International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 54-58 www.ijaem.net ISSN: 2395-5252

Secured File Transfer with Advanced Encryption Standard

Mahesh S[1], Nagarajan[2]
1.IIMCA, 2. Professor,MCA,
Sri Muthukumaran Institute Of Technology,Mangadu Sri Muthukumaran Institute Of Technology,Mangadu

----
Date of Submission: 01-09-2022 Date of Acceptance: 08-09-2022

ABSTRACT— Advanced Encryption Standard Cipher Block Chaining Mode (AES CBC) is a symmetric encryption standard. The Advanced Encryption Standard (AES) is an encryption algorithm that is used for securing sensitive unclassified information. AES is proved to be a highly secure, faster, and strong encryption algorithm. AES is used commonly because of its great competence and ease. In reality, the communication channel which is used to transfer data from transmitter to receiver is highly insecure. To resolve this problem the data is being manipulated to another form so that the person with access to the secret key can only read it. This process of manipulation of original data to another form so that an eavesdropper cannot access it is known as encryption. Advanced Encryption Standard (AES) is the most commonly used algorithm for data encryption. This algorithm can be applied to both text and image files that want their file to be secure enough. CBC mode achieves this by XOR-ing the first plaintext block with an initialization vector before encrypting it. CBC also involves creating a block as every subsequent plaintext block is XOR-ed with the ciphertext of the previous block. Thus by utilizing CBC user data can be secured by encryption and decryption which eventually makes it non-vulnerable for an eavesdropper.

I. INTRODUCTION

In the block chain, Advanced Encryption Standard Cipher Block Chaining Mode (AES CBC) is a symmetric encryption standard. The Advanced Encryption Standard (AES) is an encryption algorithm that was selected by the National Institute of Standards and Technology (NIST) for the United States government, commercial, and private organizations to use for securing sensitive unclassified information. AES is proved to be a highly secure, faster, and strong encryption algorithm. AES is used commonly because of its great competence and easiness. In reality, the communication channel which is used to transfer data from transmitter to receiver is highly insecure. To resolve this problem the data is being manipulated to another form so that the person with access to the secret key can only read it. This process of manipulation of original data to another form so that eavesdropper cannot access it is known as encryption. Advanced Encryption Standard (AES) is the most commonly used algorithm for data encryption. This algorithm can be applied to both text and image. CBC mode achieves this by XOR-ing the first plaintext block (B1) with an initialization vector before encrypting it. CBC also involves block chaining as every subsequent plaintext block is XOR-ed with the ciphertext of the previous block. In this paper, the input to the AES algorithm is Text and an image, which results in encrypted output. This encrypted output is given as an input to the AES decryption algorithm, which results in decrypted output. The algorithm is implemented using PYTHON software.

OBJECTIVE

We entrust our personal and sensitive information to lots of major entities and still have problems with data breaches, data leaks, etc. Some of this happens because of security protocols in networking, or bad practices of authentication management but there are many ways that data breaches can occur. In our application customers needs to share their highly confidential files with auditors so that expertise can work on them then revert to customers. During this file transaction, our customer's file is not secure which makes it vulnerable to hackers. Our application uses AES, the proposed technique has AES CBC (Cipher Blocker Chaining) mode. In AES CBC mode has been implemented to encrypt data in files for high-security purposes. Once the user has uploaded the file then the file data was encrypted by AES- CBC mode. The auditor or user couldn't download the file original file without decryption of data. Decrypting of data was needed the access key. The ciphertext will be decrypted by AES- CBC mode with an access key.

SLDC (Software Development Life Cycle)

The Software Development Life Cycle is a systematic process for building software that ensures the quality and correctness of the software built. SDLC process aims to produce high-quality software which meets customer expectations. The software development should be completed within the pre-defined time frame and cost.

SDLC Phases : The entire SDLC process is divided into the following stages:

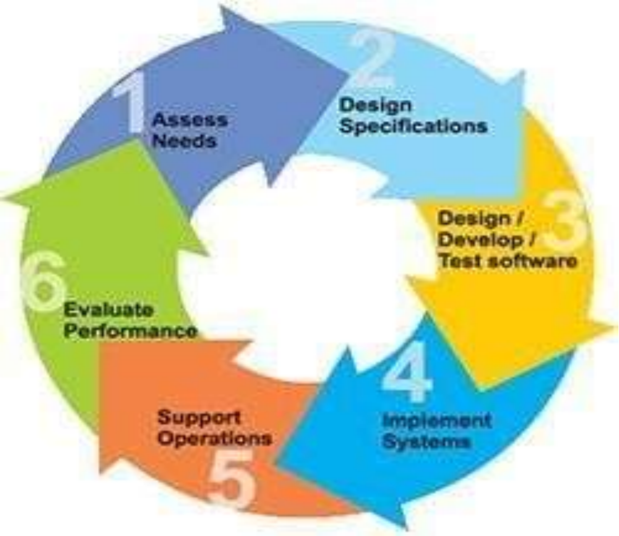
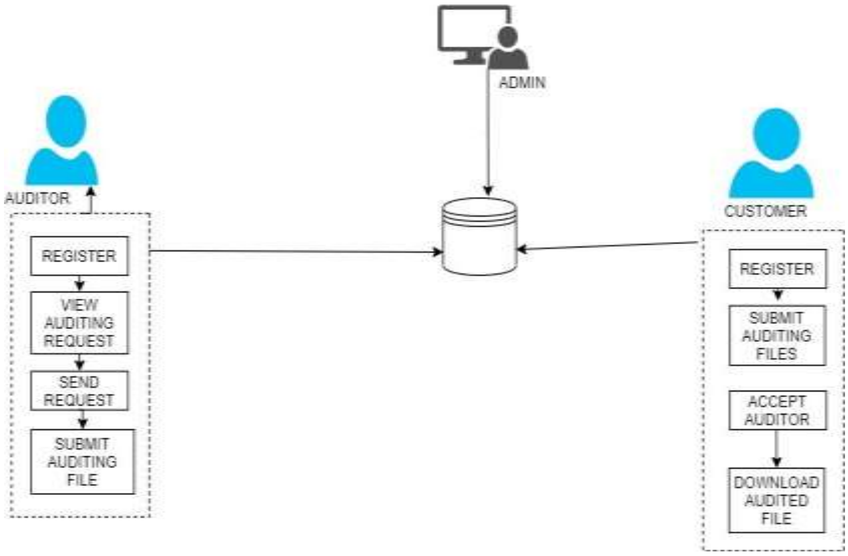


Fig: 1-SLDC Cycle – Different phases of SLDC

- Phase 1: Requirement collection and analysis
- Phase 2: A feasibility study
- Phase 3: Design
- Phase 4: Coding
- Phase 5: Testing
- Phase 6: Installation/Deployment
- Phase 7: Maintenance

System Architecture :



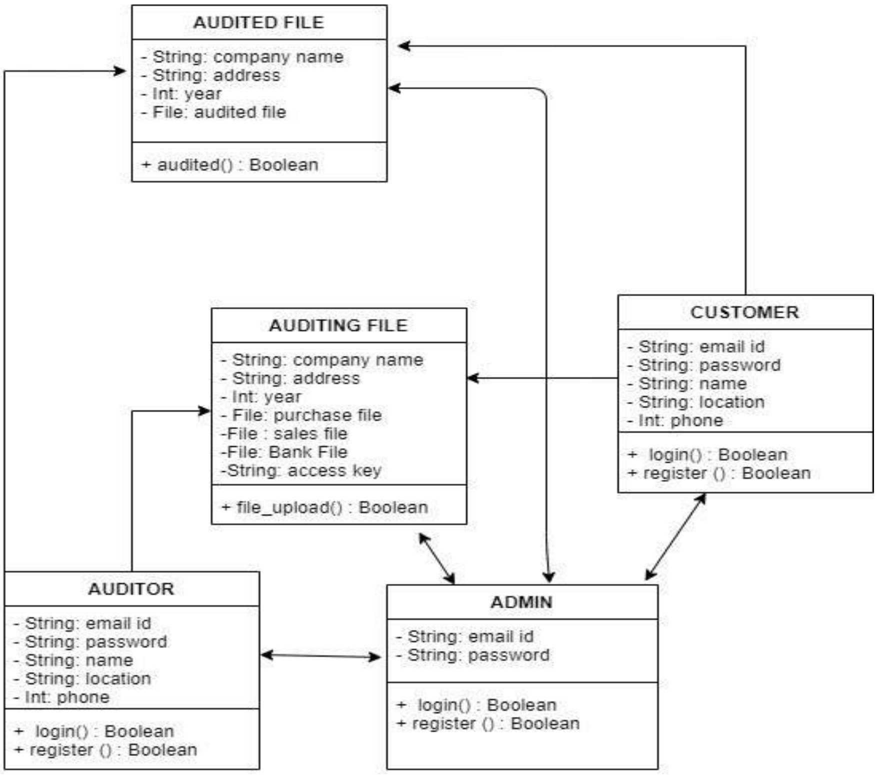
II. SECURE COMPUTING/CYBERSECURITY

A security system identifies and mitigates the system vulnerabilities, by either removing them or restricting access to them, to a very small group. The competition between inventing new security measures to protect data and inventing hacking techniques in conjunction with discovering and leveraging pre-existing vulnerabilities is infinite. Therefore, securing data and resources is becoming more and more challenging day by day. Nevertheless, there exist several different techniques to secure the data being transferred over a network and also that on a user machine. Specializes in securing data in motion through the use of the patented REAL-ID-based mutual authentication scheme. SSL is one such tool to secure data sent over a network, using ciphertext. Using SSL data is kept confidential and message integrity is maintained.

However, recently there have been network security breaches, including the famous "heartbleed" bug. But, the question that remains is "what if the user machine itself is hacked? .it can be used to ensure that the end-user is secured as well as the tunnel. It also uses techniques of authentication to assure each end-user that it is communicating with an authorized user and not a fake one. Such security measures are used to secure data in motion, meaning data that has been shared between computers. They may prove to be of minimum value if the operating system on which it resides is compromised. It is, therefore, crucial to understand and remove the security flaws in the operating system itself. We, on the other hand, are trying to secure data at rest, by coming up with various approaches, one of which is application whitelisting.

Hardening is a technique to reduce vulnerabilities of the existing operating system. It aims to eliminate security risks in an operating system. This is done by turning off all those services of the operating system which are not used are risky and allowing only those which are secure for user's data. Thus, this environment becomes a kind of locked down or reduced version of a fully-fledged operating system. Operating system hardening is a technique that allows us security on the machine level. A hardened operating system can be considered as a smaller version of an otherwise compromised operating system. Secondly, we implement a technique called application whitelisting. It is the technique of preparing a list of all applications that are safe to execute. All applications that are excluded from this list are disallowed to spawn.

Class Diagram:



III. ADVANCED ENCRYPTION STANDARD

AES is an iterative rather than Feistel cipher. It is based on a 'substitution–permutation network'. The Advanced Encryption Standard (AES) is an encryption algorithm that was selected by the National Institute of Standards and Technology (NIST) for the United States government, commercial, and private organizations to use for securing sensitive unclassified information. It comprises a series of linked operations, some of which involve replacing inputs with specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

IV. EXISTING SYSTEM

In the existing system, for the purpose of ensuring data confidentiality, they are usually encrypted before being outsourced. Traditional encryption will inevitably result in multiple different ciphertexts produced from the same plaintext by different users' secret keys, which hinders data duplication.

Convergent encryption makes deduplication possible since it naturally encrypts the same plaintexts into the same ciphertexts. One attendant problem is how to reliably and effectively manage a huge number of convergent keys. Several deduplication schemes have been proposed to deal with the convergent key management problem. However, they either need to introduce key management servers or require interaction between data owners. Within audit, the current technology inflection point may represent the biggest opportunity to date: the ability to harness big data to generate insights and drive audit quality. In the past, the amount of data—and the myriad sources from which auditors have traditionally needed to collect, organize, analyze, prepare, and assess this data—has been the critical factor in determining the length and complexity of audits.

Disadvantages of existing system :

- □ Need to manage a huge number of convergent keys.
- □ Tedious to handle keys without key servers.
- □ The running time of IBBE is much longer than that of the proposed methods.
- □ Highly noisy compared to the proposed technique
- □ Data immutability has always been one of the biggest disadvantages of the secure computing.

V. PROPOSED SYSTEM

In the proposed system, we have an Auditing System implemented to maintain the process of securing files and time management. Business owners are struggling to get their accounts to be audited by the expertise as there is a chance of data breach which leads to catastrophe. Traditional encryption will inevitably result in multiple different ciphertexts produced from the same plaintext by different users' secret keys, which hinders data duplication. The proposed technique has AES CBC mode has been implemented to encrypt data in files for high-security purposes. When customers upload files, the encryption process is started, here a 128 bits key was used to encrypt data. For converting the access key to a 128-bit key, the base64 encoder was proposed. In that file, data was split into blocks of data, each block is encrypted by a different initialization vector. Auditors request the key from the customer to decrypt the file sent by them, auditors revert files to customers then customers can decrypt the file using the key from their default settings. Our approach has proved that our application effectively secures customer auditors file transactions and creates a secure environment for the highly delicate data transmission between two or more parties.

Advantages of proposed system :

- Secure computing creates trust between different entities where trust is either nonexistent or unproven
- Our encryption algorithm creates an unalterable record of transactions with end-to-end encryption, which shuts out fraud and unauthorized activity.
- The proposed approaches have a superior speed advantage.
- No practical cryptanalytic attacks against AES have been discovered.
- Accuracy has improved compared to the existing traditional encryption method.

VI. HARDWARE AND SOFTWARE REQUIREMENTS

HARDWARE REQUIREMENTS:

✔Processor: Intel (R) Pentium (R)
✔Speed: 1.6 GHz and Above
✔RAM: 4 GB and Above
✔Hard Disk: 120 GB
✔Monitor : 15'' LED SVGA
✔Input Devices: Keyboard, Mouse

SOFTWARE REQUIREMENTS:

✔ Operating system	: Windows 7 / 8 / 8.1 / 10.
✔ Coding Language	: PYTHON.
✔ IDE	: Pycharm .
✔ Database	: MySQL

VII. CONCLUSION AND FUTURE SCOPE

The proposed approaches show not only good encryption performance but privacy has improved compared to existing. Here the application uses test data. In the future, we will launch the system to real-world applications. We show experimentally that the approach has robust security for highly confidential documents between businesses or any. In future studies, we intend to extend the proposed approaches to a wider range of applications to further demonstrate their feasibility for practical use. With secure computing implementation, sectors like trade finance witnessed reduced processing time, eliminated paperwork, and became cost-efficient while maintaining security and trust.

REFERENCES

[1]. Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002.Proceedings. The IEEE International Conference on (pp. 277-285).

[2]. Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

[3]. Yenuguvanilanka, J., & Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp.222-225).

[4]. Gaj, K., & Chodowiec, P. (2001, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.

Web Link:-

1. www.en.wikipedia.org
2. www.infosci.cornell.edu/
3. www.ischools.org