Crypto-steganographic Hybrid Blockchain Model for Network Security

B.Tech. Project Report

By

Name of the B.Tech. Students
Sandeep Shaw
Akash Kumar Sen
Surajit Bera
Arijit Mukherjee

Under Supervision of
Dr. Bijoy Kumar Mondal

Department of Computer Sc. and Engineering

Government College of Engineering and Ceramic Technology
Kolkata

May 2022

Crypto-Steganographic Hybrid Blockchain Model for Network Security

A Project Report

Submitted in partial fulfillment of the
requirements for the award of the degree
of

Bachelor of Technology

In

Computer Sc. and Engineering

By

NAME OF THE STUDENTS (with University Roll Number)
Sandeep Shaw(GCECTB-R19-3022)
Akash Kumar Sen(GCECTB-R19-3002)
Surajit Bera(GCECTB-R19-3036)
Arijit Mukherjee(GCECTB-R19-3007)

Department of Computer Sc. and Engineering

Government College of Engineering and Ceramic Technology
Kolkata

May 2022

Name and Roll No. of the Students	Signature of the Students
1. Sandeep Shaw(GCECTB-R19-3022)	
2.Akash Kumar Sen(GCECTB-R19-3002)	
3.Surajit Bera(GCECTB-R19-3036)	
4.Arijit Mukherjee(GCECTB-R19-3007)	

Place:

Date:

Government College of Engineering and Ceramic Technology

73, A. C. Banerjee Lane, Kolkata, West Bengal 700010

……………………………………………………………………

BONAFIDE CERTIFICATE

Certified that this literature survey report titled **Crypto-steganographic Hybrid Blockchain Model for Network Security** is the realistic work carried out by

1. Sandeep Shaw(GCECTB-R19-3022)

2.Akash Kumar Sen(GCECTB-R19-3002)

3.Surajit Bera(GCECTB-R19-3036)

4.Arijit Mukherjee(GCECTB-R19-3007)

who will carried out the project work under **my / our** supervision.

…………………………………… ……………………………………………

Dr. Bijoy Kumar Mondal
SUPERVISOR
Assistant Professor
Department of Computer Science and Engineering
Government College of Engineering and
Ceramic Technology
Kolkata-700010

JOINT SUPERVISOR

(**if any**)

…………………………………… ……………………………………………

Dr. K. Saha Roy
HEAD OF THE DEPARTMENT
Assistant Professor & Head
Department of Computer Science and Engineering
Government College of Engineering and Ceramic Technology,Kolkata

External Examiner

Abstract

The purpose concept of this project work is mainly focused on developing a simple but secure text messaging application that is end-to-end encrypted and provides assurance to the user by securing their data. The idea here is to address two major data security threats that usually make any regular chat application vulnerable, the former is the MITM or Man in the Middle Attack and the latter is an incident of Data Breaching. The Man in the Middle Attack is one of the most common forms of cyber attack the goal of an attack is to steal personal information, such as login credentials, account details, and credit card numbers. In order to tackle this form of cyber vulnerability, we propose to design an algorithm that could easily be used to communicate between the client and server, and even if the data is tapped by any perpetrator it will take billions of years to crack down the information and is safe against any brute force attacks. The other principal motive is to store the encrypted messages in the database server so that the admin who is authorized for such a centralized database can never view the text chat between the sender and the receiver. Even in the case of a Data Breach which is a security violation, in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so or in other terms are unintentional information disclosure, data leak, information leakage, and data spill, the data is still encrypted and the information can't be decoded very easily. Moreover on the server-side if any unauthorized user made an attempt to modify the data then this activity can easily be identified as the text chat between the sender and receiver is stored in a blockchain manner. Overall, this purpose idea promotes significant improvement over the existing concepts in terms of both security features and data integrity solutions related to the messaging chat application from the perspective of the client and server side.

Introduction

We are living in the age of computers and internet. The information on every aspects of our lives are being uploaded and transferred through internet . In a more generalized way internet is a form of computer network and as our data is uploaded and transferred through the computer networks every single minute.Our computer networks must be secured in order to prevent and survive all the third party attacks.This is the phase where the role of network security comes into action.

In this project we have proposed to build a Secure text messaging application using Cryptography and steganography together.

Later on we have also implemented Blockchain technology to store and retrieve the message data in amore secure manner.

In this project we have tried to address two major data security threats that usually make any regular chat application vulnerable, the former is the MITM or Man in the Middle Attack and the latter is an incident of Data Breaching.

Following are the fields that we are going to make use of in order to implement our proposed idea:

Computer Network:

Computer network is a system that helps us to connect and communicate a large number of self-dependent computers in the intention of sharing information and resources or in simpler words when two or more computers are connected together, the entire system of two or more connected computers is called a computer networks. Today's user-centric applications are built on the most popular and widely used form of a computer network called internet.

Network Security:

As mentioned in the last paragraph, each and every computer network shares a large number of information and resources with each other.In order to make a computer network trustworthy and reliable we have to go through three security measures confidentiality, integrity and availability.The measures taken by the application developers and the computer scientists to make confirm these three actions are known as network security.

Attacks:

The three goals of security, confidentiality, integrity and availability can be threatened by some third party unethical measures. Such phenomenons are known as attacks. Attacks can take place in any from like snooping, traffic analysis, unauthorized modification, unauthorized access, data breaching etc. But throughout the project we have decided to create an algorithm that deals with two specific type of attacks, MITM or Man in the Middle Attack and Data Breaching.

Man in the Middle Attack(MITM):

The MITM or Man in the Middle Attack is a general term of when a third person have view or modify access in a conversation between the server and the client. This breaches one of the most important aspects of network security that is confidentiality.

Cryptography:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

In our project we have tried to encrypt a text message using cryptographic hash algorithms.

Steganography:

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

In this project we have tried to use a PNG file as the pseudo non-secret file for hiding the data.

Blockchain:

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

Later on in this project we have also implemented Blockchain technology to store and retrieve the message data in a more secure manner.

Literature Survey

In this section, we provide a brief literature review on recent crypto-steganography and blockchain techniques with a focus on secure data encryption, effective steganography methods, and block-chained data integrity.

Data encryption and Steganography are one of the most widely used techniques which are used to protect data from cyber threats and cybercriminals. Moreover, these techniques of data protection have been proposed by many studies to effectively tackle the problems. The main challenge that was encountered was to generate secure and dynamic encryption and embed this data inside the image effectively. Since LSB steganography is one of the most effective ways to easily embed data to create stego-object. However, this technique comes with a drawback as it is very easy to crack by just obtaining all the least significant bit [1]. Moreover, the length of the message may vary, and therefore if the message is small enough then it would be unnecessary to embed it in a large file on the other hand if the encrypted message is very large then it might not be able to fit completely inside the file. Therefore the main challenge that was faced while designing the solution to this problem was to implement a dynamic image object that will be generated automatically based on the encrypted message unlike providing the fixed or static image.

Apart from Dynamic Image Steganography, the main aim is to provide an encryption algorithm that is secure and could generate a key to decipher the text message. After going through various cryptography concepts [2] the best alternative was to apply Symmetric Key Encryption. The reason to follow this mode of encryption is that in our messaging applications any amount of data may be passed and secondly, since encryption and decryption are done at the user/client end therefore the resource utilization of the algorithm should be less. Hence symmetric encryption is a preferred choice as the encryption process is fast, used when a large amount of data is required to transfer, and resource utilization is low as compared to asymmetric key encryption.

The examples of various Symmetric key encryption are:

- Blowfish
- AES (Advanced Encryption Standard)
- RC4 (Rivest Cipher 4)
- DES (Data Encryption Standard)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

The most commonly used symmetric key algorithms are AES-128, AES-192, and AES-256.

Symmetric key encryption is the encryption method where we use only one key for encrypting and decrypting the data. Out of various symmetric key encryption, the most reliable is the Advanced Encryption Standard 256 (AES) algorithm it includes byte substitution, shifts rows, mixes columns, and adds a round key which is the core implementation. However, in recent times, the new process of attacks is combined for boomerang and rectangle attacks. This uses the weaknesses of a few nonlinear transformations in the key schedule algorithm of ciphers and it can break some reduced-round versions of AES which is its disadvantage [3][4]. In order to overcome this problem, 512 bits symmetric key of the AES algorithm can be used to increase the robustness by keeping the processing time low [5].

After providing data security which is to be delivered from client to server, the next responsibility of the message application is to design an effective data structure that can not only provide easy CRUD operations but also check the integrity of the data whether or not it has been manipulated by adding, removing or updating the database information. In order to implement such a feature, the chat data is stored in a blockchain manner which is one of the most demanding technology. It helps in the verification and traceability of multistep transactions needing verification and traceability. It can provide secure transactions, reduce compliance costs, and speed up data transfer processing. After the client API ask for the encrypted chat data, the server will process the blockchain technology by calculating the data integrity of each chat one by one. The main disadvantage of using blockchain technology is that as the size of the data increase the time complexity to verify every transaction also increases. Therefore in our chat application as the number of user increase, the amount of data also increases linearly so in order to accommodate this blockchain technology, a NO-SQL database is utilized where data is stored in a non-structured form consisting of documents and collection. So if SQL database is used instead of querying the whole database only a particular collection of sender and receiver's data is queried out. Overall the method of storing data is hybrid in nature with the implementation of core blockchain concepts with underlying No-

SQL database frameworks[6]. Since speed is the factor that limits the use of pure blockchain concepts in these applications it is also an important concept apart from security. Therefore the emergence of creating a hybrid model to store data is the feasible option that balances both data integrity by blockchain and speed by using the traditional database approach.

Proposed Method

The idea is to build a messaging app system that provides a secure data transfer from the client to the server and stores that particular data inside the database such that the integrity of data is conserved. The methodology in which the design and analysis of the solution is proposed are:

First of all the sender and receiver credentials for the particular chat will be encoded and hashed as per Secure Hash Algorithms SHA-512 and that hashed data is passed as a key to Advanced Encryption Standard AES-512 which encrypts the message data

The encrypted message is passed as input to our dynamic LSB steganography algorithms. According to the length of the encrypted message, a particular image of given dimensions will be calculated and used for the effective embedding of data inside the image. Then the Stego-object is sent to the server via API.

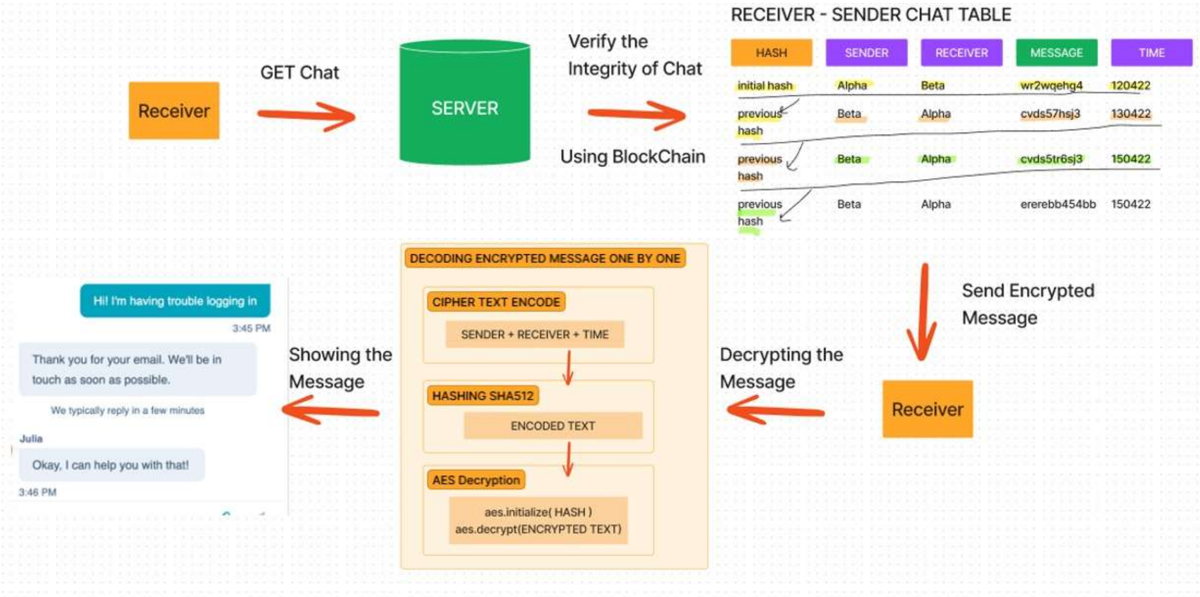
At the server, the message is decoded and the encrypted message is fetched from Stego-object and stored in the database.

While storing the encrypted message in a database, a hybrid model of blockchain and traditional database is used where the current message-id stores the hash (SHA-512) of the previous message-id.

When there is a request in the server to fetch the data of the particular chat between receiver and sender the encrypted message is first verified for data integrity and then the message is sent. On the client-side who receives this data then loops over all the chat and the chat credentials are extracted and encoded to create a hash and simply apply AES-512 decryption by passing the hashed data and the encrypted data to obtain the message back.

In this manner, the data is encrypted and decrypted on the client-side, while the encrypted message is stored on the remote database with a hybrid blockchain technology to authenticate and check tampering in data if it exists. Moreover, image steganography is also implemented which will generate dynamic images based on the encrypted message that can be accommodated very easily and effectively.

Flow Diagram



RECEIVER - SENDER CHAT TABLE

HASH	SENDER	RECEIVER	MESSAGE	TIME
initial hash	Alpha	Beta	wr2wqehg4	120422
previous hash	Beta	Alpha	cvds57hsj3	130422
previous hash	Beta	Alpha	cvds5tr6sj3	150422
previous hash	Beta	Alpha	ererebb454bb	150422

```
aes.initialize( HASH )
aes.decrypt(ENCRYPTED TEXT)
```

Hi! I'm having trouble logging in

3:45 PM

Thank you for your email. We'll be in touch as soon as possible.

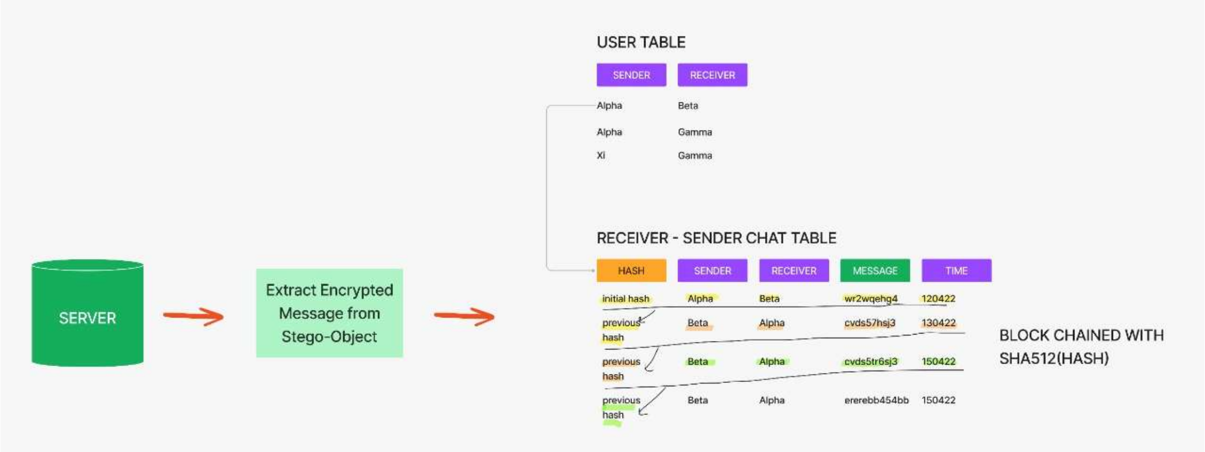
We typically reply in a few minutes

Julia

Okay, I can help you with that!

3:46 PM

Verifying and Decrypting the encrypted message on Receiver's End



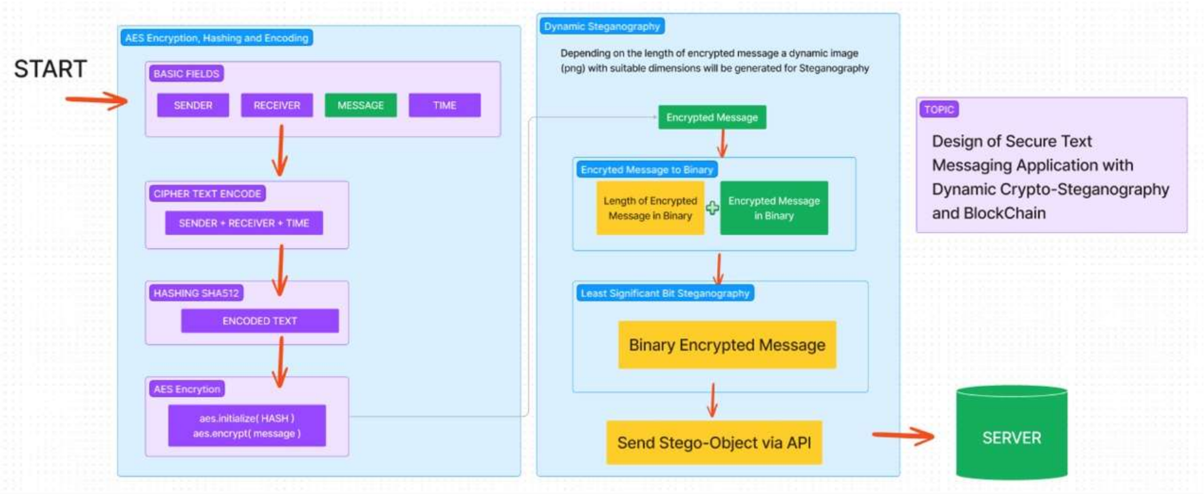
USER TABLE

SENDER	RECEIVER
Alpha	Beta
Alpha	Gamma
Xi	Gamma

RECEIVER - SENDER CHAT TABLE

HASH	SENDER	RECEIVER	MESSAGE	TIME
initial hash	Alpha	Beta	wr2wqehg4	120422
previous hash	Beta	Alpha	cvds57hsj3	130422
previous hash	Beta	Alpha	cvds5tr6sj3	150422
previous hash	Beta	Alpha	ererebb454bb	150422

Fetching Data from Stego-Object and Saving in blockChain manner


START
AES Encryption, Hashing and Encoding
BASIC FIELDS
SENDER
RECEIVER
MESSAGE
TIME
CIPHER TEXT ENCODE
SENDER + RECEIVER + TIME
HASHING SHA512
ENCODED TEXT
AES Encrytion
aes.initialize(HASH)
aes.encrypt(message)
Dynamic Steganography
Depending on the length of encrypted message a dynamic image (png) with suitable dimensions will be generated for Steganography
Encrypted Message
Encryted Message to Binary
Length of Encrypted Message in Binary
Encrypted Message in Binary
Least Significant Bit Steganography
Binary Encrypted Message
Send Stego-Object via API
TOPIC
Design of Secure Text Messaging Application with Dynamic Crypto-Steganography and BlockChain
SERVER

Sender Sending Message to Receiver

References

1. Yeuan-Kuen Lee, Graeme Bell, Shih-Yu Huang, Ran-Zan Wang, and Shyong-Jian Shyu: An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding (2009)

2. Applied Cryptography Protocols, Algorithms, and Source Code in C, A book by Bruce Schneier

3. H. Gilbert and M. Minier, “A collision attack on seven rounds of Rijndael”, Proceedings of the 3rd AES Candidate Conference, (2000) April: 230-241.

4. B. Schneier, “The GOST Encryption Algorithm”, Dr. Dobb’s Journal, v.20, n. 1, (1995) January: 123-124.

5. "DATA SECURITY USING 512 BITS SYMMETRIC KEY BASED CRYPTOGRAPHY IN CLOUD COMPUTING SYSTEM", Bijoy Kumar Mandal, Debnath Bhattacharyya and Xiao-Zhi Gao, (2019): 3-4

6. Efficient High-Performance FPGA-Redis Hybrid NoSQL Caching System for Blockchain Scalability, Abdurrashid IbrahimSankaMehdi HasanChowdhuryRay C.C.Cheung, 2021