increases to 22, with all four AES algorithm operations performed in the first 21 rounds and three of the four encryption operations performed in the last round. Decryption is performed using the reverse operations of the encryption algorithm. AES-X is suitable for applications with high security and performance requirements without increasing the overall structure compared to the original AES-128 bits. The extended key size 512-bit model of the developed project is evaluated for its capability in e-health environments. The input images and the corresponding encrypted images are displayed. A DICOM image is taken as the input image. Analysis such as key mode analysis, key sensitivity analysis, histogram analysis, correlation analysis, PSNR and MSE analysis .

**REFERENCES :**

1. Abidalrahman Moh'd & Yaser Jaraweh 2011, 'AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evaluation'. International Conference on Information Assurance and Security (IAS). IEEE, pp. 292.297.

2. Alan Kaminsky, Michael Kurdziel & Stanisław Radziszowski, 2010, 'An Overview of Cryptanalysis Research for the Advanced Encryption Standard'. The 2010 Military Communications Conference - Unclassified Program - Cyber Security and Network Management IEEE, pp. 1310-1316.

3. Alanazi, H, Zaidan, BB, Zaidan, AA, Jalab, HA, Shabbir, M & Al- Nabhani, Y 2010, 'New comparative study between DES, 3DES and AES within nine factors'. arXiv preprint arXiv:1003.4085.

  

4. Ali Inan, Gabriel Ghinita, Murat Kantarcioglu & Elisa Bertino 2012, 'A Hybrid Approach to Private Record Matching Fellow'. IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 5.

5. Ali, M, Sagheer, Salah, S, Al-Rawi, Omar, A 2011, 'Proposing of Developed Advance Encryption Standard'. E-systems Engineering (DeSE), pp. 197-202.

6. Amador, JJ & Green, RW 2005, 'Symmetric□key block cipher forimage and text cryptography'. International Journal of Imaging Systems and Technology, vol. 15, no. 3, pp. 178-188.

7. Anand Kumar, M & Karthikeyan, S 2012, 'A New 512 Bit Cipher for Secure Communication'. International .Journal of. Computer Network and Information Security, vol. 11, pp. 55-61.

8. Anand, K & Sekar, AC 2015, 'Invulnerable Colossal Information Storage Based on Dynamic Encryption Algorithm on Cloud'. International Journal of Soft Computing, vol. 10, no. 2, pp. 137-142.

  