Project Report on

IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

Submitted in partial fulfillment of the requirements of the degree of

Bachelor of Engineering in **Information Technology.**

Submitted by

Raul Dhruva

Akash Salve

Yogesh Sauw

Guided by

Prof. Yogita Ganage

MCT
MANJARA CHARITABLE TRUST
RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI
(Permanently Affiliated to University of Mumbai)
Juhu Versova Link Road, Andheri (West), Mumbai-53

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIVERSITY OF MUMBAI

2019-20

MANJARA CHARITABLE TRUST

RAJIV GANDHI INSTITUTE OF TECHNOLOGY, MUMBAI

(Permanently Affiliated to University of Mumbai)

Juhu Versova Link Road, Andheri (West), Mumbai-53

DEPARTMENT OF INFORMATION TECHNOLOGY

CERTIFICATE

Date: _____

This is to certify that, the project work embodied in this report entitled, *"**IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD**"* submitted by "***Raul Dhruva****bearing Roll No*. 812", "***Akash Salve*** *bearing Roll No*. 851", "***Yogesh Sauw*** *bearing Roll No*. 853" for the award of *Fourth year of Engineering* ***(B.E.)*** degree in the subject of ***Information Technology***, is a work carried out by them under my guidance and supervision within the institute. The work described in this project report is carried out by the concerned students and has not been submitted for the award of any other degree of the University of Mumbai.

Further, it is certify that the students were regular during the academic year 2019-2020 and have worked under the guidance of concerned faculty until the submission of this project work at ***MCT's Rajiv Gandhi Institute of Technology, Mumbai.***

Prof. Yogota Ganage
Project Guide

Prof. Swapnil Gharat
Project Coordinator

Dr. Sunil B. Wankhade
Head of Department

Dr. Sanjay U. Bokade
Principal

CERTIFICATE OF APPROVAL

This project report entitled

IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

Submitted by:

RAUL DHRUVA	***812***
AKASH SALVE	***851***
YOGESH SAUW	***853***

In partial fulfillment of the requirements of the degree of **Bachelor of Engineering** in **Information Technology** is approved.

Internal Examiner

SEAL OF INSTITUTE

External Examiner

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

ROLL NO.	NAME	SIGNATURE
812	RAUL DHRUVA	
851	AKASH SALVE	
853	YOGESH SAUW	

Date:

Place:

Acknowledgement

With all reverence, we take the opportunity to express our deep sense of gratitude and wholehearted indebtedness to our respected guide, **Prof. Swapnil Gharat**, Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai. From the day of conception of this project his active involvement and motivating guidance on day-to-day basis has made it possible for us to complete this challenging work in time.

We would like to express a deep sense of gratitude to our respected **Head of the Department**, **Dr. Sunil B. Wankhade** who went all the way out to help us in all genuine cases during the course of doing this project. We wish to express our sincere thanks to **Dr. Sanjay U. Bokade**, **Principa**l, MCT's Rajiv Gandhi Institute of Technology, Mumbai and would to like to acknowledge specifically for giving guidance, encouragement and inspiration throughout the academics.

We would like to thank all the staff of Information Technology Department who continuously supported and motivated during our work. Also, we would like to thank our colleagues for their continuous support and motivation during the project work. Finally, we would like to express our gratitude to our family for their eternal belief in us. We would not be where we are today without their support and encouragement.

Raul Dhruva

Akash Salve

Yogesh Sauw

Date:

Place:

Abstract

At present, there are various types of cryptographic algorithms providing security to information on networks, but they also have some drawbacks. Many such algorithms are used as sole security solutions when it comes to encrypting data. To overcome the drawbacks of such algorithms, we propose a new hybrid cryptographic algorithm in this project. The algorithm is designed using a combination of two cryptographic algorithms AES and ElGamal. A comparative analysis of experimental results has been done on these encryption algorithms supported various parameters affecting security and efficiency. The aim was to find the performance of AES, ElGamal cryptography algorithms and AES & ElGamal hybrid cryptography algorithm. The performance of the implemented encryption algorithms is evaluated by means of encryption and decryption time and memory usage. To create comparison experiments, for these algorithms special software was developed. The substitute language JavaScript is used for realizing the encryption algorithms in code. This new hybrid cryptographic technique has been designed to decrease encryption and decryption time and increase throughput. It is safer and powerful compared to previous cryptography models and it is used for control systems security. Also, the encrypted data is securely stored in a cloud and decrypted during retrieval to obtain the original plaintext.

Contents

Table of Contents

Chapters	Title of the Chapter/s	Pages
1 1.1 1.2 1.3 1.4 1.5 1.6 1.7 1.8	Introduction • Introduction of the project title • Background of the work • Statement of the problem • Objectives of the work • Purpose of the work • Period and Scope • Significance of the study/work • Limitation of the work	01-05
2 2.1 2.2	Literature Review • Introduction • List of research papers referred in the project work	06-08
3 3.1 3.2 3.3 3.4 3.5 3.6	Methodology • Introduction • Research design • Proposed system • Process flow of work • Functional requirements • Non-functional requirements	09-15
4 4.1 4.2 4.3 4.4 4.5 4.6 4.7	System Design • Introduction • Block diagram of system • Data flow diagram • Use case diagram • Entity relation diagram • Activity diagram • Test design for work	16-21
5 5.1 5.2 5.3 5.4	Implementation • Introduction • Environment setup • Languages used • Developing model	22-24
6 6.1 6.2 6.3 6.4	Data Analysis and Results • Introduction • User Interface of work • Data collection • Results	25-31

7 7.1 7.2 7.3 7.4	Summary, Conclusion, and Future Scope • Summary • Conclusion • Limitations • Recommendation for Further Study	32-33
	References	34

Table of figures

Fig No.	List of figures	Pages
3.1	Process flow diagram	11
3.2	The General idea of Hybrid cryptosystem	13
4.1	Block diagram of the hybrid cryptographic system	16
4.2	DFD Level 0	17
4.3	DFD Level 1	17
4.4	DFD Level 2	18
4.5	User case diagram	19
4.6	ER diagram	19
4.7	Activity diagram	20
6.1	User interface for user input page	25
6.2	User interface for encrypted text page	26
6.3	User interface for stored cipher texts	26
6.4	User interface for viewing original texts	27
6.5	Encryption time (Nanoseconds) for AES, ElGamal and Hybrid algorithms	29
6.6	Decryption time (Nanoseconds) for AES and AES + ElGamal algorithms	30
6.7	Encrypted file size comparison with plaintext size (Kilobytes) for AES, ElGamal and AES & ElGamal algorithms	30

List of tables

Sr. No.	List of tables	Pages
1	Experimental results on AES	27
2	Experimental results on ElGamal	28
3	Experimental results on AES & ELGAMAL Hybrid model	29

Chapter 1

Introduction

1.1 Introduction of the project title

Computer networks and internet applications are evolving rapidly, so data security is the challenging issue of today that touches many areas. Data is essentially a new currency of the modern world. Where it could be used by data analysts to uncover various patterns which could unveil unknown information about the data owner. In day by day operations, people came to various incidents where data was stolen from a large website and corporations by hackers like Facebook exposed the personal information of nearly 50 million users. The breach was the largest in the company's 14-year history. The attackers exploited a feature in Facebook's code to gain access to user accounts and potentially take control of them.

If the world's one of the biggest organizations like Facebook could not guarantee the security of the user's data and also might be responsible for how it handles the user's private information then it becomes very difficult for users to secure their private interest. Nowadays everyone uses the cloud to backup and store the essential data for quick access and added security. But as put above hackers may still get access to this information due to the use of known algorithms whose vulnerabilities are known which makes it easy to target.

Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. To cease unauthorized access to the user data or database, any transmission & storage process must be securely encrypted. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

The proposed new hybrid cryptographic algorithm model employs a mix of two cryptographic algorithms AES and ElGamal for secure data transfer between sender and receiver.

1.2 Background of the work

Implementing a secure encryption system for file transfer on cloud needs a lot of background checks for feasibility and compatibility. Focus mainly being on components or modules like cloud storage, encryption techniques, algorithms used, etc. A Lot of software prerequisites like processing speed, internet connectivity are also major topics for conducting

background work. Hardware requirements being memory storage, CPU, system as a whole on which the project is being implemented.

Background research leads to a successful conclusion on standards that must be used for the normal functioning of the project. Project background also enables the understanding about various technologies and their impact on the project. Interrelations being various modules can be easily determined due to pre-work done. It also leads to a generic prediction of outcome after the implementation. Various results can be predicted based on the standards used.

1.3 Statement of the problem

Unauthorized access to the user's digital assets is the major issue faced in today's world where communications as well as transactions are done online and sometimes are done over insecure mediums which makes the whole process of data transfer vulnerable to attack. Data transfer can be breached by various third-party applications or hackers for their benefit. Another problem that arises from the above issue is data security. According to statistics, more than 40% of data breaches are caused by unauthorized access which includes hackers, third-party apps, etc.

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges are still existing in this technology. Security is the most challenging issue in this technology. Cloud computing has many challenges like privacy and confidentiality of data, data remanence, data integrity, transmission of data and malicious insiders.

Many times cloud providers doesn't even provide data protection in their free services and for having extra security amount has to be paid for subscription. Even though after paying many times cloud provider uses general encryption algorithms which are proved and effective but as they are developed long time ago and has been used for years hackers are known to their vulnerabilities and issues.

Hence in these situations a single algorithm can’t be used for data security. Hence homomorphic algorithms are used. It is an encryption algorithm that provides a remarkable computation facility over encrypted data (cipher text) and returns encrypted results. This algorithm can solve many issues related to security and confidentiality issues.

1.4 Objectives of the work

1. To introduce new hybrid cryptographic algorithm model using combination of two cryptographic algorithms AES and ElGamal.
2. Provide comparison between two symmetric, asymmetric algorithms and new hybrid model in terms of parameters such as encryption time, decryption time, throughput, etc.
3. To show an effectiveness and security of new hybrid model which makes the algorithm strong against vulnerabilities.

1.5 Purpose of the work

Due to issues related to data security leading to unauthorized access, eavesdropping there are several cases reported by organizations and companies related to data security.

Recently, tech giant Facebook had an issue with data security which led to data loss of a lot of users surfing on the platform. In this modern era of booming technology, technology changes, and evolvement data breaching can cause a lot of damage to organizations. Security of data within and outside the organization has become a necessity.

Having a secure system for data transfer in place can avoid a lot of problems later on in an organization. Our focus or motivation remains by developing a smooth secure encrypted system through which all the employees can transfer critical data without having a risk of breach.

1.6 Period and Scope

The project period and scope being designed for the proposed work is as follows:

1. Project phase/ period: -

Through the time span of project development for simplicity and management reasons the project is divided into four phases:

1. Project initiation: In this phase project conceptualization and initiation is done. Preliminary investigation, literature review and feasibility study are done at this phase. Project charter and initial plan are the products of this phase.
2. Project Planning: In this phase goals and objectives of the project are identified and further refined if necessary. In this phase scope, work distribution, SDLC model, Core components etc. of the project are defined.

3. Project Design & Execution: The project is designed according to the defined requirements and checked repeatedly throughout SDLC for ensuring precise deliverables. In this phase project is developed according to a defined SDLC model and required coding knowledge and software resources are acquired. At the end of this phase a working system is obtained which can be further refined after evaluation.
4. Project control: After execution of the system it has to be evaluated to ensure it meets all the requirements and system works as it is supposed to be. To ensure that testing is done on the whole system based on various parameters. After this if any changes are required they are done in the next development iteration.

2. Project Scope: -

The proposed system will need efficient and seamless execution of the whole encryption and decryption process. The basic idea of the project is to combine AES and ElGamal algorithms to build a hybrid system that removes individual drawbacks of both encryption algorithms and also increases the throughput and reduces the encryption and decryption time of the proposed algorithm while improving protection.

The proposed system will only encrypt text for the scope of the project as encrypting images, video & audio would require a significant amount of time and computational energy. Hence it is assumed that this system would be used in situations where only crucial texts and information need to be saved on cloud.

The proposed system can be used in many messaging applications which stores messages on the cloud. It can also be used as an extension for end-to-end encryption of the messages. It can also be used for encrypting data stored on the cloud, especially documents scanned using OCR could be protected in a better way.

1.7 Significance of the work

In many cases, the most valuable asset of a manufacturing organization, besides its people, is its business data. Data assets in the cloud are under constant threats in the form of data breaches, data corruption and destruction, temporary or permanent loss of access, and temporary or permanent loss of data. Any of these issues can have serious consequences since they can cause failure to meet statutory, regulatory, or legal requirements. Cloud computing is about consolidating software and data resources and in this process manufacturing organizations are losing control over those resources.

Cloud security is important for both business and personal users. Everyone wants to know that their information is safe and secure and businesses have legal obligations to keep client data secure, with certain sectors having more stringent rules about data storage.

Hackers usually gain access to the cloud through packet sniffing & snooping also from man in the middle & brute force attack. Except for the last one all the remaining methods depend upon the intercepting communication between sender and receiver. Hence the decision was made to develop a cryptographic system that encrypts files before transmission of the file which makes it immune to external interception. And also this file will be encrypted using a hybrid system which increases its security.

1.8 Limitations of the work

Even though the proposed system is designed to provide enhanced security to the data security on cloud, still it has its limitations which are listed below:

- Images, video & audio couldn't be encrypted in the proposed system as it is designed as a proof of concept and also encryption of mentioned file format will require significant memory and computational power.
- Although the system supports text through file but in the final implementation text could only be provided by entering through the text box.
- System is currently developed with a web interface in mind hence while porting code to another platform may require modification in code.
- System is not tested on the actual cloud environment hence any unintentional behaviour cannot be predicted.

Chapter 2

Literature Review

2.1 Introduction

Literature review is examined in the Preliminary investigation and Project scope analysis phase of the project. To create a simulation of the Accident Detection system several books, research paper was studied in detail in Preliminary investigation phase. During this phase the topic was studied by all perception like its simulation and also its implementation in real world was determined. Also, the project cost estimate to implement in the real world was analysed based on three-point cost estimate process, where the cost for the project was categorized into three types which are best case, most realistic and worst case.

2.2 List of research papers referred in the project work

1) Comparative Study of Different Cryptographic Algorithms

Author Name: Baldeep Singh, Maninder Kaur. Navpreet Kaur

Observation: Due to development of network technologies it is easy to send and receive any type of information. The data or information may be related to the banking system, government or military. This confidential information can be leaked or stolen by unauthorized persons. So for this security is an important issue for confidential information. This paper is based on different algorithms used for cryptography and their comparative study. Cryptography uses two types of algorithms; symmetric key algorithm and asymmetric key algorithm.

Conclusion: This paper presents different key algorithms of symmetric and asymmetric like DES, 3DES, AES, RSA, ElGamal and Elliptic curve algorithms. All algorithms have their own pros and cons. AES is symmetric, is more secure and fast, although it needs more processing power. Also in asymmetric, RSA is secure but it use many large keys so its complexity increases that's why they had used ElGamal asymmetric cryptosystem, Elliptic curve replaces ElGamal also but it is new in market and use discrete logarithmic problem[1].

2) AES Design Improvements towards Information Security Considering Scan Attack

Author Name: Liting Yu, Dongrong Zhang, Liang Wu, Shuguo Xie, Donglin Su, Xiaoxiao Wang

Observation: With the rapid development and globalization of the semiconductor industry, data security is becoming a more critical issue for highly confidential devices, especially for cryptography related applications. Advanced Encryption Standard (AES) is widely used for information security. For AES, the most important data are plaintext and keys, which are the targets of attacks. In this paper, AES security vulnerabilities are analysed first. Information leakage would be a major concern for AES. Hence one of the most common types of attacks that could leak information at the AES implementation, inserted into AES and utilizing scan chains in or around AES to extract keys or plaintext, is discussed.

Conclusion: AES encryption is widely applied to various fields for information security. Data security for AES has drawn increasing attention from all aspects. In this paper, one major potential non-destructive AES attack, namely scan-based attack, is discussed. This attack is designed to be hardly detected for existing functional, structural or delay detections [2].

3) Study on Data Security Policy Based On Cloud Storage

Author Name: Diao Zhe, Wang Qinghong, Su Naizheng, Zhang Yuhan

Observation: The purpose of this paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy. Those were combined with the results of existing academic research by analysing the security risks of user data in cloud storage and approaching a subject of the relevant security technology, which was based on the structural characteristics of cloud storage systems.

Conclusion: Cloud storage technology develops very fast, and cloud storage security technology is facing unprecedented challenges. However, cloud storage security is not just a technical issue. It also involves the standardization, management, laws and regulations and other problems. In this paper, a few technical problems of cloud storage security are analysed from the technical point of view. To achieve the security of cloud storage completely academia, industry and government departments need to work together [3].

4) Comparative study of different cryptographic algorithms for data security in cloud computing

Author Name: Pradeep Semwal, Mahesh Kumar Sharma

Observation: Cryptography is a process of converting the user useful information to a form which is insignificant to an unauthorized person so that only authorized persons can access and understands it .For ensuring privacy there are multiple cryptographic algorithms, which is selected as per requirement of user or security specification of the organization. This paper

discusses the comparison of various cryptographic encryption algorithms with respect to its various key features & then later discusses their performance cost based on the some selected key criteria's. Some of the algorithms chosen for the purpose are DES, 3DES, IDEA, CAST128, AES, Blowfish, RSA, ABE & ECC.

Conclusion: After comparing the encryption algorithms on the parameters of encryption time, decryption time, memory usage and Avalanche effect. It can be said that Blowfish is best in terms of memory requirement, whereas RSA has a large memory requirement, so blowfish can fit well in small applications especially in embedded applications & for devices with small memory. As for encryption & decryption time is concerned RSA consumes maximum time as compare to other cryptographic algorithm whereas blowfish has least. The avalanche effect of AES is high, so AES can be preferred for application where privacy and integrity of the message is of top priority.

5) Data Access Security in Cloud Computing: A Review

Author Name: Anagha Markandey, Prajakta Dhamdhere, Yogesh Gajmal

Observation: It is a survey paper where authors are providing a comprehensible view of security through the paper. Cloud computing provides various services to the users. Data storage is one of them. But it is observed that there is a very big problem of data stealing through the internet. More is the problem of data leaking & attacks on the data on clouds. The intention of this paper is to attain data security of cloud storage and to put together an equivalent cloud storage security strategy. These strategies are combined with the outcomes of existing data by considering the security risks & user data on cloud storage & move towards the appropriate security technique, which is based on properties of cloud storage systems.

Conclusion: Cloud computing is a promising and rising innovation for the up and coming age of IT applications. The hindrance and obstacles toward the quick development of cloud computing are data security and protection issues. Decreasing data stockpiling and preparing cost is a compulsory prerequisite of any association, while examination of information and data is dependably the most essential undertakings in every one of the associations for basic leadership [5].

Chapter 3

Methodology

3.1 Introduction

Symmetric (secret key) cryptography systems use the identical cryptographic keys for both plaintext encryption and ciphertext decryption. Typically, with a symmetric key, you'll be able to exchange the key with another trusted participant. The entire security of this method stands on the secrecy of the key. During this way, the key must be kept secret to every participant.

Asymmetric (public key) cryptography is one in every of the important directions of secure data transferring. There are developed forms of public-key encryption systems. Unfortunately, there's significantly fewer developments in publicly key algorithms than in symmetric key algorithms. This can also be results of different key sharing technology. Asymmetric cryptography relies on digital signature functions. Is additionally employed in software tools, like browsers, which require to ascertain secure connection over an insecure network just like the internet or have to validate the digital signature. Digital signature is a mathematical technique providing validation of the authenticity and integrity of a message, software or digital document.

In general, the strength of the cryptosystem can’t be totally ensured. Of course, all cryptography algorithms are developed to supply the best security, but because of the very fact that technology is consistently being developed, security systems are getting less immune to every known or new attack.

3.2 Research Design

- Strength and Weakness of Symmetric Key and Asymmetric Key Cryptographic System:

  One of the strong points of symmetric key cryptography is resistance of the key against Brute Force Attack. The aptitude of a cryptographic system to shield data from attack is named its strength. Of course, the best thanks to attack encrypted messages is solely to try decryption the message with every possible key. Strength depends on various factors, including: the secrecy of the key; the issue of guessing the key or trying out all possible keys (a key search); the issue of reversing the encryption algorithm without knowing the encryption key (breaking the encryption algorithm); lack of back

doors, or other ways by which an encrypted file is decrypted more easily without knowing the key.

The weak side of symmetric key systems is to settle on the correct key. Attacks against encrypted information represent three main categories. Those are: Key search (brute force) attacks; Cryptanalysis; Systems-based attacks.

Through increasing the length of the key, the number of possible permutations is additionally exponentially increased. Meaning following, brute force attack needs more technical resources to attack the system. This type of attack is additionally called key search attack. Key search attacks aren't very effective. If the chosen secret's long enough, a key search attack isn't even possible.

Asymmetric (public key) cryptographic systems use two keys: public keys which can be distributed widely, and personal keys which are known only to the owner. During this encryption system, anyone can encrypt a message using the receiver's public key. The strength of a public key cryptography system relies on the computational effort (work considered cryptography) required to seek out the private key from its paired public key. The biggest weakness of this technique is the number of public keys. Thanks to the increasing number of users, the quantity of shared keys is additionally proportionally increased. So, public key algorithms are easier to attack than symmetric key algorithms for the explanation that the attacker (probably) encompasses a copy of the general public key that was accustomed to encrypt the message.

- Hybrid Cryptosystem :-

Hybrid encryption merges two or more encryption systems. It’s a mix of asymmetric and symmetric encryption to learn from the strengths of every variety of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is taken into account a highly secure form of encryption as long because the public and personal keys are fully secure. A hybrid system is introduced with the subsequent schema: Key encapsulation scheme, which may be a public-key cryptosystem; an information encapsulation scheme, which may be a symmetric-key cryptosystem.

Public key cryptosystems depend on hard mathematical functions. For instance, RSA relies on the sensible difficulty of product factorization by large prime numbers. In hybrid systems for encryption and decryption process is employed fast symmetric

key systems. For key management is employed slower asymmetric algorithms, with strong mathematical functions within the background.

Both symmetric and asymmetric key algorithms have their advantages and drawbacks. Symmetric key algorithms are faster than asymmetric algorithms. The most common requirement is that the secret key must be shared during a secure way. Asymmetric systems provide secure transmission of keys, but this process needs far more time. To enhance this problem is to use the hybrid algorithm, which implies using differing kinds of cryptosystems together.

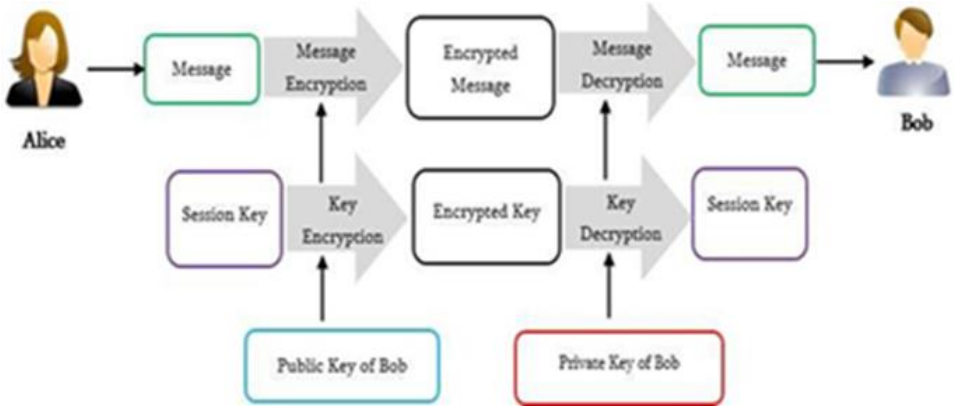

Fig. 3.1 The General idea of Hybrid cryptosystem

The main idea of a hybrid cryptographic system is the generation of random keys for symmetric systems. The next step is to encrypt the key for asymmetric systems. As a result, a secret key obtained that can be used for the encryption of plaintext. During the decryption process first, a private key is used, and then the key is published (Fig. 3.1). In above figure Alice wants to send a message to Bob in a secure way, considering all aspects of security. For that, both sides use a hybrid cryptosystem.

- Advanced Encryption Standard :-

Advanced Encryption Standard (AES) or the same Rijndael is the symmetric key encryption algorithm. For AES there are selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. Algorithms can be judged on their ability to resist attack as compared to other submitted ciphers. Security is considered the most important factor in the competition. Algorithms can be evaluated also with suitability and overall, relative simplicity of implementation in hardware or software.

- El Gamal Cryptography :-

ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange and provides additional security layer by asymmetrically encrypting keys, previously used for symmetric message encryption. The security of this algorithm is based on the Discrete Logarithm Problem. Generally, the ElGamal cryptosystem is used in a hybrid cryptosystem. The plaintext is encrypted with a symmetric cryptosystem and ElGamal is then used to encrypt the key. Asymmetric cryptosystems like ElGamal are usually slower than symmetric ones. It is faster to encrypt the key with ElGamal and the message (which can be randomly large) with a symmetric cipher.

ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm. At first happens key generation process with following steps:

- Alice generates random prime p;
- then is chosen g generator, with following criteria g < p;
- Alice randomly chooses integer x with following criteria 1< x < p;
- Alice computes y = gx mod p ;
- Alice publishes y, g, p and sends them to Bob as public keys. Alice retains x as her private key, which must be kept secret.

The second step of the ElGamal algorithm is encryption of plaintext. After receiving public keys from Alice, Bob starts to encrypt plaintext using those keys with following steps:

- At first user has plaintext M. Bob chooses random prime key k with following criteria 1< k < p – 1;
- than computes a and b numbers whereas, a = gk mod p, and b = yk M mod p;
- Exactly those (a, b) is the encrypted plaintext.

The decryption algorithm works as follows: to decrypt a ciphertext (a, b) is decrypted with private key x. For this must calculate the following M=b(ax)1modp.

The security of the ElGamal scheme depends on different lengths of random k key. The negative side of this algorithm is doubled length of encrypted message. ElGamal algorithm security reasons are necessary to use different k key for each M and M' different plaintexts. Otherwise, if user use the same k key then user will have (a, b)

and (a', b') ciphertexts, for them the following equation b(b')1 = M(M')1 is used. That means the following, M' can be easily calculated if M is already known.

3.3 Proposed System

As found through literature study that singular encryption systems are more prone to have vulnerabilities and hence it is decide to develop a hybrid cryptosystem. Feasible and efficient encryption algorithms were also researched. Through which decision was made to make use of the symmetric key AES algorithm and asymmetric key ElGamal algorithm.

This project proposes a new model of hybrid cryptosystem with combination of two AES (symmetric) and ElGamal (Asymmetric) algorithms. This model is a combination of those two cryptosystems. Whole process is divided into two parts. First part is encryption of the encryption key. Second part is encryption of the plaintext (Message) with this key.

In the beginning the sender provides the key, which is used for the AES encryption system. But at first, this key must be encrypted using the ElGamal algorithm. For encryption users must provide y, g, p public keys and x private keys. As a result, user will get an encrypted key, which is actually introduced with A and B encrypted ciphers. Second part of this model is encryption of the message itself. One of these keys (A or B, or A and B) or both will be used for encryption of plaintext. Decryption process will be done in reverse mode.

For the proposed hybrid algorithm's implementation encryption and decryption processes of different data sizes using the software code is realized in the node.js platform.

3.4 Process Flow

The usual process flow of this project can be seen in the figure 3.2 where the sender sends a message which is first encrypted at the local machine of the sender then it is transmitted or stored in the cloud. Whereas on the receiver side or when the user retrieves data from the cloud it is transmitted from cloud to receiver's machine and decrypted at receiver's end.

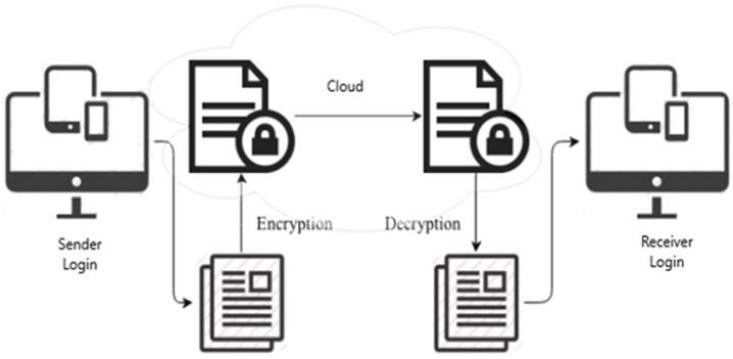

Fig. 3.2 Process flow diagram

3.5 Functional Requirements

- User Data Protection:-

  Policies must be clearly defined in the system for data (access control or information flow rules), and must develop various means to implement the policy, possibly support off-line storage, import, and export, and provide integrity when transferring user data between concerned parties.

- Identification and authentication:-

  Users of the system must be identified and authenticated with means of username & passwords. Also necessary steps should be taken to store the password in such a way that it cannot be used when the system is compromised. Also appropriate authentication of users should be provided.

- Security Management:-

  Access control must be properly implemented in the system to terminate unauthorized access to crucial information. Also assign roles of special privileges to trusted users only. And these privileged users' actions on the system should be monitored and operations on the system should be carried out without any fault.

- Key Management:-

  As in the proposed system two cryptographic algorithms are used (AES & ElGamal) for providing security. Both of them have different ways of key management approaches. Hence when combining both of them a secure transmission way must be developed for key sharing.

3.6 Non-functional Requirements

- Safety Requirements:-

  The system must have appropriate levels of backup and disaster recovery procedures in place to protect the public keys and encrypted texts & system logs.

- Security Requirements:-

  The system should only be available to the legitimate users and only authorized to interact if authenticated with correct credentials.

- Reliability:-

  The framework must caution any inability to effectively encrypt texts. The system must update the records of encrypted text in the database without fail.

- User Friendly System:-

  The system must have consistent fluid experience through all UI elements and be consistent & responsive.

- Performance test requirement:-

  The system must make available the results of all performance tests to form a benchmark for future reference and performance levels for the system.

  The System must successfully perform full regression testing for changes as appropriate and for new releases.

Chapter 4

System Design

5.1 Introduction

This is the software development stage and it is based on the user requirements and the detailed analysis of a system that was analysed on from the system analysis. Basically this system design is converting the requirements into a tangible reality. Hence, the system designed must meet user's requirements. The purpose of this system design is to create a technical solution that satisfies the functional requirements for the proposed system.

5.2 Block diagram of system

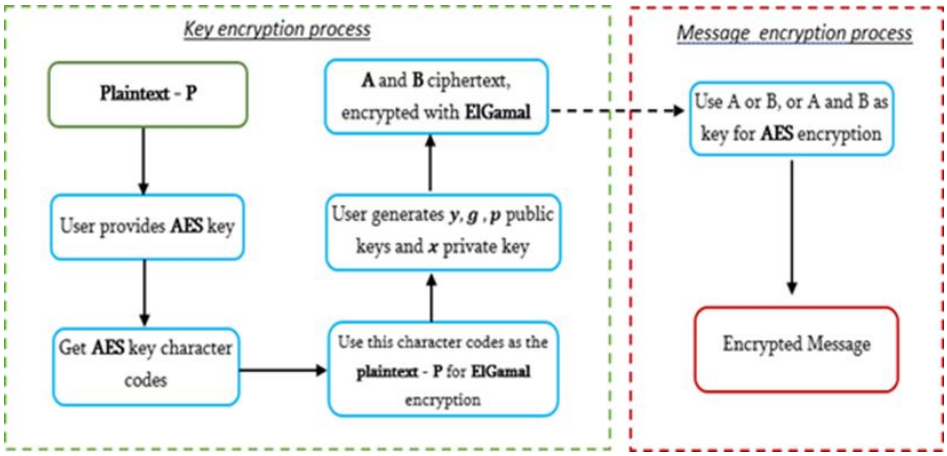

Fig. 4.1 Block diagram of the hybrid cryptographic system

The process of hybrid encryption is divided into two parts:

- Key encryption process:-

  In the first part sender provides a key which is employed for AES encryption is encrypted using ElGamal encryption for which required y, g, p public key and x private key is provided by sender. As a result, user is going to get encrypted key, which is really introduced with A and B encrypted ciphers.

- Message encryption process;-

  The second part of this model is the encryption of the message itself. One amongst these keys (A or B, or A and B) or both are going to be used for encryption of plaintext. The decryption process is going to be drained reverse mode.

5.3 Data flow diagram

The Data Flow Diagram (DFD) is a structured analysis and design method. It is a traditional visual representation of the information flows within a system. Data Flow Diagram (DFD) is widely used for software analysis and design. A neat and clear DFD can depict a good amount of the system requirements graphically.

The Data Flow Diagram (DFD) depicts the logic models and expresses data transformation in a system. It includes a mechanism to model the data flow and supports decomposition to illustrate details of the data flows and functions. A Data Flow Diagram cannot present information on operation sequence. Therefore, it is not a process or procedure modelling method.

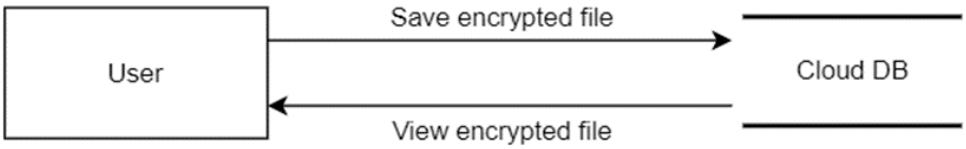

Fig. 4.2 DFD Level 0

- DFD Level 0:-

  It is also known as context diagram. It's designed to be an abstraction view, showing the system as a single process with its relationship to external entities. It represents the entire system as single bubble with input and output data indicated by incoming/outgoing arrows.

  The purpose of this project is to develop a way through which data could be stored in the cloud securely which is presented in the above diagram.

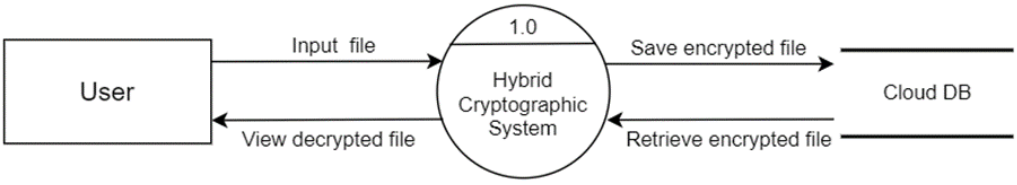

Fig. 4.3 DFD Level 1

- DFD Level 1:-

  In 1-level DFD, context diagram is decomposed into multiple bubbles/processes.in this level the main functions of the system is highlighted and break down the high level process of 0-level DFD into sub processes.

The proposed system encrypts the data at the user's local machine before it is sent to the cloud. The proposed system acts as an intermediary that provides additional security to the whole transmission process between concerned parties.

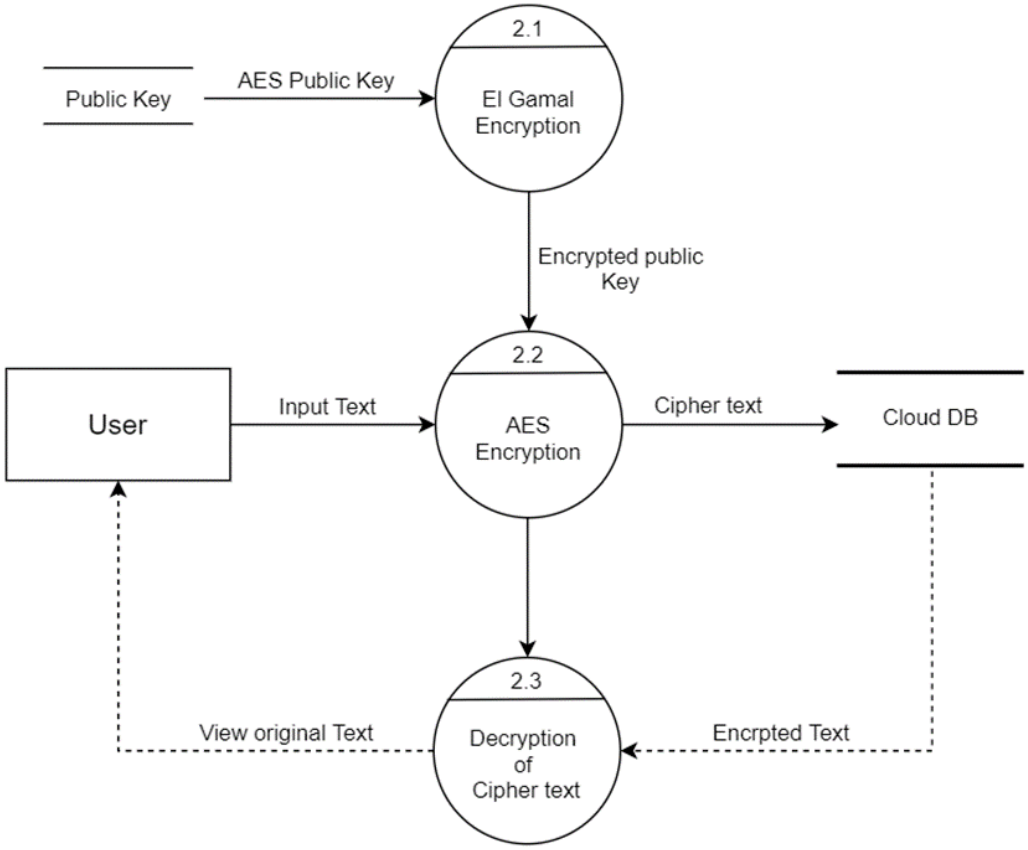

Fig. 4.4 DFD Level 2

- DFD Level 2:-

  2-level DFD goes one step deeper into parts of 1-level DFD. It can be used to plan or record the specific/necessary detail about the system's functioning.

  At this level the whole implementation of the proposed system could be seen. The two part process of key encryption and then message encryption can be seen in the diagram. Also the decryption of the encrypted text can also be seen.

5.4 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. A use case diagram can identify the different types of users of a system and the different use cases and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses.

The user of the system could login into the system if the user doesn't have an account on the system he/she could register it in the system. While logging in, the system authenticates users via means of username and password.

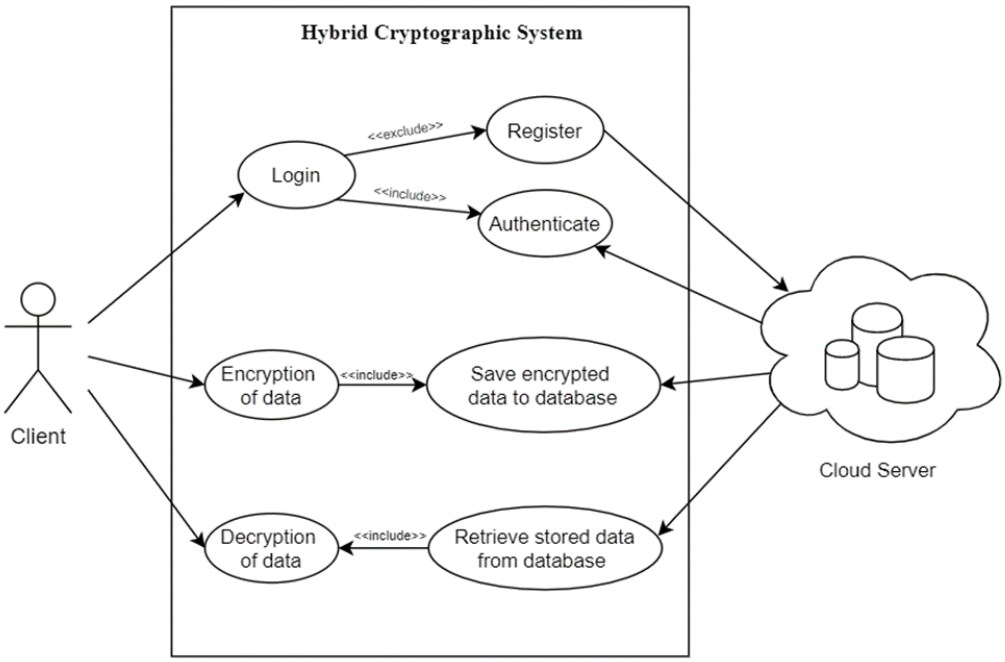

Fig. 4.5 Use case diagram

After logging in the system if the user wants to encrypt a new text message then the user will enter text into the system and similarly if the user wants to decrypt previously stored messages in the cloud he/she could also do that and obtain original text message.

5.5 Entity relation diagram

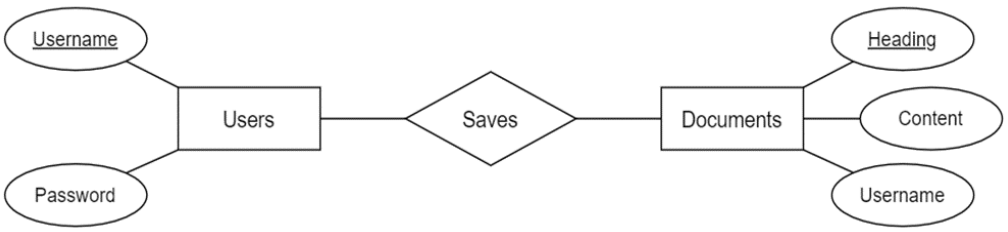

Fig. 4.6 ER Diagram

Entity Relational Model is a high-level conceptual data model diagram. ER modelling helps you to analyse data requirements systematically to produce a well-designed database. The Entity-Relation model represents real-world entities and the relationship between them. It is considered a best practice to complete ER modelling before implementing database.

5.6 Activity diagram

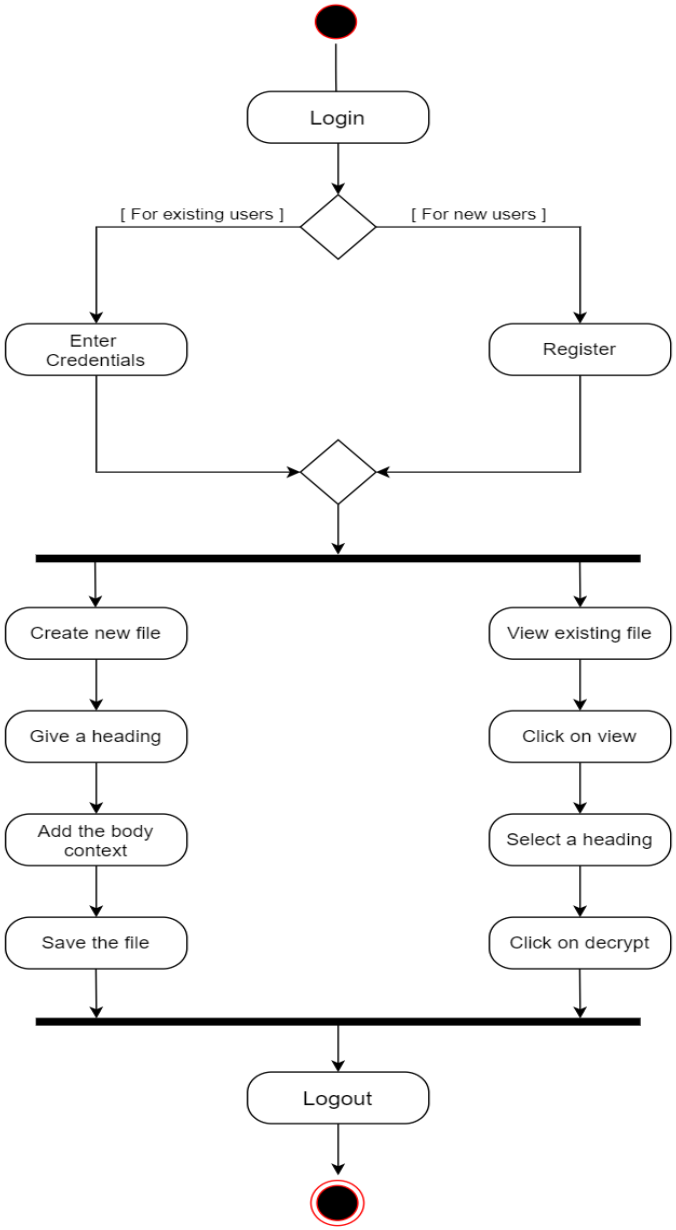

Fig. 4.7 Activity diagram

5.7 Test design for work

Systems design service is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. Service design is the activity of planning and organizing people, infrastructure, communication and material components of a service in order to improve its quality and the interaction between the service

provider and its customers. Service design may function as a way to inform changes to an existing service or create a new service entirely.

The purpose of service design methodologies is to establish best practices for designing services according to both the needs of customers and the competencies and capabilities of service providers. For this purpose, service design uses methods and tools derived from different disciplines, ranging from ethnography to information and management science to interaction design.

- Unit Testing:-

  Unit testing is a software development process in which the smallest testable parts of an application, called units, are individually and independently scrutinized for proper operation. Unit testing can be done manually but is often automated. Unit testing is a component of test-driven development (TDD), a pragmatic methodology that takes a meticulous approach to building a product by means of continual testing and revision. Test-driven development requires that developers first write failing unit tests. Then they write code and refactor the application until the test passes. TDD typically results in an explicit and predictable code base.

  Unit testing involves only those characteristics that are vital to the performance of the unit under test. This encourages developers to modify the source code without immediate concerns about how such changes might affect the functioning of other units or the program as a whole. The development team needs to learn what unit testing is, how to unit test, what to unit test and how to use automated software tools to facilitate the process on an on-going basis. The great benefit to unit testing is that the earlier a problem is identified, the fewer compound errors occur.

- Integration Testing:-

  Integration testing involves the overall testing of a complete system of many subsystem components or elements. The system under test may be composed of hardware, or software, or hardware with embedded software, or hardware/software with human-in-the-loop testing.IT consists, initially, of the "process of assembling the constituent parts of a system in a logical, cost-effective way, comprehensively checking system execution (all nominal & exceptional paths), and including a full functional check-out." Following integration, system test is a process of "verifying that the system meets its requirements, and validating that the system performs in accordance with the customer or user expectations."

Chapter 5

Implementation

5.1 Introduction

Implementation refers to the way how the system concept is carried out using the project plan. It is a very crucial step in SDLC where actual execution of the system is done. Result of this step is a working system which must be evaluated for its performance. If all the system requirements and project objectives are not well understood then the developed system may not perform as desired.

5.2 Environment setup

- Node.js :-

  Node.js is an open-source, cross-platform, JavaScript runtime environment that executes JavaScript code outside of a web browser. Node.js lets developers use JavaScript to write command line tools and for server-side scripting—running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser. Consequently, Node.js represents a "JavaScript everywhere" paradigm, unifying web-application development around a single programming language, rather than different languages for server- and client-side scripts. Though .js is the standard filename extension for JavaScript code, the name "Node.js" doesn't refer to a particular file in this context and is merely the name of the product. Node.js has an event-driven architecture capable of asynchronous I/O.

- MongoDB-:

  MongoDB is an open source database management system (DBMS) that uses a document-oriented database model which supports various forms of data. It is one of numerous no relational database technologies which arose in the mid-2000s under the NoSQL banner for use in big data applications and other processing jobs involving data that doesn't fit well in a rigid relational model. Instead of using tables and rows as in relational databases, the MongoDB architecture is made up of collections and documents.

5.3 Languages used

- JavaScript:-

  JavaScript often abbreviated as JS, is a programming language that conforms to the ECMAScript specification. JavaScript is high-level, often just-in-time compiled, and multi-paradigm. It has curly-bracket syntax, dynamic typing, prototype-based object-orientation, and first-class functions. Alongside HTML and CSS, JavaScript is one of the core technologies of the World Wide Web. JavaScript enables interactive web pages and is an essential part of web applications. The vast majority of websites use it for client-side page behaviour, and all major web browsers have a dedicated JavaScript engine to execute it.

- HTML:-

  Hypertext Markup Language (HTML) is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document.

- JSON:-

  JavaScript Object Notation is an open standard file format, and data interchange format, that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and array data types (or any other serializable value). It is a very common data format, with a diverse range of applications, such as serving as replacement for XML in AJAX systems.

5.4 Developing model

The prototyping model is applied when detailed information related to input and output requirements of the system is not available. In this model, it is assumed that not all the requirements may be known at the start of the development of the system. It is usually used when a system does not exist or in case of a large and complex system where there is no manual

process to determine the requirements. This model allows the user to interact and experiment of working model of the system known as prototype**.**

1. Requirement gathering and analysis:

   A prototyping model begins with the requirement analysis and requirements of the system are defined in detail. The user is interviewed in order to know the requirements of the system.

2. Quick Design:

   When requirements are known, preliminary design or a quick design for the system is created. It is not a detailed design and includes only the important aspects of the system, which gives an idea of the system to the user. A quick design helps in developing the prototype.

3. Build Prototype:

   Information gathered from quick design is modified to form the 1stprototype, which represents the working model of the requirement system.

4. User Evaluation:

   Next, the proposed system is presented to the user for thorough evaluation of the prototype to recognize its strengths and weaknesses such as what is to be added or removed. Comments and suggestions are collected from the user and provided to the developer.

5. Refining Prototype:

   Once the user evaluates the prototype and if he is not satisfied, the current prototype is refined according to the requirements. That is, a new prototype is developed with the additional information provided by the user. The new prototype is evaluated just like the previous prototype. This process continuous until all the requirements specified by the user is met. Once the user is satisfied with the developed prototype, a final system is developed based on the final prototype.

6. Engineer Product:

   Once the requirements are completely met, the user accepts the final prototype. The final system is evaluated thoroughly followed by the routine maintenance on regular basis for preventing large-scale failures and minimizing downtime.

Chapter 6

Data Analysis & Results

6.1 Introduction

After the project has been implemented completely, information products and results could be analysed to measure the system performance and to ensure if the system is meeting all the requirements. These analyses usually contain statistics which are compared and tested to yield results from comparison and other procedures.

In the proposed system statistical data is used for both AES and El Gamal cryptographic system and Hybrid cryptosystem. These statistics have four parameters namely encryption time, decryption time, memory used and cipher text size. All four of them together would help us to evaluate system performance of all the systems through experimental research.

6.2 User interface of work

The user interface (UI), in the industrial design field of human-computer interaction, is the space where interactions between humans and machines occur. The goal of this interaction is to allow effective operation and control of the machine from the human end, whilst the machine simultaneously feeds back information that aids the operators' decision-making process.

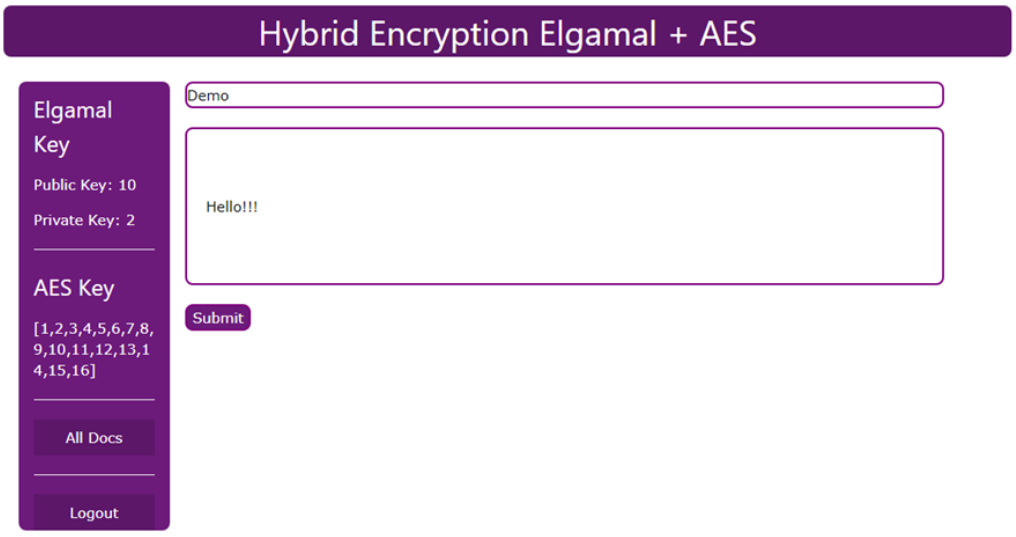

Fig. 6.1 User interface for user input page

This is the first window which is displayed in the system after the user has logged in the system. This window includes the heading box which is used to identify different texts stored in the cloud similar as the subject in the mail system.

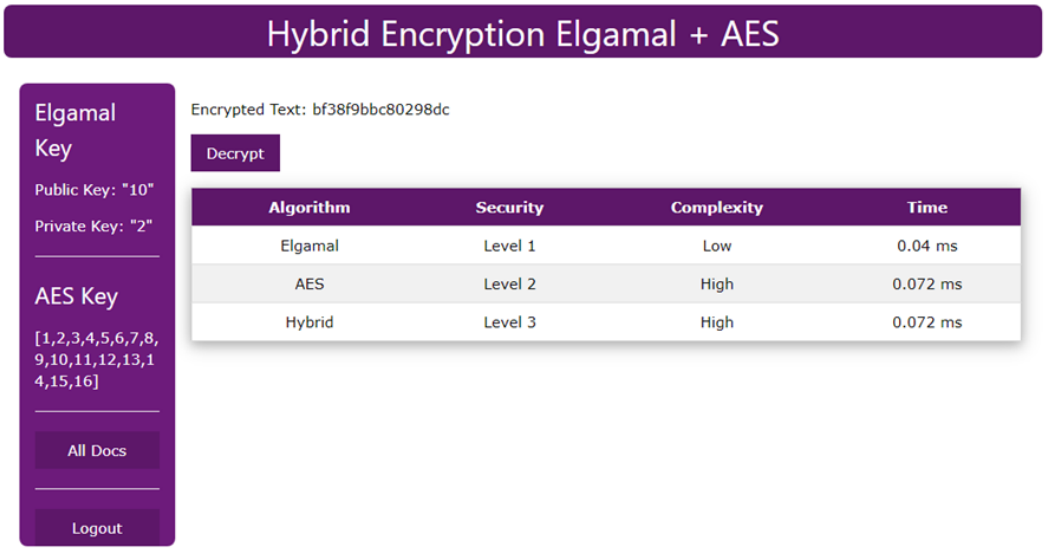

Fig. 6.2 User interface for encrypted text page

After the user has encrypted the test this window appears. Here in the upper side the cipher text can be seen and a report of each algorithm AES, ElGamal & hybrid can be seen in the page. At the left side of the page public and private key used for the encryption in both AES and ElGamal are displayed.

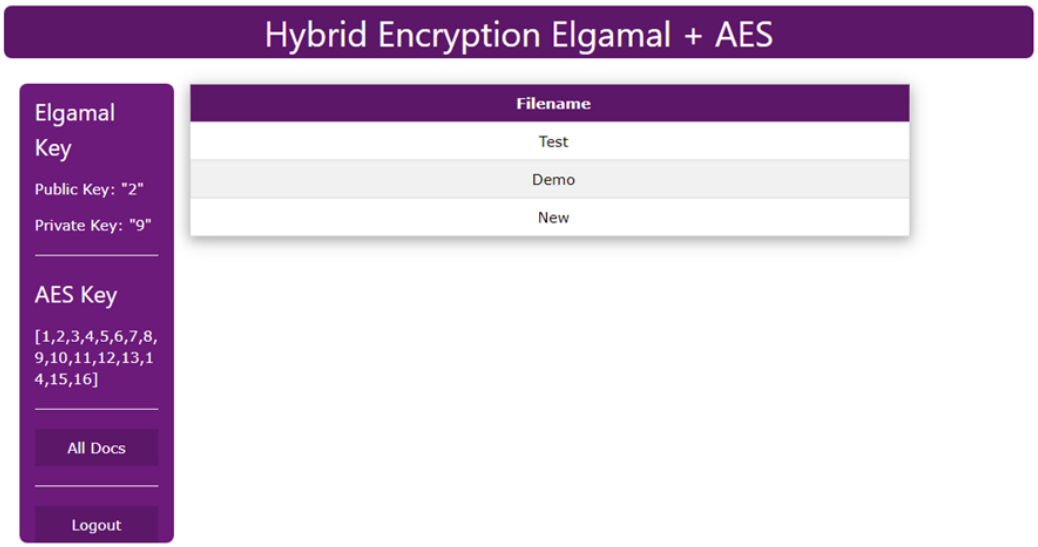

Fig. 6.3 User interface for stored cipher texts

This window appears when the user clicks on the ‘All Docs’ button on the left side of the page which contains all the previously stored cipher texts in order they were created. These cipher texts could be identified by the heading given at encryption time.

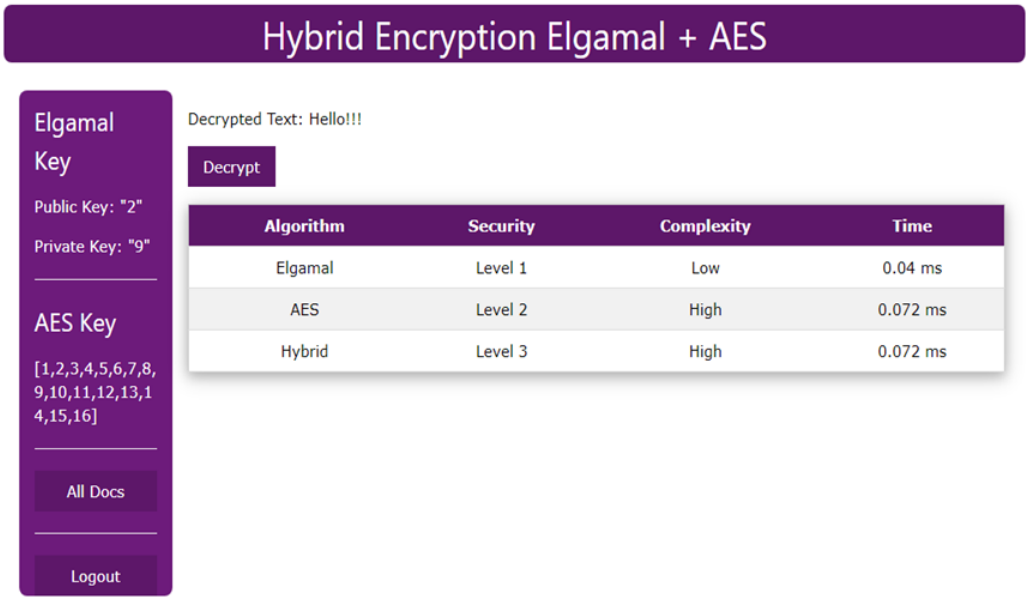

Fig. 6.4 User interface for viewing original texts

This window appears when a user wants to view his/her encrypted texts. When clicked on the 'Decrypt' button, the cipher text changes into corresponding simple text. Throughout the system UI on the left side of the pages is the same for providing keys information & direct access to 'All Docs' and 'Logout' buttons.

6.3 Data collection

Data collection is essential for system performance measurement. Here in this case text inputs of different sizes are given to all three systems and the results are noted as shown in the tables.

Table I. Experimental results on AES

Plainetext size (Kilobytes)	**Encryption Time (nanoseconds)**	**Decryption Time (nanoseconds)**	**Used RAM (Bytes)**	**Encrypted text size (Kilobytes)**
32	10885816	13183260	10438616	44
64	11619392	19435850	11616928	87
128	12595776	23731067	14259312	175
256	14941600	39475025	19446952	350

383	17911200	51462211	25536712	525
512	19578712	56630859	29827912	700
640	21102120	64556965	11701832	876
1024	23745952	72088845	30773720	1401
1664	23917200	67403987	32465440	2277
2048	27348528	135473361	46150064	2802
3328	39767696	250928350	70698544	4554
4096	47157952	227850681	97370664	5604
5120	45313504	283950147	75567816	7006
6144	95522296	308917134	68862920	8407
7168	106414488	354152143	80110040	9808

Table II. Experimental results on ElGamal

Plainetext size (Kilobytes)	**Encryption Time (nanoseconds)**	**Decryption Time (nanoseconds)**	**Used RAM (Bytes)**	**Encrypted text size (Kilobytes)**
32	30563800	28566844	56142968	92
64	111413712	32170582	118217248	736
128	172191288	77038870	291667624	1103
256	275272096	113553330	332891746	1839
383	336428336	145442172	365965008	2942
512	361937784	172920490	271493032	5883
640	439920368	231472754	218697896	7721
1024	557353760	382681610	239611976	13603

Table III. Experimental results on AES & ELGAMAL Hybrid model

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size (Kilobytes)
32	11422808	11475187	10554248	44
64	12139408	14042938	12480872	87
128	13122456	19254605	14083528	175
256	15349104	32248157	18823832	350
383	18497728	43386244	24424880	525
512	20011400	48810538	28279896	700
640	21598680	67133177	29075848	876
1024	21195488	81189868	29961968	1401
1664	21283344	96277607	31385096	2277
2048	23800368	115473678	35746432	2802
3328	39792256	175045003	60485784	4554
4096	47208608	200580406	89747792	5604
5120	45346272	255886133	86760704	7006
6144	95557608	301044625	103606520	8407
7168	106426216	332311451	104075496	9808

6.4 Results

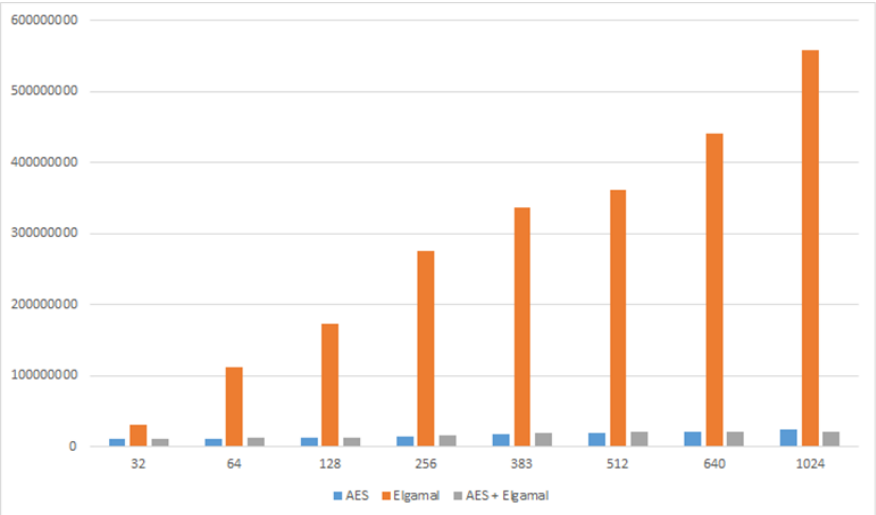

Fig. 6.5 Encryption time (Nanoseconds) for AES, ElGamal and Hybrid algorithms

After this experimental research, comparison between the described systems by its encryption time can be done. As comparative research is done on AES, ElGamal and Hybrid AES & ElGamal, so it can be simply understood that the time required for encryption of Hybrid AES-ElGamal is less than the time requirement of ElGamal. AES needs less encryption time than the hybrid system (Figs 6.5, 6.6). The strength of this hybrid system could be considered one of the competition with others.

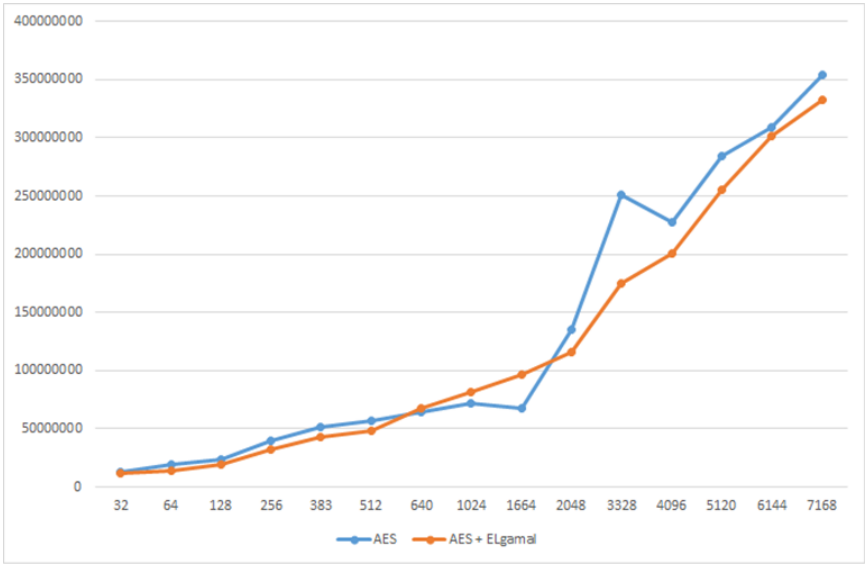

Fig. 6.6 Decryption time (Nanoseconds) for AES and AES + ElGamal algorithms

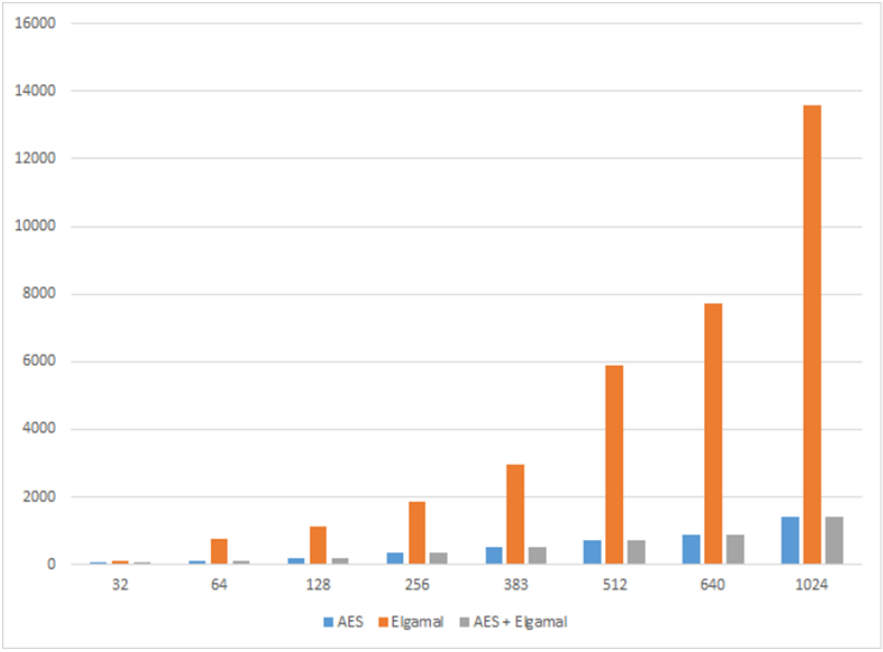

Fig. 6.7 Encrypted file size comparison with plaintext size (Kilobytes) for AES, ElGamal and AES & ElGamal algorithms

During experiments on the proposed hybrid algorithm a comparison of plaintext size and encrypted file size (Kilobytes) was done. Results show that during an encryption process with AES algorithm encrypted file size becomes on average ~1.37 times bigger than plaintext file size. Using the ElGamal algorithm, encrypted file size becomes on average ~9.34 times bigger than plaintext file size. Figure 6.7 shows encrypted file size comparison chart results on the proposed algorithms. According to results, the new hybrid model has better results compared with the ElGamal algorithm.

Chapter 7

Summary, Conclusion, and Future Scope

7.1 Summary

As more individuals and organizations are moving towards adaptation of cloud technology in their daily tasks and operations because of its advantages over traditional computing and storage. It has become terribly crucial to secure the data that is resided at the cloud provider's side. Several such cloud systems use traditional security methods which that used as sole security solutions when it involves encrypting information. To overcome the drawbacks of such algorithms, a new hybrid cryptographic algorithm was developed.

The algorithm is designed using a combination of two cryptologic algorithms AES and ElGamal. After the implementation of the proposed system, experimental analysis was also done between the proposed and existing systems. This new hybrid cryptographic technique has been designed to decrease encryption and decryption time and increase throughput. It is safer and powerful compared to previous cryptography models and it's used for management systems security. Also, the encrypted data is securely kept in a cloud and decrypted during retrieval to get the original plaintext.

7.2 Conclusion

Compared with encryption and decryption speed experimental research shows that symmetric algorithm AES is quicker, but asymmetric algorithm ElGamal is healthier to produce security. The symmetric algorithm AES requires very low computational power. AES is one of the most effective algorithms of symmetric encryption cryptography. ElGamal algorithm gives high throughput as compared to AES and other algorithms.

The hybrid of AES and ElGamal algorithm has characteristics of both the algorithms. This makes the algorithm strong against vulnerabilities. This hybrid structure of AES and ElGamal provides more security by increasing the complexity. Because the result shows, the proposed AES & ElGamal hybrid algorithm model is relatively better than ElGamal in terms of encryption/decryption time and better than AES in terms of its security. The complexity of the system is provided by a mixture of two algorithms. Given results are often implemented in aviation for control systems yet as other critical aviation information systems security ensuring.

7.3 Limitations

- Images, video & audio couldn’t be encrypted within the proposed system because it is intended as a symptom of concept and also encryption of the mentioned file format would require significant memory and computational power.
- Although the system supports text through file but within the final implementation text could only be provided by entering through the text box.
- System is currently developed with an online interface in mind hence while porting code to a different platform may require modification in code.
- System isn't tested on the particular cloud environment hence any unintentional behaviour can't be predicted.

7.4 Recommendation for Future Study

The major changes or updates which can be done in future consists of upgradation of same technology and hybrid algorithm used for encryption of information. These upgradation are for future scope because technology evolves rapidly and many minute modules within the implemented system can be modified for betterment. Another upgrade for future is optimization of resources used in the system. It goes hand in hand along with technology. Resource optimization consists of memory optimization, processing optimization, etc. Security plays a major role in the overall success of system. Hence, upgrading security is very vital for future scope. The overall future scope and its objectives consists of making a compact and secure system along with its various software modules which can in general handle a lot of situations and scenarios faced by the implemented system. Other formats than text can further be added as an input. In future along with encryption hash function also can be used to improve security. System could be further developed as an extension for end-to-end encryption of the messages. It can be also used for encrypting data stored on cloud especially documents scanned using OCR could be protected better way.

References

Books,

[1] Atul Kahate. May 2019. *Cryptography and Network Security*, Tata Mc Graw Hill, 4th Edition.

[2] William Stallings. March 2013. *Cryptography and Network Security, Principles and Practice*, 6th Edition, Pearson Education.

Journal papers,

[1] Baldeep Singh, Maninder Kaur, Navpreet Kaur, "Comparative Study of Different Cryptographic Algorithms", *3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 2017 (Fall).

[2] L. Yu, D. Zhang, L. Wu, S. Xie, D. Su and X. Wang, "AES Design Improvements Towards Information Security Considering Scan Attack," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, 2018, pp. 322-326.

[3] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," *2017 ieee 3rd International Conference On Big Data Security On Cloud (Bigdatasecurity), IEEE International Conference On High Performance And Smart Computing (HPSC), And IEEE International Conference On Intelligent Data And Security (Ids*), Beijing, 2017, pp. 145-149.

[4] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall*), Dehradun, 2017, pp. 1-7.

[5] A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," *2018 International Conference on Computing, Power and Communication Technologies (GUCON),* Greater Noida, Uttar Pradesh, India, 2018, pp. 633-636.

IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

[1]Akash Salve, [2]Raul Dhruva, [3]Yogesh Sauw, [4]Yogita Ganage

[1]Student BE, [2]Student BE, [3]Student BE, [4]Professor
[1]Department of Information Technology,
[1]MCT's Rajiv Gandhi Institute of Technology, Mumbai, India

Abstract : Computer networks and internet applications are evolving rapidly, so data security is that the challenging issue of today that touches many areas. To cease unauthorized access to the user data or database, any transmission & storage process must be securely encrypted. The goals of this paper are: 1) To propose new hybrid cryptographic algorithm model employing a mix of two cryptographic algorithms AES and ElGamal; 2) Provide comparison between two symmetric, asymmetric algorithms and proposed hybrid model; 3) to suggest effectiveness and security of recent hybrid model which makes the algorithm strong against vulnerabilities. Currently, many encryption algorithms are available to securely encrypt the information but some algorithms exhaust many computing resources like memory and CPU time. This paper presents a comparative analysis of experimental results on these encryption algorithms supported various parameters affecting security and efficiency. The target of this research is to see the performance of AES, ElGamal cryptography algorithms and AES & ElGamal hybrid cryptography algorithm. The performance of the implemented encryption algorithms is evaluated by means of encryption and decryption time and memory usage. To create comparison experiments, for these algorithms special software was developed. The substitute language JavaScript is used for realizing the encryption algorithms in code. As a result, the paper shows that the new hybrid encryption model is safer and powerful compared to previous cryptography models and it's used for control systems security.

IndexTerms **- cryptography, encryption, decryption, hybrid cryptosystem, public key cryptosystems.**

I. INTRODUCTION

Symmetric (secret key) cryptography systems use the identical cryptographic keys for both plaintext encryption and ciphertext decryption [1], [2]. Typically, with a symmetric key, you'll be able to exchange the key with another trusted participant. The entire security of this method stands on the secrecy of the key. During this way, the key must be kept secret to every participant.

Asymmetric (public key) cryptography is one in every of the important directions of secure data transferring. There are developed form of public-key encryption systems. Unfortunately, there's significantly fewer developments publicly key algorithms than in symmetric key algorithms [1], [2]. This can be also results of different key sharing technology. Asymmetric cryptography relies on digital signature functions. Is additionally employed in software tools, like browsers, which require to ascertain secure connection over an insecure network just like the internet or have to validate the digital signature. Digital signature is a mathematical technique providing validation of the authenticity and integrity of message, software or digital document.

In general, the strength of the cryptosystem can't be totally ensured. Of course, all cryptography algorithms are developed to supply the best security, but because of the very fact that technology is consistently being developed, security systems are getting less immune to every known or new attack.

II. STRENGTH AND WEAKNESS OF SYMMETRIC KEY AND ASYMMETRIC KEY CRYPTOGRAPHIC SYSTEM

One of the strong points of symmetric key cryptography is resistance of the key key against Brute Force Attack. the aptitude of a cryptographic system to shield data from attack is named its strength. Of course, the best thanks to attack encrypted messages is solely to try decryption the message with every possible key [3]. Strength depends on various factors, including: the secrecy of the key; the issue of guessing the key or trying out all possible keys (a key search); the issue of reversing the encryption algorithm without knowing the encryption key (breaking the encryption algorithm); lack of back doors, or other ways by which an encrypted file is decrypted more easily without knowing the key [1], [4].

The weak side of symmetric key systems is to settle on the correct key. Attacks against encrypted information represent three main categories. Those are: Key search (brute force) attacks; Cryptanalysis; Systems-based attacks [5] – [7].

Through increasing the length of the key, the number of possible permutations is additionally exponentially increased. Meaning following, brute force attack needs more technical resources to attack the system. This type of

attack is additionally called key search attack. Key search attacks aren't very effective. If the chosen secret's long enough, a key search attack isn't even possible [8] – [10].

Asymmetric (public key) cryptographic system uses two keys: public keys which can be distributed widely, and personal keys which are known only to the owner [1]. During this encryption system, anyone can encrypt a message using the receiver's public key. The strength of a public key cryptography system relies on the computational effort (work consider cryptography) required to seek out the private key from its paired public key. The most weakness of this technique is number of public keys. Thanks to increasing number of users, quantity of shared keys is additionally proportionally increased [11]. So that, public key algorithms are easier to attack than symmetric key algorithms for the explanation that the attacker (probably) encompasses a copy of the general public key that was accustomed encrypt the message [4].

III. HYBRID CRYPTOSYSTEM

Hybrid encryption merges two or more encryption systems [12] – [14]. It's a mix of asymmetric and symmetric encryption to learn from the strengths of every variety of encryption. These strengths are respectively defined as speed and security [15], [16]. Hybrid encryption is taken into account a highly secure form of encryption as long because the public and personal keys are fully secure [17]. A hybrid system is introduced with the subsequent schema: Key encapsulation scheme, which may be a public-key cryptosystem; an information encapsulation scheme, which may be a symmetric-key cryptosystem [1].

Public key cryptosystems depend on hard mathematical functions. For instance, RSA relies on the sensible difficulty of product factorization by large prime numbers. In hybrid systems for encryption and decryption process is employed fast symmetric key systems. For key management is employed slower asymmetric algorithms, with strong mathematical functions within the background.

Both symmetric and asymmetric key algorithms have their advantages and drawbacks. Symmetric key algorithms are faster than asymmetric algorithms. The most requirement is that secret key must be shared during a secure way. Asymmetric systems provide secure transmission of keys, but this process needs far more time. To enhance this problem is to use the hybrid algorithm, which implies using differing kinds of cryptosystems together.

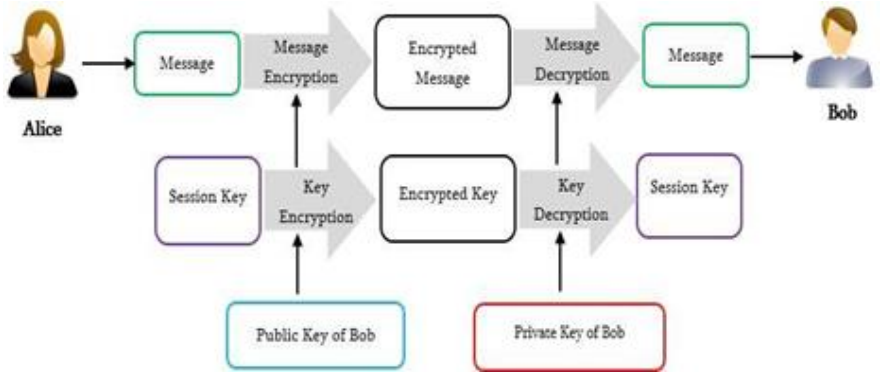

Fig. 1. The General idea of Hybrid cryptosystem

The main idea of a hybrid cryptographic system is the generation of random keys for symmetric systems. The next step is to encrypt the key for asymmetric systems. As a result we have secret key which can be used for encryption of plaintext. During the decryption process first, we use private key, and then we publish the key (Fig. 1). In Figure 1 Alice wants to send a message to Bob in a secure way, considering all aspects of security. For that, both sides use a hybrid cryptosystem.

IV. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) or the same Rijndael is the symmetric key encryption algorithm. For AES there are selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits [1], [2]. Algorithms can be judged on their ability to resist attack as compared to other submitted ciphers. Security is considered the most important factor in the competition. Algorithms can be evaluated also with suitability and overall, relative simplicity of implementation in hardware or software.

V. ELGAMAL CRYPTOGRAPHY

ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange and provides additional security layer by asymmetrically encrypting keys, previously used for symmetric message encryption. The security of this algorithm is based on Discrete Logarithm Problem. Generally, the ElGamal cryptosystem is used in a hybrid cryptosystem. The plaintext is encrypted with a symmetric cryptosystem and ElGamal is then used to encrypt the key. Asymmetric cryptosystems

like ElGamal are usually slower than symmetric ones. It is faster to encrypt the key with ElGamal and the message (which can be randomly large) with a symmetric cipher [16].

ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

At first happens key generation process with following steps [16]:

- Alice generates random prime p;
- then is chosen g generator, with following criteria g < p;
- Alice randomly choses integer x with following criteria 1< x < p;
- Alice computes y = gx mod p ;
- Alice publishes y, g, p and sends them to Bob as an public keys. Alice retains x as her private key, which must be kept secret.

The second step of ElGamal algorithm is encryption of plaintext. After receiving public keys from Alice, Bob starts to encrypt plaintext using those keys. We have following steps [16]:

- at first we have plaintext M. Bob chooses random prime key k with following criteria 1< k < p – 1;
- than computes a and b numbers whereas, a = gk mod p, and b = yk M mod p;
- exactly those (a, b) is the encrypted plaintext.

The decryption algorithm works as follows: to decrypt a ciphertext (a, b) is decrypted with private key x. For this must calculate following M = b (ax) 1 mod p [16].

The security of the ElGamal scheme depends on different length of random k key. The negative side of this algorithm is doubled length of encrypted message. ElGamal algorithm security reasons is necessary to use different k key for each M and M' different plaintexts. Otherwise, if we use same k key we will have (a, b) and (a', b') cyphertexts, for them we have following equation b(b')1 = M(M')1. That means following, we can easily calculate M' if we know M.

VI. SOFTWARE IMPLEMENTATION AND EXPERIMENTS OF AES AND ELGAMAL CRYPTOSYSTEMS

Cryptosystems have different system requirements and time intervals. For calculation of those parameters during the encryption/decryption process, was done through experiment using software code on JavaScript, nodeJS IDE. Generally, the time required to encrypt data is termed as encryption time of the cryptographic system the other way around for the decryption process [16]. Encryption time depends on the structural characteristic of the algorithm. Table I shows the encryption time of the AES algorithm. Experiments on-time efficiency was done on the ElGamal cryptosystem. Was used different size plaintext. As a result, we've Table II.

Table I. EXPERIMENTAL RESULTS ON AES

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size (Kilobytes)
32	10885816	13183260	10438616	44
64	11619392	19435850	11616928	87
128	12595776	23731067	14259312	175
256	14941600	39475025	19446952	350
383	17911200	51462211	25536712	525
512	19578712	56630859	29827912	700
640	21102120	64556965	11701832	876
1024	23745952	72088845	30773720	1401
1664	23917200	67403987	32465440	2277
2048	27348528	135473361	46150064	2802
3328	39767696	250928350	70698544	4554
4096	47157952	227850681	97370664	5604
5120	45313504	283950147	75567816	7006
6144	95522296	308917134	68862920	8407
7168	106414488	354152143	80110040	9808

Table II. EXPERIMENTAL RESULTS ON ELGAMAL

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size(Kilobytes)
32	30563800	28566844	56142968	92
64	111413712	32170582	118217248	736
128	172191288	77038870	291667624	1103
256	275272096	113553330	332891746	1839
383	336428336	145442172	365965008	2942
512	361937784	172920490	271493032	5883
640	439920368	231472754	218697896	7721
1024	557353760	382681610	239611976	13603

VII. PROPOSED AES&ELGAMAL HYBRID CRYPTOSYSTEM FRAMEWORK

This paper proposes a replacement model of a hybrid cryptosystem with a mix of two AES (symmetric) and ElGamal (Asymmetric) algorithms. This model could be a combination of these two cryptosystems. The full process is split into two parts. The primary part is encryption of the encryption key. The second part is that the encryption of the plaintext (Message) with this key.

In the beginning, the sender provides the key, which is employed for the AES system. But initially, this key must be encrypted using the ElGamal algorithm. For encryption, the user must provide y, g, p public keys, and x private key. As a result, we are going to get encrypted key, which is really introduced with A and B encrypted ciphers. The second part, of this model, is that the encryption of the message itself. One amongst these keys (A or B, or A and B) or both are going to be used for encryption of plaintext. The decryption process is going to be drained reverse mode. Figure 2 shows the scheme of the provided hybrid cryptosystem.

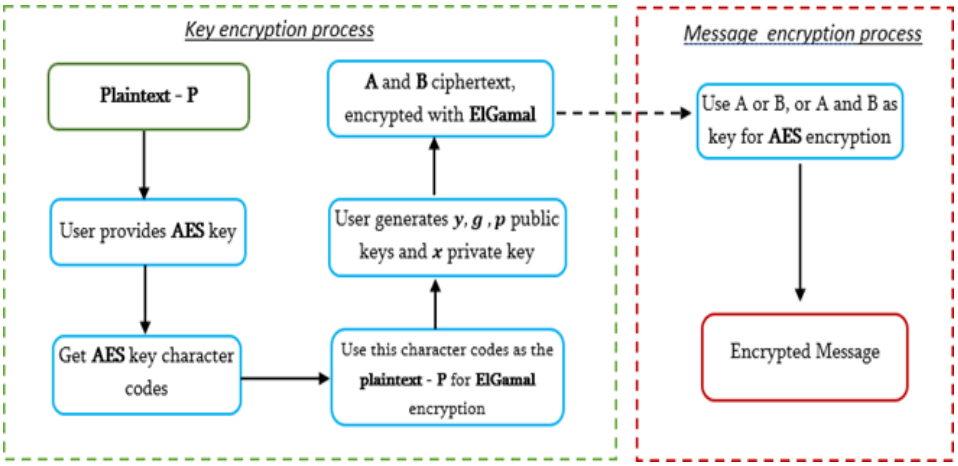

Fig. 2. The general architecture of hybrid cryptosystem obtained by the combination of AES + ElGamal cryptosystems.

For provided hybrid algorithm have been implemented encryption and decryption processes of different size data using the software code realized in the nodeJS platform. Table III shows the provided hybrid system efficiency data.

After this experimental research, we can compare the described systems by its encryption time. Was done comparative research on AES, ElGamal and Hybrid AES & ElGamal, so it can be simply understood that the time required for encryption of Hybrid AES-ElGamal is less than time requirement of ElGamal. AES needs less encryption time than provided hybrid system (Figs 3, 4). The strength of this hybrid system could be considered one of the competition with others.

TABLE III. EXPERIMENTAL RESULTS ON AES & ELGAMAL HYBRID MODEL

Plainetext size (Kilobytes)	Encryption Time (nanoseconds)	Decryption Time (nanoseconds)	Used RAM (Bytes)	Encrypted text size (Kilobytes)
32	11422808	11475187	10554248	44
64	12139408	14042938	12480872	87
128	13122456	19254605	14083528	175
256	15349104	32248157	18823832	350
383	18497728	43386244	24424880	525
512	20011400	48810538	28279896	700
640	21598680	67133177	29075848	876
1024	21195488	81189868	29961968	1401
1664	21283344	96277607	31385096	2277
2048	23800368	115473678	35746432	2802
3328	39792256	175045003	60485784	4554
4096	47208608	200580406	89747792	5604
5120	45346272	255886133	86760704	7006
6144	95557608	301044625	103606520	8407
7168	106426216	332311451	104075496	9808

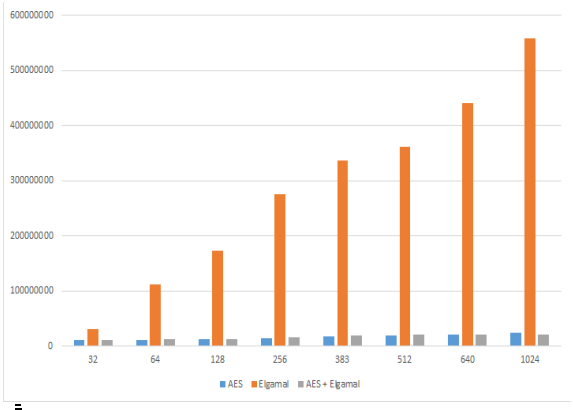

Fig. 3. Encryption time (Nanoseconds) for AES, ElGamal and AES+ElGamal algorithms.

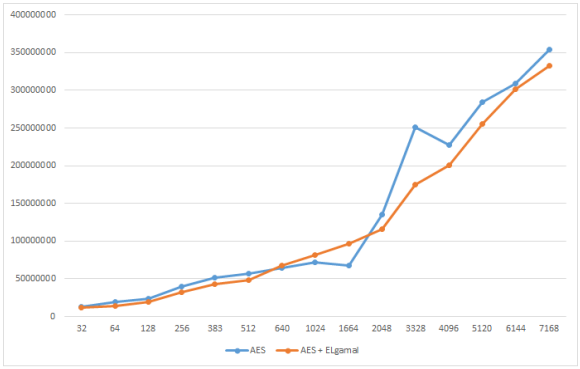

Fig. 4. Decryption time (Nanoseconds) for AES and AES+ElGamal algorithms.

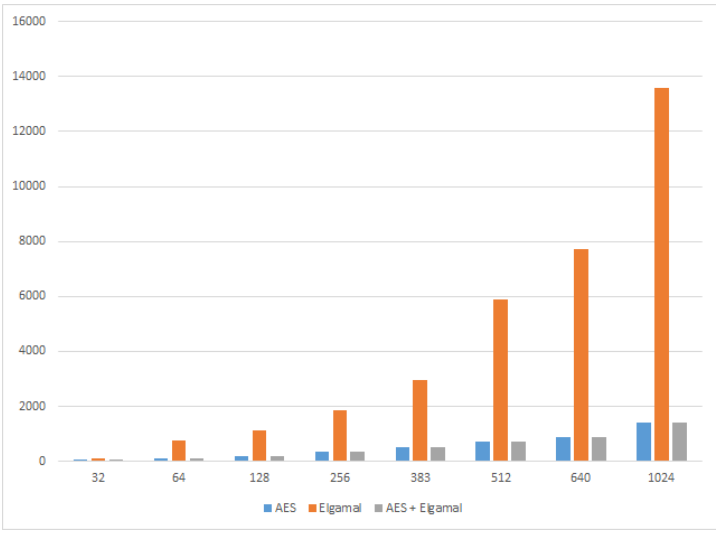

Fig 5. Encrypted file size comparison with plaintext size (Kilobytes) for AES, ElGamal and AES&ElGamal algorithms.

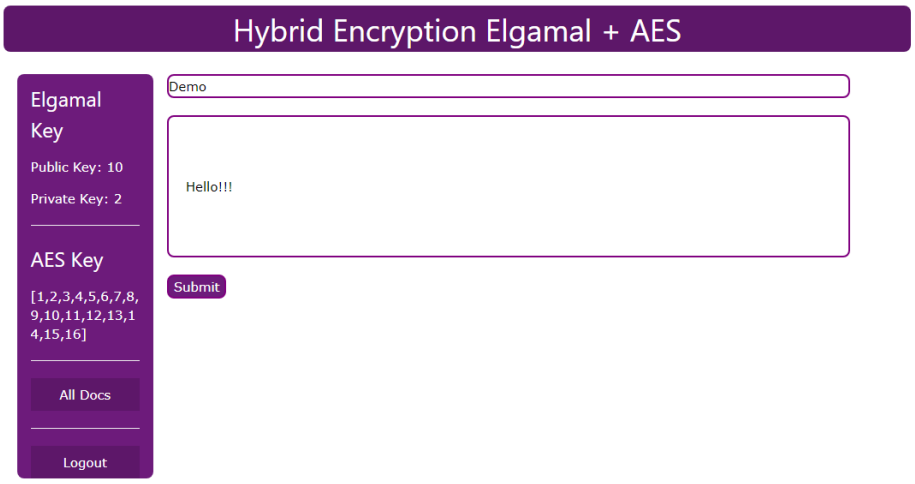

Fig 6. User interface for proposed system

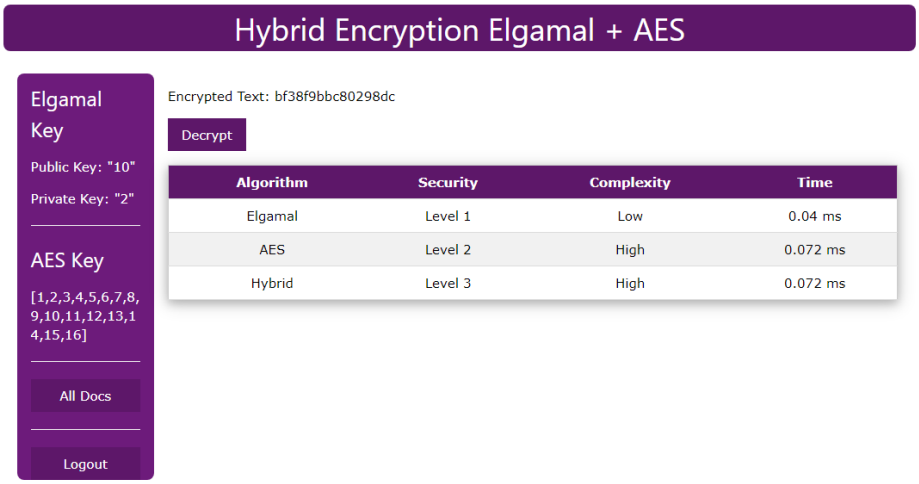

Fig 7. User interface for encryption and decryption in proposed system

During experiments on the proposed hybrid algorithm was done comparison of plaintext size and encrypted file size (Kilobytes). Results show that during an encryption process with AES algorithm encrypted file size becomes averagely ~1.37 times bigger than plaintext file size. If we are using ElGamal algorithm encrypted file size becomes averagely ~9.34 times bigger than plaintext file size. Figure 5 shows encrypted file size comparison chart results on proposed algorithms. According to results new hybrid model has better results compared with the ElGamal algorithm.

VIII. CONCLUSION

This paper explained and analyzed two varieties of systems: Symmetric and Asymmetric cryptosystems. The paper provides a replacement model of hybrid algorithm using AES and ElGamal cryptosystems. A special software tool was created and implemented for the proposed system.

Compared with encryption and decryption speed experimental research shows, that symmetric algorithm AES is quicker, but asymmetric algorithm ElGamal is healthier to produce security. The symmetric algorithm AES requires very low computational power. AES is one amongst the most effective algorithms of symmetric encryption cryptography. ElGamal algorithm gives high throughput as compared to AES and other algorithms. The hybrid of AES and ElGamal algorithm has characteristics of both the algorithms. This makes the algorithm strong against vulnerabilities. This hybrid structure of AES and ElGamal provides more security by increasing the complexity. Because the result shows, the proposed AES & ElGamal hybrid algorithm model is relatively better than ElGamal in terms of encryption/decryption time and better than AES in terms of its security. The complexity of the system is provided by a mixture of two algorithms. Given results are often implemented in aviation for control systems yet as other critical aviation information systems security ensuring.

For future work are often described as an improved version of this hybrid model, can also be tired combination with other cryptography algorithms to produce faster encryption and decryption processes, lower power and memory consumption.

REFERENCES

[1] Atul Kahate. May 2019. Cryptography and Network Security, Tata Mc Graw Hill, 4th Edition.

[2] William Stallings. March 2013. Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education.

[3] Ilya Kizhvatov. 2009. Physical Security of Cryptographic Algorithm Implementations, L'UNIVERSITÉ DU LUXEMBOURG.

[4] Simson Garfinkel, Alan Schwartz, and Gene Spafford. Practical UNIX and Internet Security, 3rd Edition Securing Solaris, Mac OS X, Linux & Free BSD.

[5] The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.

[6] S Baldeep Singh, Maninder Kaur, Navpreet Kaur. 2017 (Fall). Comparative Study of Different Cryptographic Algorithms, 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA).

[7] Lalit Singh, Dr. R.K. Bharti. November 2017. Comparative Performance Analysis of Cryptographic Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11.

[8] B. Mao, Modern Cryptography: Theory and Pactice. Moscow, Wilyams, 2005.

[9] Diao Zhe, Wang Qinghong, Su Naizheng, Zhang Yuhan. 2017. Study on Data Security Policy Based On Cloud Storage, IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids).

[10] Phillip Rogaway and Mihir Bellare, Introduction to Modern Cryptography, 2005

[11] Pradeep Semwal, Mahesh Kumar Sharma. 2017 (Fall). Comparative study of different cryptographic algorithms for data security in cloud computing, 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA).

[12] "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security. 2011.

[13] Adleman, Leonard M., Rothemund, Paul W.K., Roweis, Sam, and Winfree Erik, (June 10–12, 1996). "On Applying Molecular Computation to the Data Encryption Standard," Proceedings of the Second Annual Meeting on DNA Based Computers. Princeton University.

[14] Ronald Cramer, Victor Shoup,. "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack", 2004.

[15] Dennis Hofheinz and Eike Kiltz, "Secure Hybrid Encryption from Weakened Key Encapsulation," 2007.

[16] Taher ElGamal (1985). "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"

[17] https://www.techopedia.com/definition/1779/hybrid-encryption

Certificate of Publication

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | E-ISSN 2348-1269, P- ISSN 2349-5138

An International Open Access Journal

The Board of

International Journal of Research and Analytical Reviews (IJRAR)

Is hereby awarding this certificate to

Akash Salve

In recognition of the publication of the paper entitled

IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

Published in IJRAR (www.ijrar.org) UGC Approved (Journal No : 43602) & 5.75 Impact Factor

Volume 7 Issue 1 , Date of Publication:March 2020 2020-03-12 10:45:24

PAPER ID : IJRAR2001891

Registration ID : 216328

R.B.Joshi

EDITOR IN CHIEF

UGC and ISSN Approved - International Peer Reviewed Journal, Refereed Journal, Indexed Journal, Impact Factor: 5.75 Google Scholar

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS | IJRAR

An International Open Access Journal / Approved by ISSN and UGC

Website: www.ijrar.org | Email id: editor@ijrar.org | ESTD: 2014

IJRAR | E-ISSN 2348-1269, P- ISSN 2349-5138

Certificate of Publication

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | E-ISSN 2348-1269, P- ISSN 2349-5138

An International Open Access Journal

The Board of

International Journal of Research and Analytical Reviews (IJRAR)

Is hereby awarding this certificate to

Raul Dhruva

In recognition of the publication of the paper entitled

IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

Published in IJRAR (www.ijrar.org) UGC Approved (Journal No : 43602) & 5.75 Impact Factor

Volume 7 Issue 1 , Date of Publication:March 2020 2020-03-12 10:45:24

PAPER ID : IJRAR2001891

Registration ID : 216328

R.B.Joshi

EDITOR IN CHIEF

UGC and ISSN Approved - International Peer Reviewed Journal, Refereed Journal, Indexed Journal, Impact Factor: 5.75 Google Scholar

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS | IJRAR

An International Open Access Journal / Approved by ISSN and UGC

Website: www.ijrar.org | Email id: editor@ijrar.org | ESTD: 2014

IJRAR | E-ISSN 2348-1269, P- ISSN 2349-5138

Certificate of Publication

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | E-ISSN 2348-1269, P- ISSN 2349-5138

An International Open Access Journal

The Board of

International Journal of Research and Analytical Reviews (IJRAR)

Is hereby awarding this certificate to

Yogesh Sauw

In recognition of the publication of the paper entitled

IMPLEMENTATION OF HYBRID CRYPTOGRAPHY SYSTEM ON CLOUD

Published in IJRAR (www.ijrar.org) UGC Approved (Journal No : 43602) & 5.75 Impact Factor

Volume 7 Issue 1 , Date of Publication:March 2020 2020-03-12 10:45:24

PAPER ID : IJRAR2001891

Registration ID : 216328

R.B.Joshi

EDITOR IN CHIEF

UGC and ISSN Approved - International Peer Reviewed Journal, Refereed Journal, Indexed Journal, Impact Factor: 5.75 Google Scholar

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS | IJRAR

An International Open Access Journal | Approved by ISSN and UGC

Website: www.ijrar.org | Email id: editor@ijrar.org | ESTD: 2014

IJRAR | E-ISSN 2348-1269, P- ISSN 2349-5138