TRANSFER OF SECURE FILES USING ADVANCED ENCRYPTION STANDARD

Dr.J.Jebathangam$_2$, Associate Professor,VISTAS.Email:jthangam.scs@velsuniv.ac.in

Dr.K.Kasturi$_3$ Associate Professor,VISTAS.Email:kasturi.scs@velsuniv.ac.in

K.GURU MSC IT, VISTAS

ABSTRACT:

. Most of the files on the web platform are unprotected. The data is gathered and encrypted by this model. By using a user-defined access key, the file was encrypted. The AES algorithm is a symmetric-key algorithm, which means that the data is encrypted and decrypted using the same key. The AES block cypher mode known as CBC (short for cipher-block chaining) outperforms the ECB mode at disguising patterns in plaintext. CBC mode does this by XORing the initialization vector with the first plaintext block (B1) before encrypting it. Block chaining is also a part of CBC because each new plaintext block is XORed with the previous block's ciphertext. The proposed method uses CBC AES encryption For high-security needs, the CBC mode of AES has been developed to encrypt data in files. Here, data was encrypted using a 128-bit key. The base64 encoder was suggested as a way to transform the access key into a 128-bit key. Data was divided up into chunks in that file. Different initialization vectors (IVs) are used to encrypt each block. The reverse order of the encryption process is used in the decryption of an AES ciphertext. By using AES-CBC, the auditing files have been encrypted. After the user submitted the file, AES-CBC mode was used to encrypt the file's data. Without data decryption, the auditor or user could not download the original file. The access key was needed to decrypt the data. With the aid of an access key, the cipher text will be decoded using AES-CBC mode. Cipher text was divided into data blocks. An initialization vector decrypts the first block of data.

KEYWORDS: AES-CBC mode, initialization vectors, Cipher text

INTRODUCTION:

In information security, where data is encrypted at the sender and decrypted at the receiver, cryptographic methods are crucial. The National Institute of Standards and Technology (NIST) adopted the Advanced Encryption Standard (AES), a symmetric block cypher, in 2001. The block size is the fixed length of plaintext that is processed by a block cypher. The plaintext must be divided into many blocks if its length exceeds the block size. Normally, the plaintext's final block needs to be padded to fit the block size. Formal descriptions of how block encryption on plaintext that is larger than a block size is handled are known as modes of operation. Additionally, they offer required services like sincerity, reliability, and confidentiality.

OBJECTIVE:

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. This model might be applied to site audits

AES-CBC

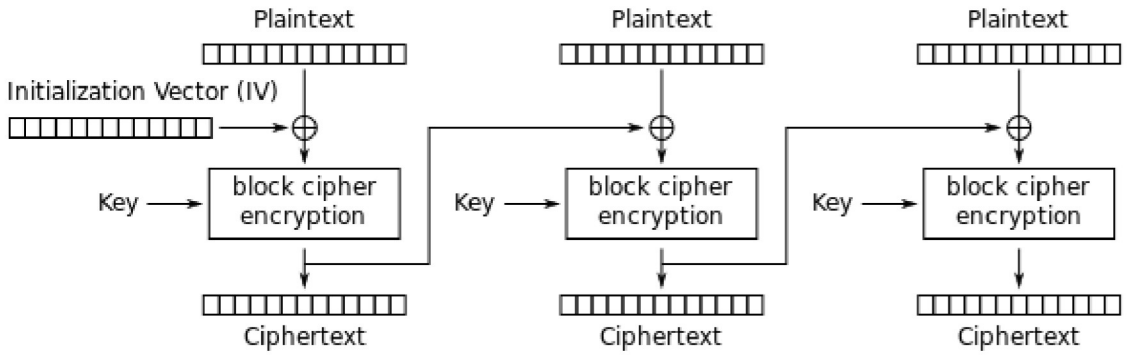
The issue in ECB is resolved by the CBC mode. It lessens the possibility of repeating patterns in the cypher text.

CBC (short for **cipher-block chaining**) is a AES block cipher mode that trumps the ECB mode in hiding away patterns in the plaintext. CBC mode achieves this by XOR-ing the first plaintext block (B_1) 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.

Following are the steps involved in CBC encryption and decryption:

C_i=Ek($P_i \oplus C_i-1$),with C_0=IV [Encryption]

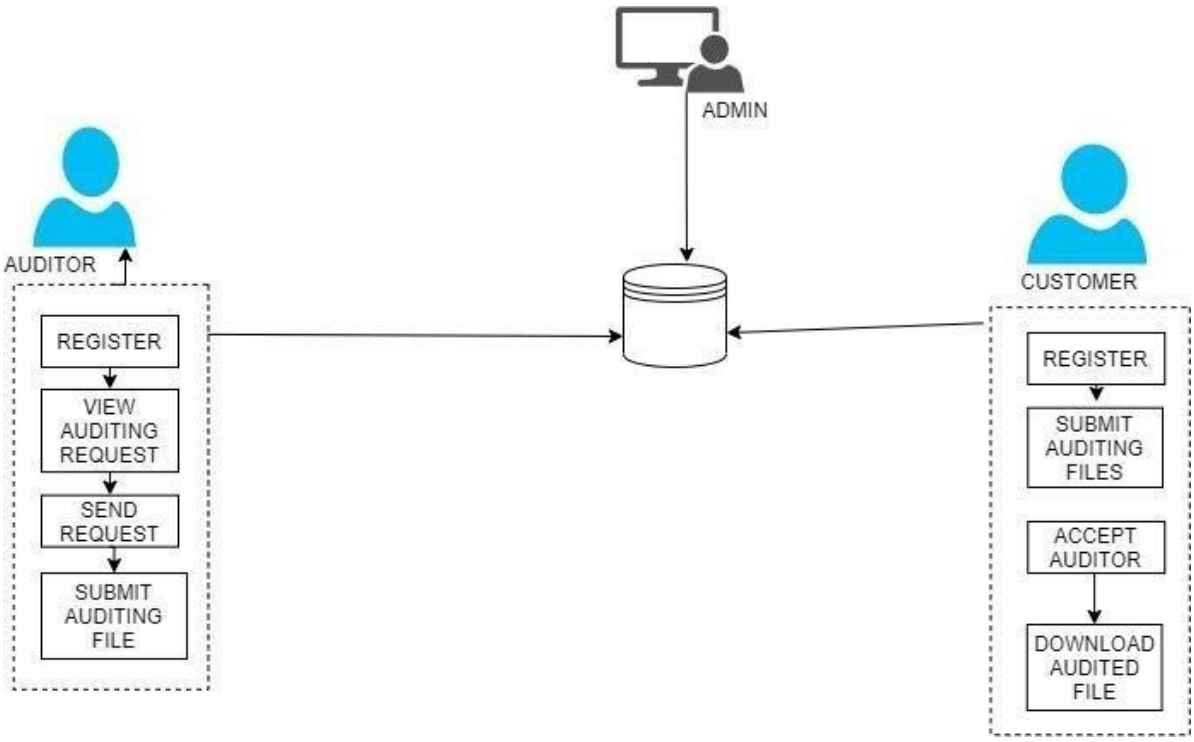
P_i=Dk(Ci)$\oplus C_i-1$,with C_0=IV [Decryption]



Cipher Block Chaining (CBC) mode encryption

This option allows for the more safe handling of large plaintext that may contain repeating patterns . As a result, if the same plaintext is encrypted more than once, the application of IV makes the resulting cypher texts different. Due to its chaining mechanism, CBC mode takes longer to process than ECB mode [8]. To prevent the spread of channel noise errors, CBC can be synchronised . The CBC mode is not advised for disc encryption because, unlike ECB, it does not support parallelism .

SYSTEM ARCHITECTURE:



Module Description:

Modules:

1) Customer

2) Auditor

3) Admin

- Customer:

This module provides information about the customer and auditing details. If the customer is new to the applications, they must register in the application before they can access this application easily. The customer can register details with proper validation, and all the fields will be required for the registration process. The customer can register the company auditing files with proper validation. An accessible key is required before uploading in order to encrypt the file.An accessible key is required before uploading in order to encrypt the data. The auditor sent a request for a password to access the file after viewing the request. The consumer can give permission for the auditor to receive an access password. The audited file can be obtained from the customer once the process is finished.

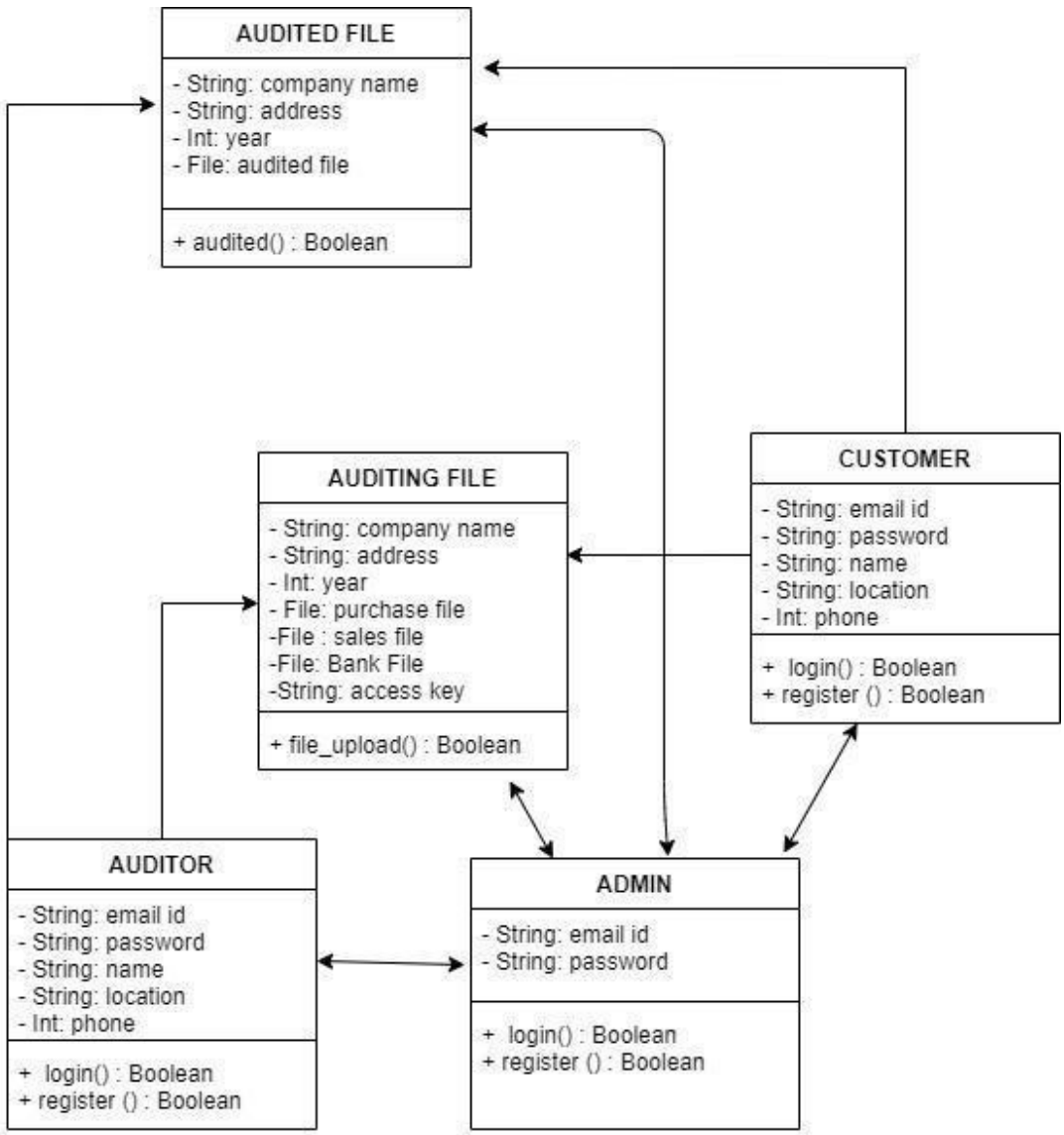
- Auditor:

The comprehensive data and information about the auditors are provided in this module. If the auditor is brand-new to the application, they must register before they may simply access this application. All of the fields must be filled out in order for the auditor to register the information with correct validation. The auditor has access to the client's auditing request and may ask the client for a password. After downloading, the auditor sends a file that has been audited to the client.

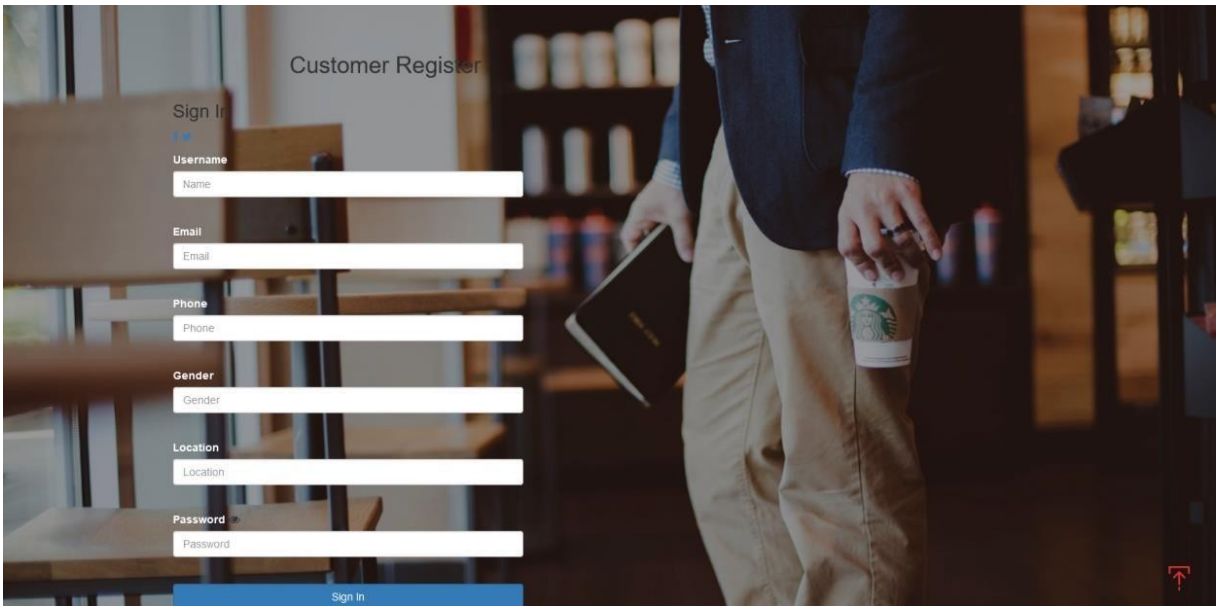
- **ADMIN** :

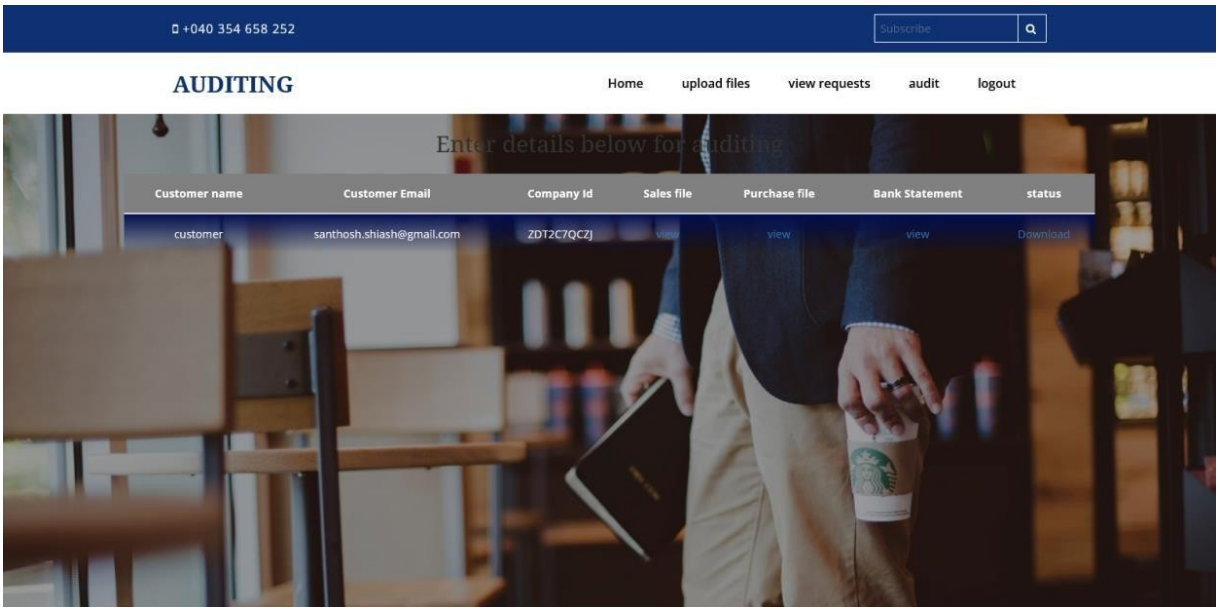
The comprehensive data and information about the auditors are provided in this module. If an auditor is new to an application, they will wish to register once they can access it without difficulty. All of the fields must be filled out in order for the auditor to register the information with correct validation. The administrator can check the list of auditors, the progress of the auditing file process, and the list of clients.

CLASS DIAGRAM



GRAPHICAL USER INTERFACE (GUI)





CONCLUSION:

Internet usage is rapidly increasing nowadays. Exchange of data is massive now a days. Information used in Business are very important and it must be protected against any unauthorized access. Some information is vital and must be safeguarded against unauthorized access. Encryption Technology is used to prevent unauthorized access to original data, Encryption algorithm plays an important role. Many algorithms are used now a days to encrypt the data. In terms of efficiency AES Symmetric Key algorithm which is widely endorsed and implemented, is one of the best algorithms in terms of efficiency. The proposed method is used for secure file transfer by encryption and decryption method using AES. The auditing files have been encrypted by AES-CBC. 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 original file without decryption of data. Decrypting of data was needed the access key. The cipher text will be decrypted by AES-CBC mode with an access key. Cipher text split to block of data. The first block of data is decrypted by an initialization vector. According to the research, AES algorithm provides secured file transfers without the interruption of hackers trying to access the unauthorized data.

REFRENCES

[1] Mahajan, Prerna and Abhishek Sachdeva, 2013. A Study of Encryption Algorithms AES, DES and RSA for security. Global Journal of Computer Science and Technology.

[2]Kumar, L. P., & Gupta, A. K. (2016, May). Implementation of speech encryption and decryption using advanced encryption standard. In *2016 IEEE international conference on recent trends in electronics, information & communication technology (RTEICT)* (pp. 1497-1501). IEEE.

[3]Abomhara, M., Zakaria, O., Khalifa, O. O., Zaidan, A. A., & Zaidan, B. B. (2022). Enhancing selective encryption for H. 264/AVC using advanced encryption standard. *arXiv preprint arXiv:2201.03391*.

[4]Kaur, J., Lamba, S., & Saini, P. (2021, March). Advanced encryption standard: attacks and current research trends. In *2021 international conference on advance computing and innovative technologies in engineering (ICACITE)* (pp. 112-116). IEEE.

[5] Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to

encrypt and decrypt data. *Cryptography and Network Security*, *16*, 1-11.

[6]Prabhakaran, V., & Kulandasamy, A. (2021). Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. *Neural Computing and Applications*, *33*(21), 14459-14479.