International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Security all formats file using hybrid encryption

Varuna Kshirsagar, Purvi Mandlik, Nagare Siddhi, Pacharne Komal

How to Cite this Article:

Kshirsagar, V., Mandlik, P., Siddhi, N. & Komal, P. (2026). Security all formats file using hybrid encryption. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.267

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.

https://doi.org/ 10.55041/ijcope.v2i4.267

Abstract

Data security and encryption is one of the most useful at highly essential aspects of enabling effective security of the data against attacks and intrusions. This is an effective and useful technique that has been evolved significantly over the past few years. For the purpose of encryption the AES was prominently used before. The data encryption standard is highly effective but was prone to encryption failure against brute force attacks that have been highly effective against this encryption standard. Therefore the advanced encryption standard has been used since then to improve the performance of encryption significantly. The advanced encryption standard has been useful and realization of effective security but has been optimized specifically for achieving high throughput and high bandwidth for a variety of implementations. In this methodology we propose an enhancement to the AES encryption approach through the improvement of key generation process through the utilization of the genetic algorithm. The effective and useful implementation of genetic algorithm has been significantly useful for improving the performance of the AES encryption con siderably.

Keywords: Data Security, Advanced Encryption Standard (AES), Genetic Algorithm, Key Generation, Cryptography.

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

With the rise information technology and the large amount of information being generated every day there is a need for an effective realization of a secure technique for safeguarding this information effectively. This information age has led to a lot of information explosion which can be addressed as a large number of people have a lot of personally identifiable information about themselves such as bank accounts social media IDs corporate ID is along with various identification documents that need to be secured to prevent them from malpractice. In the event of a data leakage this can be a problematic scenario as it can be highly difficult to prevent any identity theft and other problems that can be significantly dangerous and lead to a lot of complications for the individuals.

There are various techniques that have been utilized for the purpose of securing the data effectively. The traditional techniques have been designed around preventing the access to the data for any random individual. Through this process the data is isolated effectively and any attacker cannot get access to this data due to it being extremely isolated. This technique is not effective for various other documents and information that needs to be shared with other individuals at the same time prevented from misuse. For this purpose the encryption or cryptography is one of the most effective techniques that are utilized for safeguarding for securing the data with great security [1]. The encryption standards or cryptography comes in various flavors according to the implementation and the various characteristics of the data.

1.1.1 WHAT IS AES?

These cryptographic approaches tend to modify the data effectively to prevent any misuse effective identification. Through the cryptographic process are generally identifiable data is converted into random characters through the process of encryption

[2] . Encryption is one of the two most important processes that are performed in cryptography for the purpose of effectively e transforming the representation of data from one structure to another unique structure. This makes it extremely difficult to identify what kind of information or data is there that is encrypted by the attacker, this allows the data to be effectively protected from the malicious users effectively.

But the data also needs to be utilized coherently by the receiver or should be in the readable form for the owner of the data at least. For this purpose a decryption process is performed which effectively transforms the data from its encrypted cipher text into the normal text that was originally utilized for the encryption process [3]. Which is the other and the most important half of the cryptographic process which restore the original data which that can be utilized effectively for whatever purpose the data is being used. This entire approach is formed due to these two main procedures of cryptography and there are a number of different algorithms that are being used for the purpose of achieving this approach.

The data encryption standard was on the first and widely used techniques for the purpose of encryption to

safeguard the data from data leaks. This is highly effective and was utilized for a long time before certain vulnerabilities we noticed in this encryption standard. The data encryption standard was highly susceptible to brute force attacks that could break into such algorithms and arrival the secure cipher text and convert it into the plaintext effectively compromising the data. For this purpose the data encryption standard which is highly uncertain was dropped altogether and a new approach called the advanced encryption standard supported by Rijndael algorithm was utilized [4]. This continues to be the most secure and an industry standard that is being utilized for the purpose of achieving cryptography by the National institute of standards and technology. These are effectively used in implementing cryptography in a lot of different approaches such as service cellular phones from where is firewalls etc.

1.1.2 WHAT IS GENETIC ALGORITHM?

The genetic algorithm is a highly effective and useful algorithm that is designed through inspiration from the Darwin's theory of evolution [5]. The genetic approach implement effective realization of revolutionary mechanism to enable highly effective and useful optimization of entire processes accurately. The genetic algorithm is highly useful as it combines affective theory that governs evolution to achieve highly inter esting results in a number of generations for a lot of different problems [6]. The im plementation of the genetic algorithm is highly diverse and can be useful for achieving improvements significantly that can be used for optimization.

The genetic algorithm employs a number of methodologies to achieve effective optimization through the execution of a wide variety of implementations. The ele ments consisting in the genetic algorithm are extremely useful in achieving this process through the illustration of the evolutionary mechanism [7]. These elements are se lection which is the selection of the most appropriate candidate or individual for the purpose of reproduction.

The selection allows effective candidates for reproduction which are the fittest ones among the lot.

The genetic algorithm also employs crossover mechanism that provides crossovers between two individuals for creating an offspring through reproduction.

This crossover enables useful exchange of information which can create a highly useful and new offspring with unique characteristics.

The genetic algorithm also employs the utilization of mutation which is an arbi trary procedure that changes one of the elements of the genes. This is a highly useful implementation that achieves the reduction in premature convergence which can be a problem in the genetic algorithm.

1.1.3 KEY GENERATION

The key generation approach is one of the most integral parts of the encryption methodologies. The field of cryptography revolves around key generation and effective approaches for the purpose of generating keys in achieving a secure environment for the users. These keys are highly valuable and the generation of these keys determine the level of complexity that is there in the cryptographic technique. This level of complexity e improves the overall security with an improvement in the complexity of the approach. Therefore the key generation is the most vital component that allows for effective and useful improvements in the encryption. There

are a number of different key sizes that are utilized in Advanced Encryption Standard. These keys are divided according to the size vary in a larger size is a lot more effective security than the lower one. But this is not directly proportional as some of the applications require a lower amount of computational power that can be effectively useful for the encryption and decryption purposes therefore a lower size of key is utilized in such applications. Most of these keys are generated through field gate programmable array is which are the physical elements improving the security on a particular device. The key generation process is effectively elaborated in the section given below.

1.1.3.1 TECHNIQUES FOR KEY GENERATION

But there are certain influences that have been significant in achieving the imple mentation of AES as we see today. The AES implementations normally for improving the security of where is implementation concentrates on achieving high throughput. This is due to the fact that most of these implementations do not have extensive computational capabilities to achieve complicated calculations easily. Therefore for this purpose a lot of field gate programmable arrange are used is the can be effectively useful for providing physical security to the devices as well as improve the agility of the algorithm. The height of food is highly useful as it supports incredible security and also realizes a high bandwidth that can be effective for a variety of applications.

1.1.3.2 NEW AND PROPOSED METHOD FOR KEY GENERATION

To achieve considerable improvement in the process of key generation in the Ad vanced Encryption Standard through the effective implementation of the Genetic Algorithm.

1.1.4 LIMITATIONS OF CURRENTLY USED TECHNIQUES

The current techniques for the effective key generation utilize field gate programmable erase for easier implementation and effective realization of this approach. This is done to enable effective improvements in the throughput, which can significantly increase effectiveness of the key generation making them highly secure through the use of physical devices. Wiki generation approaches have also been design to achieve very high bandwidth for the execution of the key generation process. The large bandwidth allows for effective realization of a wide variety of applications that makes it a universal implementation which can be e very useful for different types of applications.

1.2 PROBLEM DEFINATION

To achieve considerable improvement in the process of key generation in the Ad vanced Encryption Standard through the effective implementation of the Genetic Algorithm.

CHAPTER 2
LITERATURE SURVEY

Citation	Author	Title	Methodology	Drawbacks
1	K.Sandyarani, Dr.P.Nirmal Kumar	Design And Analysis Of AES-CM With Non Linearity S-Box Archi tecture	This paper outlines an effec tive technique for the pur pose of enabling Advanced Encryption Standard in the satellites for eas ier and safer encryptions of the data being transmitted. The data being transported from the satellite is highly valuable and confidential.	No Drawback is noticed in the overall eval uation of this research article.
2	Fang Rao, Jianjun Tan	Energy Con sumption Research of AES En cryption Algorithm in ZIGBEE	This paper discusses the consumption of energy and the effective utilization of encryption protocols in de vices with limited power. The authors state that an effective energy efficient technique needs to be imple mented for the purpose of achieving encryption on the ZigBee network. For this purpose and AES algorithm has been revised and an ef fective encryption has been achieved on limited energy consumption.	The main draw back is that this technique has been performed in a simulated environment.
3	Sandhya Koteshwara, Amitabh Dasy and Keshab K. Parhi	Performance Comparison of AES GCM-SIV and AES GCM Al gorithms for Au	This research article the authors have elaborated on the topic of authenticated encryption that effectively maintains the integrity of the the shared message along with the confiden tiality intact. They have been various approaches that have been utilised to achieve this	The main draw back is that the technique has not achieved significant im provement over the conventional approaches.

		thenticated Encryption on FPGA Platforms	technique but most of them have not been as effective in their imple mentation. Therefore to improve this the authors of proposed utilisation of ad vanced encryption standard along with issuance resis tance for achieving effective authenticated encryption that can be applicable on FPGA platforms.	
4	Ritambhara, Alka Gupta, Manjit Jaiswal	An Enhanced AES Algo rithm Using Cascading Method On 400 Bits Key Size Used In Enhancing The Safety Of Next Genera tion Internet Of Things (IOT)	In this paper the authors discuss about encryption standards that are being utilized for securing the data and transferring. This is due to the fact that in this information is there is an increase in the amount of data that is being gen erated and shared with one another over vast networks. Therefore for this purpose the authors have propose an enhanced algorithm for implementing advanced en cryption standard that uti lizes cascading method for securing internet of things devices.	The main limita tion of this ap proach is the in creased key size due to the cas cading effect.
5	Chong Hee KIM	Differential Fault Anal ysis against AES-192 and AES-256 with Minimal Faults	In this publication the au thors have propose the framework of encryption through advanced encryp tion standard. The ears is being used extensively for the purpose of achieving all round security and protec tion of the data. But there is a lack of effective analysis of differential fault in AES 256 and AES 192. There fore this research article fo cuses on achieving the min	The main lim itation of this approach is that the system requires a min imum of three pairs for achiev ing the secret key of the 256 bit advanced encryption standard.

			imal faults in the advanced encryption standard imple mentation.	
6	No´emieFloissacand Yann L'Hyver	From AES 128 to AES 192 and AES 256, How to Adapt Differential Fault Analysis Attacks on KeyExpansion	The advanced encryption standard has been effec tively elaborated for the purpose of identifying the differential fault and effec tively analysing it from an attack point of view. The authors have attack the AES encryption standard through injection of faults and analysis of the same ex tensively.	No Drawback is noticed in the overall eval uation of this research article.
7	Feng-Hsiag Hsiao, Guang-Wei Liou	Application of Advanced Encryption Standard to Chaotic Synchroniza tion Systems: Using an Improved Genetic Al gorithm as Auxiliary	The advanced encryption standard has been analyzed in this research article for the purpose of improving the efficiency and imple mentation in chaotic syn chronization systems. This type of systems are not as effective for advanced en cryption standard therefore the authors have improved this approach through the utilization of an auxiliary consisting of the genetic al gorithm.	The main lim itation of this approach is the increased computational complexity that is observed.
8	Aura Conci, Andre Luiz Brazil, Si mone Ba cellar Leal Ferreira and Trueman	AES Cryp tography in Color Image Steganography by Genetic	The authors in this ap proach have analyzed steganography techniques on color images through the utilization of the advanced encryption standard. The advanced encryption stan dard is highly difficult to achieve cryptography in the images therefore the authors	No Drawback is noticed in the overall eval uation of this research article.

	MacHenri	Algorithms	and proposed the utilization of the genetic algorithm to achieve the goal.	
9	Rodrigo S. Semente, Andr´es O. Salazar, Fe lipe D.M. Oliveira	CRYSEED: An Au tomatic 8-bit Cryp tographic Algorithm Developed with Genetic Programming	The authors in this paper have analyzed a large num ber of encryption techniques for the purpose of imple mentation in constant en vironments such as wire less sensor networks. Most of the approaches have not been able to effec tively achieve security as well as maintain the effi ciency of the low power sys tems in the wireless sensor networks. The effort to im prove this the authors of proposed the implementa tion of genetic programming for achieving a highly effi cient cryptography for wire less sensor networks.	The main limita tion of this pro cess is the lack of effective analysis of the proposed technique.
10	Avinash Ray, Anjali Potnis, Prashant Dwivedy, Shahbaz Soofi, UdayB hade	Comparative Study of AES, RSA, Genetic, Affine Trans form with XOR Oper ation, And Watermark ing for Image Encryption	In this research article the authors have effectively analyzed the implementa tion of various encryption protocols for the purpose of watermarking and achiev ing image encryption. The authors have compared XOR operation, affine transform, genetic, RSA and AES cryptographic techniques for the study.	The main limita tion of this study is that there has not been any ef fective technique that has been proposed in this approach.

11	Takeshi Tsujimura, Takahiro Hashimoto, and Kiyotaka Izumi	Genetic Rea soning for Finger Sign Identifica tion Based on Forearm Electromyo gram	This research article deals with the effective collec tion of finger science data through electromyogram sensors for the purpose of gesture detection. The authors have implemented genetic reasoning to iden tify the finger signals accurately through the electromyogram data.	The main lim itation is that the authors have only utilized my oelectric signals from the forum region only.
12	V. Ten, B. Matka rimov,N. Isembergenov	Approach to control of hybrid renewable power system on the basis of the AE method using a genetic algorithm	The research article in this approach have been ana lyzed for the purpose of implementing a renewable and hybrid power system based on wind, water and solar combinations. The authors and effectively uti lize genetic algorithm to solve the optimization prob lem for achieving additional equilibrium in the hybrid power system.	The main lim itation of this approach is that this approach has not been effectively tested in a real-time environment.
13	K.kalaiselvi, DrAnand Kumar	Enhanced AES Cryp tosystem by using Genetic Algorithm and Neural Network in S-box	This research article de fines an effective approach for the purpose of achieving secure communication and data transfer through the use of cryptography. The authors in this research are proposed an improved AES algorithm through the use of neural networks and ge netic algorithm.	The main lim itation of this approach is that the authors have implemented SP boxes for their timing attack performance.

14	Dr.R.V.Kshirsagar,M.V.Vyawahare	FPGA Implementation of High speed VLSI Architectures for AES Algorithm	In this research article the authors have effectively propose accept or graphics keep for the purpose of achieving secure services for various implementations where low power consumption is required. The photo achieve their goals the authors have implemented very large scale infrastructure along with field programmable gate arrays to achieve advanced encryption standard.	The main draw back of this approach is that the authors can only implement high-throughput through the use of intermediate buffers and partitioning.
15	Thanapol Hong songkiat, Prabhas Chongstitvatana	AES Implementation for RFID Tags: The Hardware and Software Approaches	The researches in this research article have proposed an effective enhancement in the advanced encryption standard for the purpose of being implemented on a CMOS architecture. This implementation has been achieved AES and encryption for RFID tags through the use of appropriate software and hardware.	The main limitation of this approach is that the authors have proposed a change in hardware as well as software of the devices for the purpose of implementation of this approach.

CHAPTER 3

SCOPE OF THE PROJECT

Scope of Securing all format File using Cyber Security is explained below -

3.1 File-Level Encryption System

The Encrypting File System is a widely used file security mechanism that protects sensitive data by encrypting individual files or folders. It uses symmetric encryption to convert plaintext into ciphertext, ensuring that only authorized users with the correct decryption key can access the data. The system generates a File Encryption Key (FEK), which is further protected using public-key cryptography for enhanced security. It works transparently within the operating system, allowing users to access encrypted files without manual decryption. EFS also supports secure backup by keeping files encrypted during storage or transfer. However, if the private key is lost, data recovery becomes difficult. It is mainly used in Windows environments for protecting confidential files. This system ensures confidentiality and prevents unauthorized access even if the file is stolen.

References url : https://en.wikipedia.org/wiki/Encrypting_File_System

3.2 Intrusion Detection System (IDS) with Encryption

An Intrusion Detection System is an existing security system that monitors network or system activities to detect unauthorized access and protect sensitive files. It continuously analyzes incoming and outgoing traffic to identify suspicious patterns or malicious behavior. When an intrusion is detected, the system generates alerts for administrators to take immediate action. IDS can be combined with encryption techniques to secure data during transmission and storage, ensuring both confidentiality and integrity. It uses signature-based and anomaly-based detection methods to identify known and unknown attacks. IDS plays a crucial role in preventing data breaches and cyber-attacks such as malware and unauthorized file access. However, it may struggle with detecting new attack patterns and can generate false positives. Overall, it enhances file security by providing real-time monitoring and threat detection.

References url : https://www.geeksforgeeks.org/ethical-hacking/intrusion-detection-system-ids/

CHAPTER 4
METHODOLOGY

The methodology for Securing all format file is developed under waterfall model architecture as shown in the below figure 1.

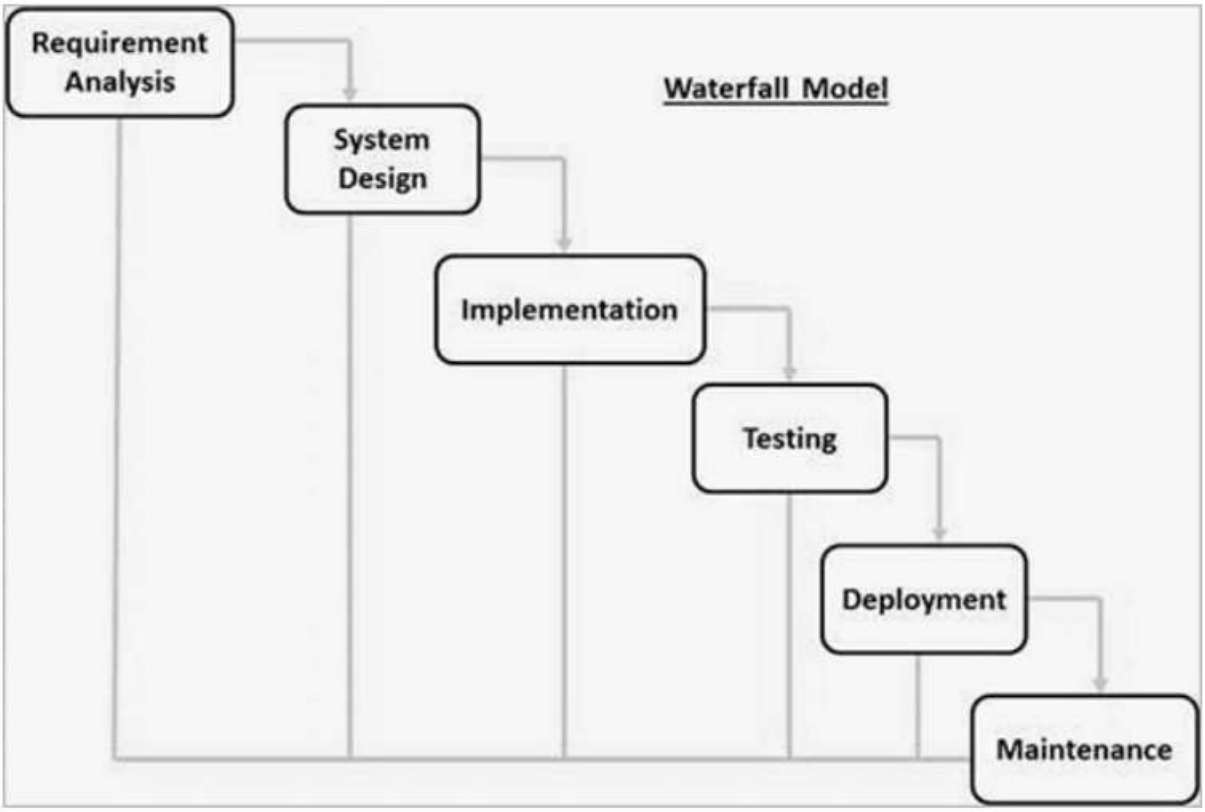


Fig 1 : Water fall model Architecture

The sequence phases in water fall model according to our project are mentioned below.

4.1 Requirement Analysis – Here requirement analysis are done based on following points

- ✓ Base paper for Securing all format file
- ✓ Studying on Cyber security
- ✓ Knowledge on Encryption models

4.2 System Design: The System of Securing all format file is designed by using the following hardware and software.

Minimum Hardware Specification:

- CPU : core i5
- RAM : 8 GB
- HDD : 500 GB

Software Specification:

- Coding Language : Java
- Development Kit : JDK 1.8
- Frontend : Swing Framework
- Development IDE : Netbeans 8.2

4.3 Implementation:

Proposed system is designed by using the following modules

Module 1: Data Input & Preprocessing

- The system accepts the file as input and divides it into manageable data blocks.
- Each data block is prepared for encryption by converting it into a suitable binary/byte format.
- Initial preprocessing ensures uniform structure for further cryptographic operations.

Module 2: AES Encryption Process

- Byte Substitution is applied using S-box transformation to enhance confusion in data.
- Row Shifting and Mix Columns operations are performed to provide diffusion across the data blocks.
- Add Round Key step combines the data with generated keys to produce encrypted intermediate output.

Module 3: Genetic Algorithm-based Key Generation

- Initial keys are generated using parameters like date and time instance for randomness.
- Genetic operations such as crossover are applied to create new key combinations.
- Mutation and selection processes optimize the key strength for improved security.

Module 4: Final Encryption & Output

- The optimized key is integrated into the AES rounds for final encryption.
- Multiple rounds of transformation ensure high security and resistance to attacks.
- The final encrypted data is generated and stored securely as output.

4.5 Deployment of the system:

The developed software is deployed in the laptop of above mentioned configuration with the help of the mentioned software.

4.6 Maintenance of the system:

As this software is tested for the quick recovery, so maintenance of the system is not a challenging task. This is because the tools and the software used are open source, so there is no question of licensing the required software.

CHAPTER 5

DETAILS OF DESIGN, WORKING AND PROCESSES

5.1 DETAILS OF DESIGN

5.1.1 Data Flow Diagrams

5.1.1.1 DFD level 0

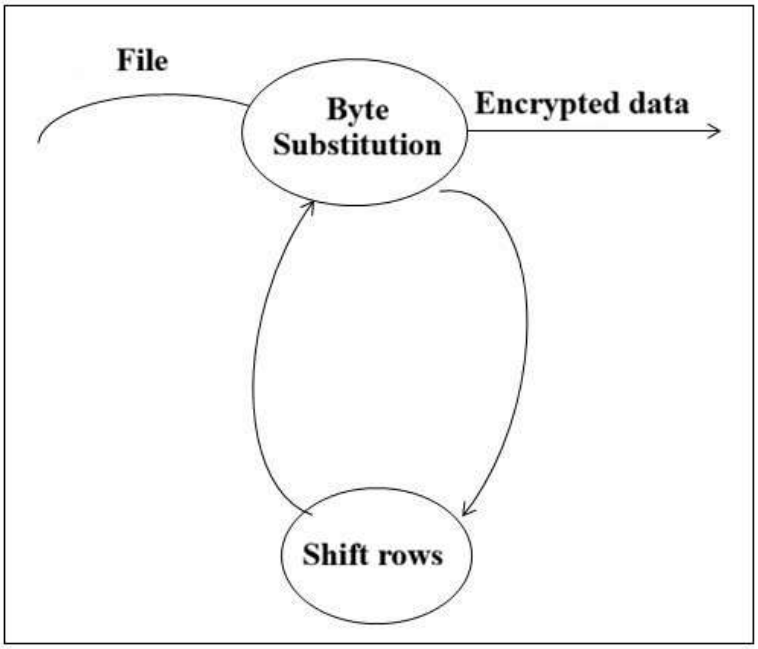


Fig 2 DFD level 0

A level 0 data flow diagram (DFD), also known as a context diagram, shows a data system as a whole and emphasizes the way it interacts with external entities.

5.1.1.2 DFD level 1

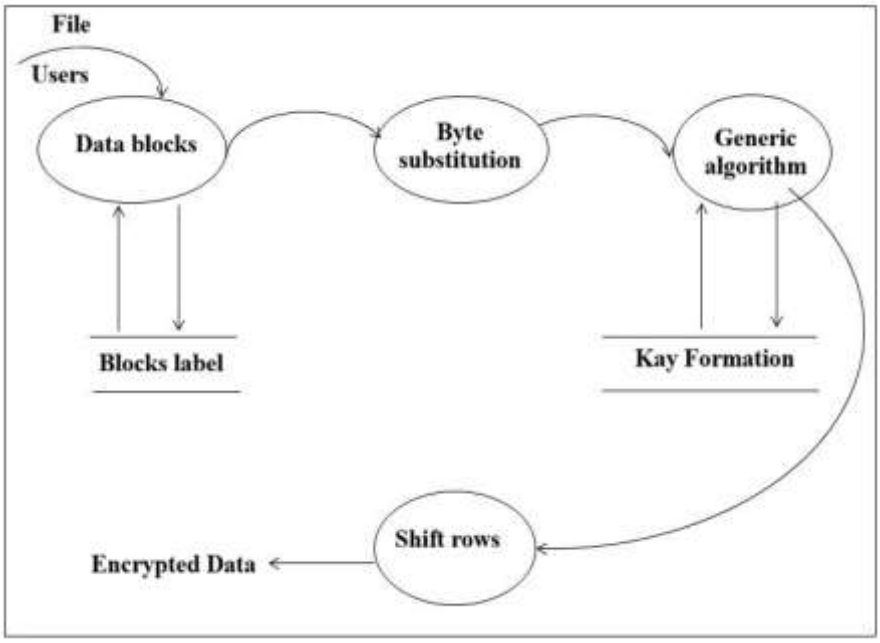


Fig 3 DFD level 1

A level 1 DFD notates each of the main sub-processes that together form the complete system

5.1.1.3 DFD level 2

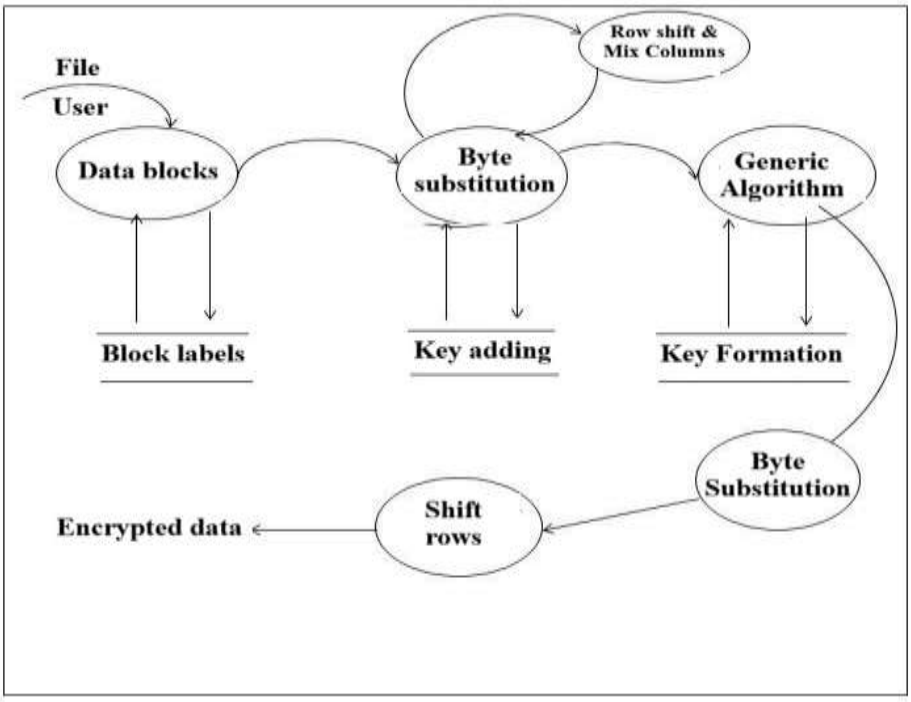
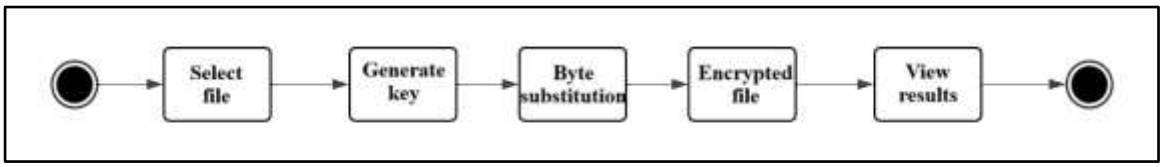


Fig 4 DFD level 2

A level 2 data flow diagram (DFD) offers a more detailed look at the processes that make up an information system than a level 1 DFD does. It can be used to plan or record the specific makeup of a system.



5.1.2Activity Diagram

Fig 5: Activity Diagram

This diagram displays the various activities that are performed in the methodology and its sequence in the system.

5.1.3 Use case Diagram

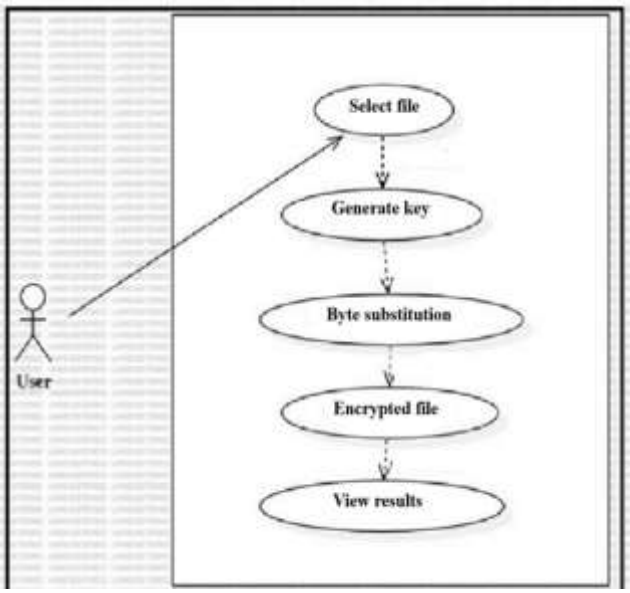
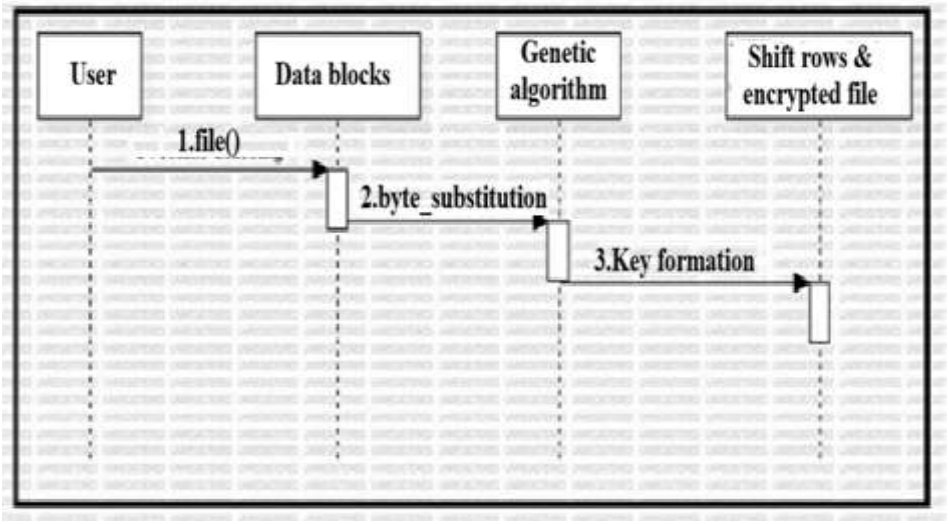


Fig 6: Use case Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved.



5.1.4 Sequence Diagram

Fig 7 Sequence Diagram

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

5.1.5 Component Diagram

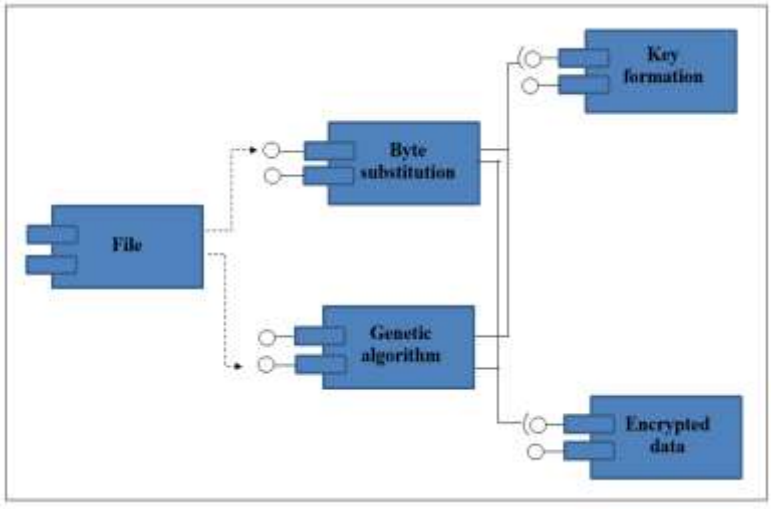


Fig 8 Component Diagram

The component diagram details the various components of the system along with their input and output characteristics.

5.1.6 Deployment Diagram

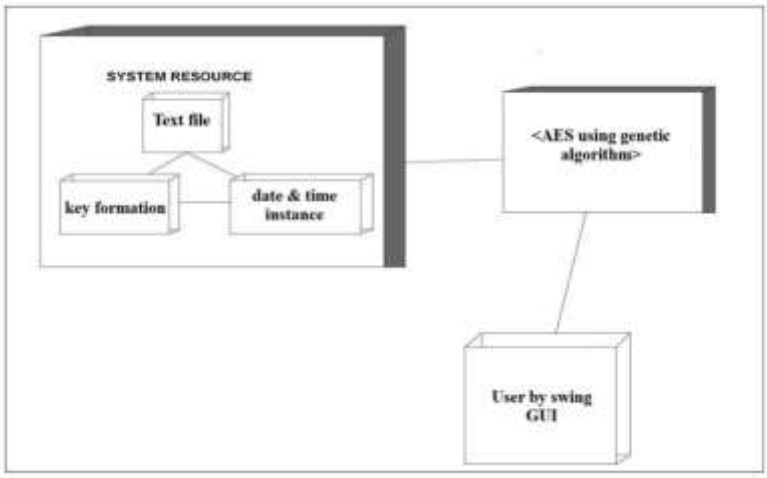


Fig 9 Deployment Diagram

Deployment Diagram is a type of diagram that specifies the physical hardware on which the software system will execute. It also determines how the software is deployed on the underlying hardware.

5.1.7 Package Diagram

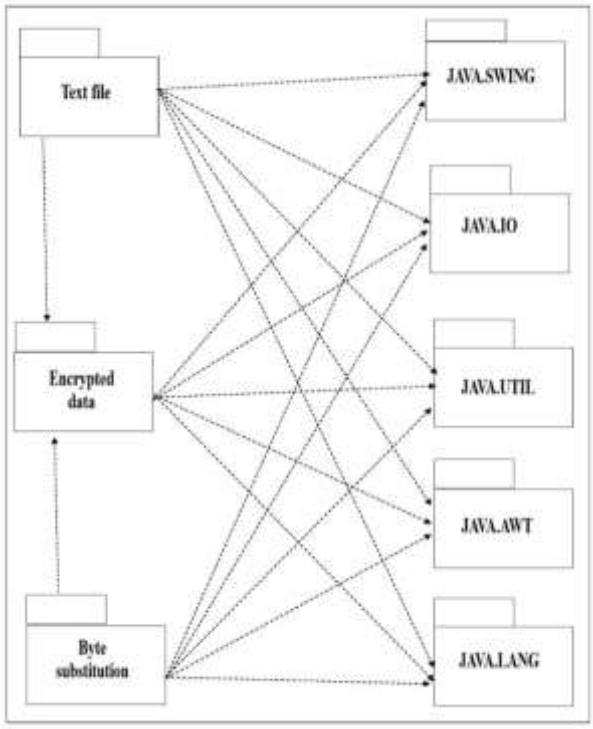
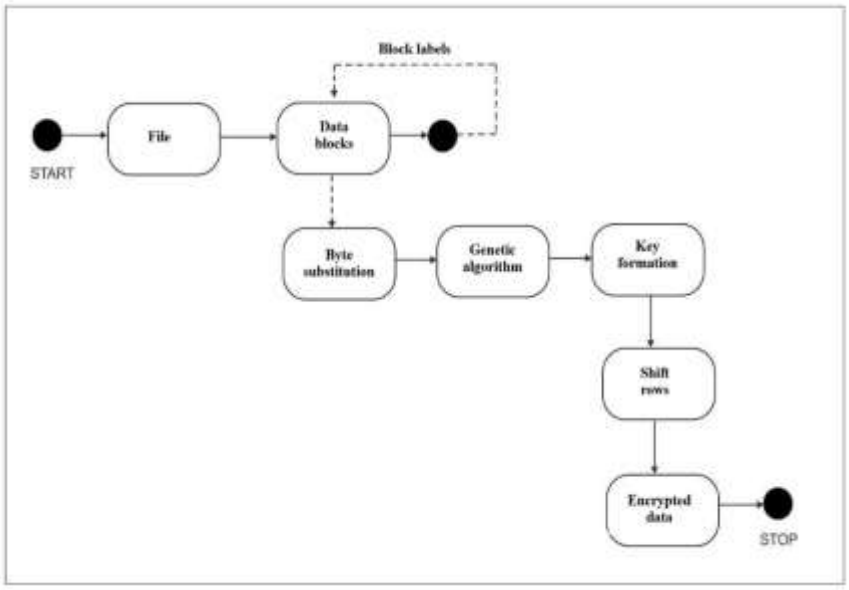


Fig 10 Package Diagram

The package diagram illustrates the various packages that are utilized in the system along with their inter dependencies within the system.



5.1.8 State Transition Diagram

Fig 11: State Transition Diagram

A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction.

5.1.9 Action Plan

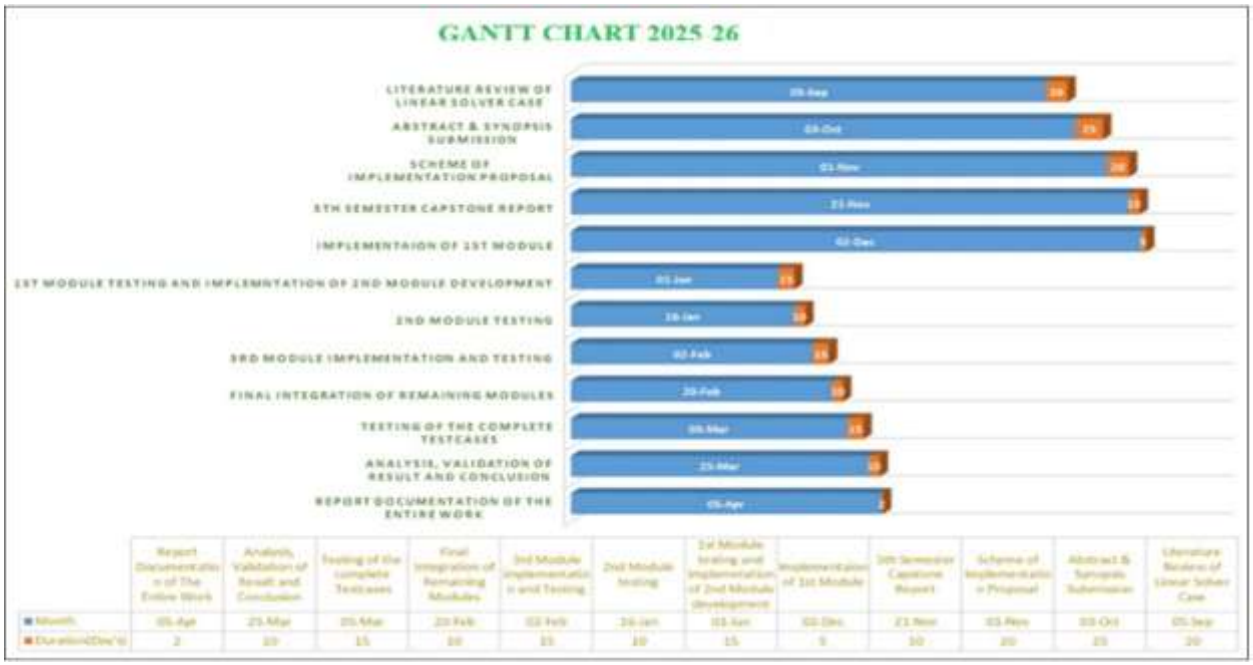
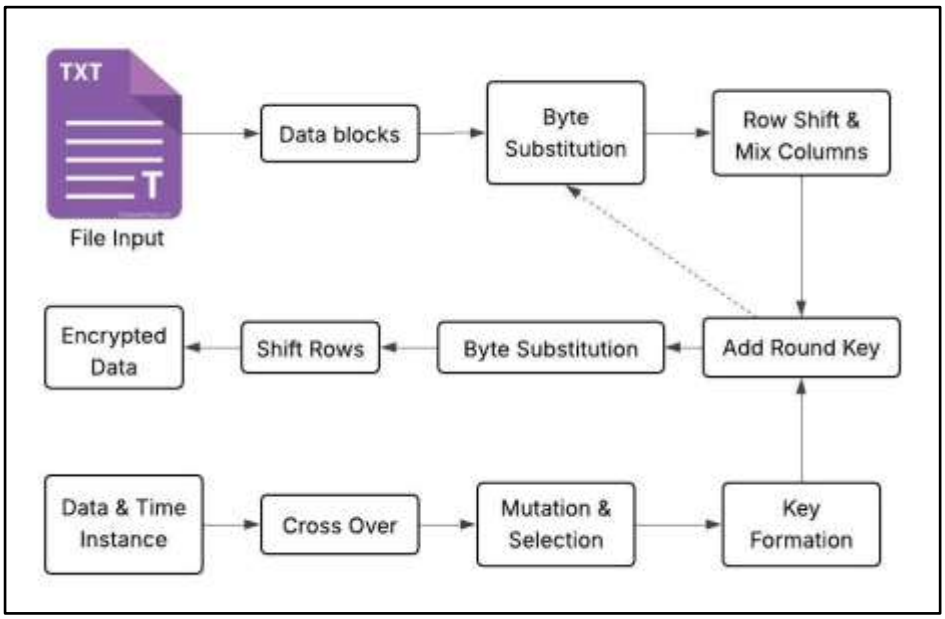


Fig 12: Action Plan



5.2 WORKING AND PROCESSES

Figure 13: System Diagram

The steps that are encountered in implementing of the Advanced Encryption Standard algorithm along with the key generation using the genetic algorithm are depicted in the above figure. And the steps that are included in this process are explained in details with the below mentioned steps.

Step1: Key generation through Genetic Algorithm: To generate a key for encryption using AES algorithm a current time instance is considered as the initial population. This time instance contains date, month,year,hour,minutes second at tributes. These attributes are concatenated into a string and fed to the MD5 hashing algorithm to generate a 32 character hash keys. This 32 character hash key is used to cross over to the modulus operation for the required number of key characters.
Based on this crossover a mutation of the key characters is done based on the rotation of the key stored in an array. Then, based on this mutation right fitting key characters are being selected and concatenated to the empty key string assigned at the beginning.This generated key is set the size of 8 characters and is used for the AES encryption process. The key generation model can be depicted in the algorithm 1 as mentioned below

Algorithm 1 :Key Generation through Genetic Algorithm

//Input: $InstancedataandtimeStringDT_{STR}$

//Output: $SecureKeyS_{KEY}$

Function:$KeyGenerator(D_{STR})$

1: Start

2: $S_{KEY} = \emptyset$

3: $HashKeyH_{KEY} = MD5(D_{STR})$

4: $N = H_{KEY} MOD 8$

5: *IfN* < 8, *then*

6: P=N+1

7: *fori* = 0*to*S_{KEY} *length* < 8

8: i=i+P

9: *if i* < H_{KEY} *length, then*

10: $S_KEY = S_KEY + H_KEY [i]$

11: $H_KEY = rotate(H_KEY)$

12: end if

13: else

14: end if

15: else

16: i=0

17: end for

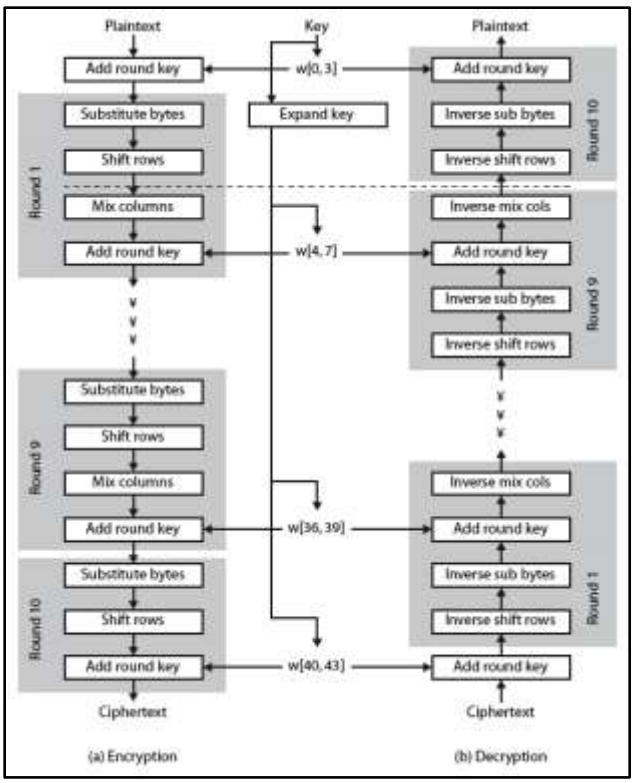
18: end if

19: return S_{KEY}

20: Stop

Step 2: Data Block and Byte Substitution– The fed file is read into the byte array and then, this byte array is divided into blocks of 128 bytes. The last block is padded to equalize the size of the 128 bytes, so that all blocks are maintained equally.These blocks of the bytes are stored in an array to substitute according to the Exclusive OR operation mode. Then this data is framed into a matrix of 4 X 4, which is called state array.

Step 3: Row Shifting and mixing column: Now the obtained state array in the previous step is subjected to shifting of the rows and mixing of the columns for the given number of the rounds. For each of the iterations the key which is generated through genetic algorithm is weaved into the byte substitution process to obtain the tough cipher text.This process of AES structure can be pictorially shown in below figure.



AES Structure

Step 4: Byte Substitution and Shift Rows: This is the last step of the AES Encryption where shifted array after many rounds is subjected to the substitution of the other bytes based on the position and finally the rows are again shifted from the 4 X 4 matrix. After this process all the bytes are concatenated to obtain a single byte array to convert this into a string. The obtained string will cipher text for the given input data.

CHAPTER 6

RESULT AND APPLICATIONS

6.1 RESULTS

PLEASE PUT THE SCREENSHOTS OF YOUR PROJECT HERE AND CONTINUE THE FIGURE NUMBERS

(PUT AS MUCH AS CAN)

6.2 Applications

- ✓ Offices
- ✓ Software Companies
- ✓ Secure text and book sharing

6.3 TEST CASES

6.3.1 Performance Testing:

The system performance is evaluated based on encryption and decryption speed, ensuring efficient processing of large files with minimal delay.

6.3.2 System Testing:

The system is tested with multiple files to verify stability, correctness, and smooth execution of AES encryption with genetic algorithm-based key generation.

6.3.3 Recovery System:

The system can be restored quickly after failure by reinstalling required software and redeploying the application without data loss.

6.3.4 Security Testing

6.3.4.1 Stress Testing:

The system is tested with a high volume of data to ensure it handles maximum load without performance degradation or failure.

6.3.4.2 Unit Testing:

Each module, including AES encryption and genetic key generation, is tested independently to ensure accurate functionality.

6.3.4.3 Black Box Testing:

Inputs and outputs are tested without internal knowledge to verify correct encryption results and system behavior.

6.3.5 Integration Testing:

All modules are combined and tested together to ensure proper interaction and successful secure file encryption and decryption.

6.3.6 Test Cases for the User

ID	TEST CASE	INPUT	PASS CRITERIA
ENC_PROC	File Encryption Process	Input File	File is successfully encrypted using AES algorithm
KEY_GEN	Key Generation (GA)	Initial Parameters	Strong optimized key is generated correctly
DEC_PROC	File Decryption Process	Encrypted File	Original file is accurately retrieved
SYS_SEC	System Security Check	Multiple Files/Data	System prevents unauthorized access and attacks

Table 6.1: Test Cases

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

The proposed system for securing all format files using Cyber Security techniques provides a reliable and efficient solution for protecting sensitive data. By integrating Advanced Encryption Standard (AES) with Genetic Algorithm-based key generation, the system enhances the strength and randomness of encryption keys. This approach significantly improves resistance against brute force and unauthorized access attacks. The use of optimized key generation ensures better performance without compromising security. The system effectively encrypts and decrypts files while maintaining data integrity and confidentiality. Testing results demonstrate that the system performs well under various conditions, including large data inputs. It also ensures quick recovery and stable operation in case of failures. The modular design makes the system scalable and easy to maintain. Overall, the proposed method offers a robust, secure, and efficient framework for file protection in modern cyber environments.

Future Work

Future work can focus on integrating blockchain for enhanced data integrity and adding multi-factor authentication to further strengthen file security. The system can also be extended to support cloud-based secure storage and real-time threat detection using AI.

CHAPTER 8

APPENDIX

8.1 Security for all format file through Hybrid Encryption using Cyber Security

- ✓ https://www.geeksforgeeks.org/client-server-model/
- ✓ https://www.britannica.com/technology/client-server-architecture
- ✓ https://cio-wiki.org/wiki/Client_Server_Architecture
- ✓ https://www.techopedia.com/definition/27669/windows-file-protection-wfp
- ✓ https://www.datto.com/products/file-protection/
- ✓ https://en.wikipedia.org/wiki/Windows_File_Protection

CHAPTER 9

REFERNCES AND BIBLIOGRAPHY

1. K. Sandyarani and P. N. Kumar, ”Design and analysis of AES-CM with non linearity S-box architecture,” 2013 International Conference on Current Trends in Engineering and Technology (ICCTET), 2013, pp. 252-254, doi: 10.1109/IC CTET.2013.6675960.
2. Fang Rao and Jianjun Tan, ”Energy consumption research of AES encryption al gorithm in ZigBee,” International Conference on Cyberspace Technology (CCT 2014), 2014, pp. 1-6, doi: 10.1049/cp.2014.1330.
3. S. Koteshwara, A. Das and K. K. Parhi, ”Performance comparison of AES GCM-SIV and AES-GCM algorithms for authenticated encryption on FPGA platforms,” 2017 51st Asilomar Conference on Signals, Systems, and Computers, 2017, pp. 1331-1336, doi: 10.1109/ACSSC.2017.8335570.
4. Ritambhara, A. Gupta and M. Jaiswal, ”An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT),” 2017 International Conference on Com puting, Communication and Automation (ICCCA), 2017, pp. 422-427, doi: 10.1109/CCAA.2017.8229877.
5. C. H. Kim, ”Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults,” 2010 Workshop on Fault Diagnosis and Tolerance in Cryptog raphy, 2010, pp. 3-9, doi: 10.1109/FDTC.2010.10.
6. N. Floissac and Y. L’Hyver, ”From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key Expansion,” 2011 Work shop on Fault Diagnosis and Tolerance in Cryptography, 2011, pp. 43-53, doi: 10.1109/FDTC.2011.15.
7. F. Hsiao and G. Liou, ”Application of Advanced Encryption Standard to Chaotic Synchronization Systems: Using an Improved Genetic Algorithm as Auxiliary,” 2014 International Conference on IT Convergence and Security (ICITCS), 2014, pp. 1-4, doi: 10.1109/ICITCS.2014.7021740.
8. A. Conci, A. L. Brazil, S. B. L. Ferreira and T. MacHenry, ”AES cryptography in color image steganography by genetic algorithms,” 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), 2015, pp. 1-8, doi: 10.1109/AICCSA.2015.7507100.
9. R. S. Semente, A. O. Salazar and F. D. M. Oliveira, ”CRYSEED: An auto matic 8-bit cryptographic algorithm developed with genetic programming,” 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, 2014, pp. 1065-1068, doi: 10.1109/I2MTC.2014.6860905.
10. A. Ray, A. Potnis, P. Dwivedy, S. Soofi and U. Bhade, ”Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption,” 2017 International

Conference on Recent Innovations in Signal processing and Embedded Systems (RISE), 2017, pp. 274-278, doi: 10.1109/RISE.2017.8378166.

11. T. Tsujimura, T. Hashimoto and K. Izumi, ”Genetic reasoning for finger sign identification based on forearm electromyogram,” 2014 International Conference on Applied Electronics, 2014, pp. 297-302, doi: 10.1109/AE.2014.7011724.
12. V. Ten, B. Matkarimov and N. Isembergenov, ”Approach to Control of Hy brid Renewable Power System on the Basis of AE-Method Using Genetic Algo rithm,” 2013 12th International Conference on Machine Learning and Applica tions, 2013, pp. 199-202, doi: 10.1109/ICMLA.2013.123.
13. K. Kalaiselvi and A. Kumar, ”Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box,” 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), 2016, pp. 1-6, doi: 10.1109/ICCTAC.2016.7567340.
14. R. V. Kshirsagar and M. V. Vyawahare, ”FPGA Implementation of High Speed VLSI Architectures for AES Algorithm,” 2012 Fifth International Conference on Emerging Trends in Engineering and Technology, 2012, pp. 239-242, doi: 10.1109/ICETET.2012.53.
15. T. Hongsongkiat and P. Chongstitvatana, ”AES implementation for RFID Tags: The hardware and software approaches,” 2014 International Computer Science and Engineering Conference (ICSEC), 2014, pp. 118-123, doi: 10.1109/IC SEC.2014.6978180.

****