International Journal of Research in Engineering, Science and Management
Volume-3, Issue-6, June-2020
www.ijresm.com | ISSN (Online): 2581-5792

Secure Messaging Application Using Blockchain Technology

Prashant Madhav Sonawane[1*], Shruti Sangmesh Hiremath[2], Rohit Sanjay Rathod[3], M. J. Gaikwad[4]

[1,2,3]*Student, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India*

[4]*Professor, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India*

*Corresponding author: prashantsonawane3398@gmail.com

***Abstract*: The convergence that brought with the globalizing world extremely affects the network and also the communication sectors. principally closed supply and centralized systems area unit used for network and communication. This contradicts with the knowledge security principles and privacy. These centralized systems cannot totally meet the conception of clear, reliable, quick and uninterrupted communication. Distributed, decentralized and conjointly clear communication is feasible with the blockchain technology. during this study, a communication application that relies on blockchain technology is projected. Application options and potential advantages area unit mentioned.**

***Keywords*: Public ledger, AES Encryption, Military Grade Encryption, Public-private key.**

1. Introduction

Communication is Associate in Nursing inevitable and vital dimension of the human life. The evolution of the communication from the past to these days, has reached a world space through the medical aid. the information that offer name to our era, gave the chance to gather giant knowledge within the communication sector; creating this the middle of attention by the central systems like states and corporations that manage the world. This international power is monopolized by centralized systems with closed (proprietary) computer code. Non-transparent, centralized applications square measure inadequate as we have a tendency to square measure in Associate in Nursing era that the private and structure info security is vital. Controlled and centralized systems don't satisfy the flexibleness for the user. The centralized platforms additionally do have one purpose of failure. these days we have a tendency to upset varied on-line services, wherever everyone deals with varied technologies. These technologies square measure created for folks to create our access to new world simply. there's tremendous use of on-line applications, websites that need giant storage. giant knowledge is handled by the net systems. the gathering of knowledge in whole world is regarding 2 hundredth in previous few years. the information is captured from user, controlled by the systems and operations square measure performed on knowledge. It needs a lot of system accuracy and protection to non-public knowledge. Ex. Email, WhatsApp, Instagram, Facebook, Bank transactions, time period estate etc. however the person is unknown regarding the information, wherever and the way it's used wherever it's hold on or whether or not {the knowledge the info the information} is handled by some organizations for his or her own use or data is been hacked by different person. Since the protection towards the private knowledge is been decreasing day by day. Example- Facebook one among the massive on-line social network collected three hundred petabytes of user knowledge throughout its beginning. These results in lawlessly accessing personal knowledge for his or her own purpose while not having rights on that. Decentralized and clear platforms should be developed as an answer. Blockchain technology could be a candidate for that. The blockchain technology empowers users to regulate their own digital identity, share and communicate with trust. Communication applications that square measure supported blockchain technology; use uneven ciphers and consensus based algorithms and exploitation P2P network structure. These applications will solve the wants of the user. during this study, Associate in Nursing application known as Cryptochat is projected that could be a blockchain based mostly communication application; the operating principles and therefore the potential advantages square measure mentioned well.

A. Motivation

Now-a-days social media is extremely vital for communication. The individuals share varied data, documents and their personal information victimization social media. Due to this, the data shared among the individuals may be hacked or accessed by a trespasser. To avoid this a secure application ought to be developed so the message may be transferred firmly to the proper person. The documents and information may be shared victimization varied technologies.

B. Problem definition and objectives

The people come across various security problems the aim of the project is to transfer the message to the right person securely.

Vision:

- Safety of Personal data

- Secure Transmission
- High Storage

Issue:

- Unsecured data transfer
- *E*asily Hackable

Solution:

- To develop a system which transfer a data between users safely.

Objectives:

The core objective of the project is to transfer the data securely across the users. This can be done by using cryptographic techniques to secure the data, which is used for communicating between the members of the blockchain. This communication leads to transfer of sensitive data from a valid sender to a valid receiver. The blockchain provides these cryptographic functions along with a proper storage. The data is always added or appended to blockchain. The data cannot be deleted or updated.

C. Project Scope and Limitation

Scope:

The purpose of this technique is to produce security to the user's personal information and messages that square measure transferred between the users. Communication is associate inevitable and necessary dimension of the human life. The evolution of the communication from the past to nowadays, has reached a worldwide space through the medical care. Communication applications that square measure supported blockchain technology; use uneven ciphers and consensusbased algorithms and mistreatment P2P network structure. These applications will solve the requirements of the user. Cryptochat may be a blockchain based mostly communication

Limitations:

The limitation is that system requires a stable net connection for connecting to API server.

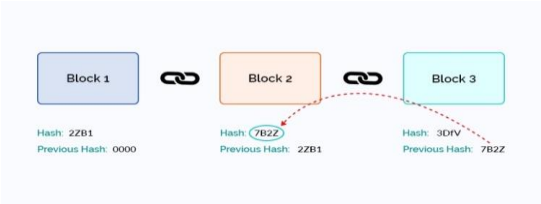
D. Methodologies and Problem Solving

- Blockchain Technology

A blockchain could be a growing list of records, referred to as blocks, that square measure connected victimisation cryptography every block contains a cryptographical hash of the previous block, a timestamp, and dealings knowledge. Blockchain could be a decentralized, distributed, public ledger. Blockchain is outlined as assortment of blocks. Block is the tiniest unit of blockchain that records recent transactions. each transactions square measure classified and hold on on a public ledger. In blockchain, the primary block is termed as genesis block. After genesis block the block is additional consequently by victimisation hash of genesis block. Blockchain technology the most recent word in money service hasthe capability to store, share and influence the transactions in an exceedingly totally different manner. The Satoshi Nakamoto bought Bitcoin and Blockchain over paper in July 2009, the primary blockchain was introduced and have become well-liked. Blockchain technology is that the one United Nations agency builds a trust between 2 member or 2 entities. once there's a digital dealing between 2 persons then no a 3rd party concerned in dealings system. Blockchain provides additional security to the info.

Blocks:

Block consists of data and hash of previous block.



- RSA Encryption:

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.

Algorithm The RSA algorithm holds the following features,

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers. • The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key

2. Literature Survey

Table 1
Literature survey

S. no.	Paper	Advantages	Disadvantages
1.	Secure Communication using Blockchain.	Provides smart security, Handling events between multiple user.	Complex design, Chat is slow for several user.
2.	Decentralizing Identity with Privacy for Secure Messaging.	Simple logic is employed.	When the user authorizes the requests ahead of time or on a regularly occurring basis, it is also a danger If user's knowledge is deleted then it's unable to trace it.
3	A Secure Private Instant Messenger.	Simple UI Uses SHA-256 Algorithm	Storage Issue Unable to handle Load Reduces efficiency

3. Software Requirement Specification

A. Project Scope

The purpose of this method is to supply security to the user's personal information and messages that square measure transferred between the users. Communication is associate inevitable and necessary dimension of the human life. The evolution of the communication from the past to these days, has reached a world space through the digitalisation. Communication applications that square measure supported blockchain technology; use uneven ciphers and consensusbased algorithms and victimisation P2P network structure. These applications will solve the requirements of the user. Cryptochat could be a blockchain primarily based communication application.

B. AAssumption and Dependencies

Assume:

We have a tendency to assume that someone ought to have an honest web affiliation obtainable.

Dependencies:

We have a tendency to square measure addicted to a decent web affiliation

C. Functional Requirement

Internet:

User ought to have a stable net association in order that a system are going to be able to send sure necessary knowledge to cloud.

Application:

Cryptochat should be properly put in in each sender and receiver.

Software Interfaces:

- Operative System: we've got chosen automaton package for its best support and user-friendliness.
- Java: we've got chosen Java artificial language that is intended with fea- tures to facilitate knowledge analysis and visualisation.

D. Non Functional needs

- Performance Requirement:

The system should offer response in minimum time i.e. the delay ought to be less. this is often a vital demand for America since the person are going to be traversing in between area supported systems instruction therefore delay ought to be as minimum as potential.

- Safety Requirement

Safety of someone and of an information is of a key concern. data ought to be firmly transmitted to server with none changes in data and therefore the person mustn't col- lide with any obstacle whereas traversing in rooms.

- Security Requirement

Any modification to be done to information ought to be done by solely a certified person.

- Availability

If the web service gets noncontinuous whereas causing data to the server, the infor- mation will be send once more for verification.

- Usability

As the system is straightforward to handle and navigates within the most expected method with no delays. therein case the computer program reacts consequently and transverses quickly between its states.

- Maintainability

The system shall give the potential to back-up the information.

- Robustness

The system won't be dampened simply and cannot whole have an effect on by one application failure.

E. System Requirements

Database Requirements

- Database: SQL

Technology

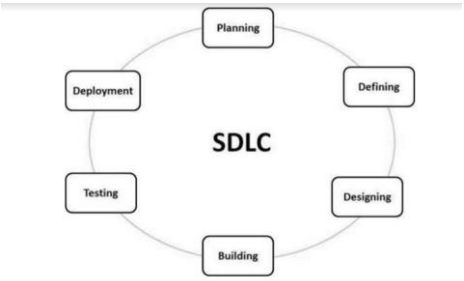
- Blockchain

Software Requirements

- Platform: Android Studio
- Coding Platform: Java

F. Analysis Model

SDLC model to be applied the repetitious SDLC model doesn't would like the total list of necessities before the project starts. the event method might begin with the wants to the useful half, which might be swollen later. the method is repetitive, permitting to create new versions of the merchandise for each cycle. each iteration includes the event of a separate element of the system, and afterward, this element is adscititious to the useful developed earlier. Speaking with maths nomenclature, the repetitious model may be a realization of the sequent approximation method; meaning a gradual closeness to the planned final product form. The key to a winning use of associate degree repetitious code development life cycle is rigorous validation of necessities, and verification and testing every of every} version of the code against those necessities among each cycle of the model. because the code evolves through consecutive cycles, tests should be recurrent and extended to verify every version of the code.



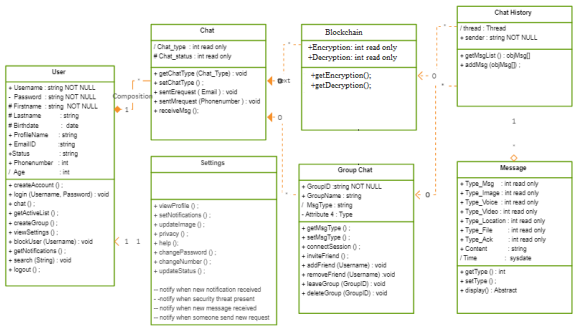
International Journal of Research in Engineering, Science and Management
Volume-3, Issue-6, June-2020
www.ijresm.com | ISSN (Online): 2581-5792

4. System Design

The system design consists of the system elements as sender, receiver, nodes, network, Blockchain network.

- Sender: The sender sends the information to the receiver. First, the data is encrypted and transport the blockchain network.
- Nodes: The nodes on the network ar the validators of the transmittal knowledge.
- Blockchain: The blockchain network then tranfers knowledge to the blockchain information.
- Information: The Record of transferred knowledge is keep on blockchain.
- Receiver: the information is decrypted on receiver facet. The receiver receives the information from the system.

A. *Class Diagram*



A class diagram may be a style of static structure diagram that describes the structure of a system by showing the system's categories, their attributes, operations (or methods), and also the relationships among objects.

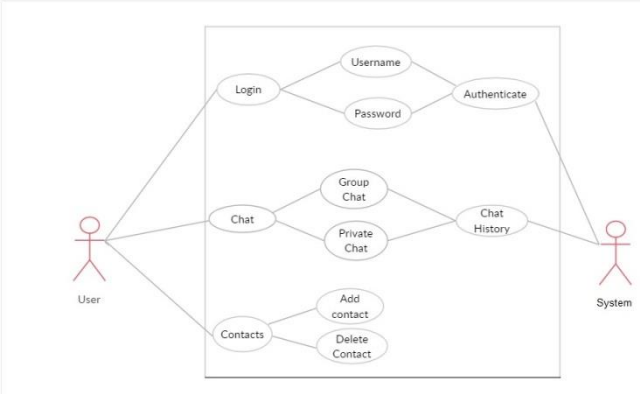
The category diagram is that the main building block of object-oriented modeling. it's used for general abstract modeling of the structure of the appliance, and for elaborated modeling translating the models into programming code. category diagrams can even be used for information modeling. [1] The categories in a very category diagram represent each the most parts, interactions within the application, and also the categories to be programmed.

In the diagram, categories are diagrammatic with boxes that contain 3 compartments:

- The highest compartment contains the name of the category. it's written in daring and targeted, and also the 1st letter is capitalized.
- The center compartment contains the attributes of the category. they're left-aligned and also the 1st letter is little.
- Very cheap compartment contains the operations the category will execute. they're additionally left-aligned and also the 1st letter is little.

a) User: it's named the registered user to the system. User category contains attributes like forename, Last name, sign etc.
b) Chat: Chat is completed by exploitation registered sign solely.
c) Setting: This category has functions like privacy, notifications, amendment passwords. conjointly it inform the user once message is arrived.
d) Blockchain: This category contains the cryptography and cryptography algorithmic rule.
e) Cluster chat: we are able to forms the teams by exploitation multiple users.
f) Chat history: It stores the chat histories of user.
g) Message: we are able to send completely different form of messages within the style of text, videos, and images.

B. *Use case Diagram*



A use case diagram at its simplest may be an illustration of a user's interaction with the system that shows the connection between the user and also the totally different use cases during which the user is concerned. A use case diagram will determine the totally different the various kinds of users of a system and also the different use cases and can usually be in the middle of alternative kinds of diagrams furthermore. the employment cases area unit painted by either circles or ellipses. whereas a use case itself would possibly drill into plenty of detail concerning each risk, a use-case diagram will facilitate offer a higher-level read of the system. it's been same before that "Use case diagrams area unit the blueprints for your system". they supply the simplified and graphical illustration of what the system should truly do. the aim of the employment case diagrams is solely to supply the high level read of the system and convey the necessities in laypeople's terms for the stakeholders. further diagrams and documentation may be wont to offer an entire purposeful and technical read of the system.

Our project has 2 actors:

- User: User will login to the system victimisation username and parole. User will type the teams of multiple user or he/she will do individual chat conjointly.
- System: System attest the user. If username or parole isn't approved or correct then user cannot login to the system.

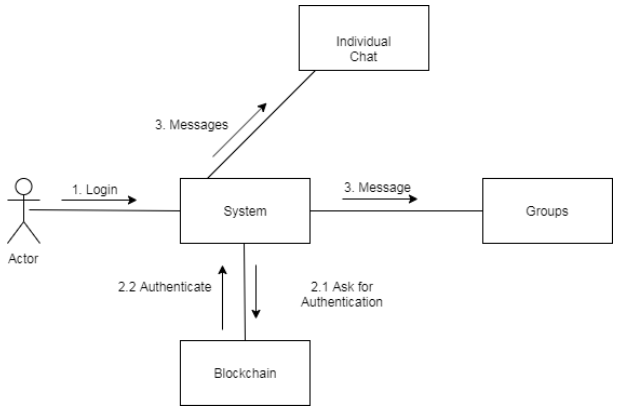
C. Activity Diagram

An activity diagram portrays the management be due a begin purpose to an end purpose showing the assorted call ways that exist whereas the activity is being dead. we are able to depict each successive process associate degreed simultaneous process of activities victimisation an activity diagram. they're utilized in business and method modelling wherever their primary use is to depict the dynamic aspects of a system.

An activity diagram is employed to model the progress portraying conditions, constraints, successive and simultaneous activities.

An activity diagram are often accustomed illustrate a business method (high level implementation) to a standalone formula (ground level implementation).

D. Communication Diagram



Communication diagram (called collaboration diagram in UML one.x) could be a reasonably UML interaction diagram that shows interactions between objects and/or elements (represented as lifelines) mistreatment sequenced messages in an exceedingly free-form arrangement.

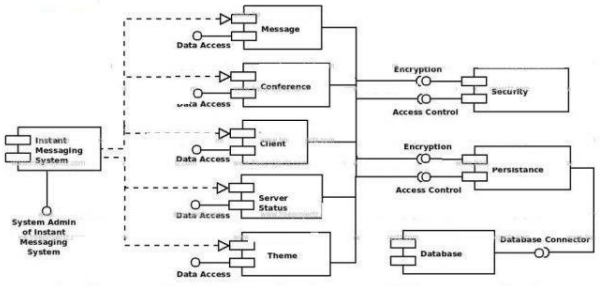
Communication diagram corresponds (i.e. might be reborn to/from or replaced by) to a straightforward sequence diagram while not structuring mechanisms like interaction uses and combined fragments. it's additionally assumed that message passing (i.e., the order of the receptions square measure totally different from the order of causing of a given set of messages) won't surface or is impertinent.

User login to the system. System raise blockchain for attest the user. Blockchain attest the user. If user is allowed then solely user will login to the system. when the authorization then solely system enable the user to try and do cluster chat or individual chat.

E. Component Diagram

Component diagram may be a special quite diagram in UML. the aim is additionally totally different from all alternative diagrams mentioned up to now. It doesn't describe the practicality of the system however it describes the parts wont to create those functionalities.

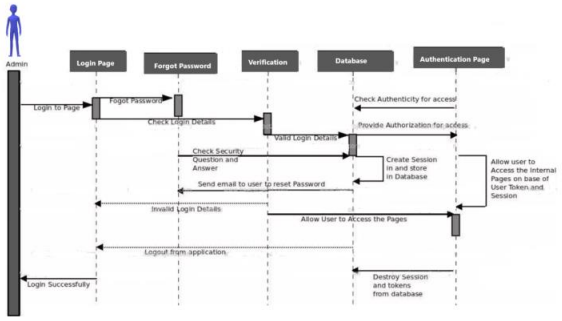
Therefore, from that time of read, part diagrams square measure wont to visualize the physical parts in an exceedingly system. These parts square measure libraries, packages, files, etc.



Part diagrams may be represented as a static implementation read of a system. Static implementation represents the organization of the parts at a selected moment. the aim of the part diagram will be summarized as,

- Visualize the parts of a system.
- Construct executables by victimization forward and reverse engineering.
- Describe the organization and relationships of the parts.

F. Sequence Diagram



UML Sequence Diagrams square measure interaction diagrams that detail however operations square measure administered. They capture the interaction between objects within the context of a collaboration. Sequence Diagrams square measure time focus and that they show the order of the interaction visually by mistreatment the vertical axis of the diagram to represent time what messages square measure sent and once.

Sequence Diagrams captures:

- The interaction that takes place AN exceedingly|in a very} collaboration that either realizes a use case or an operation (instance diagrams or generic diagrams)
- High-level interactions between user of the system and also the system, between the system and alternative systems, or between subsystems (sometimes called system sequence diagrams)

Purpose of Sequence Diagram

- Model high-level interaction between active objects AN exceedingly in a very system.
- Model the interaction between object instances inside a collaboration that realizes a use case.
- Model the interaction between objects inside a

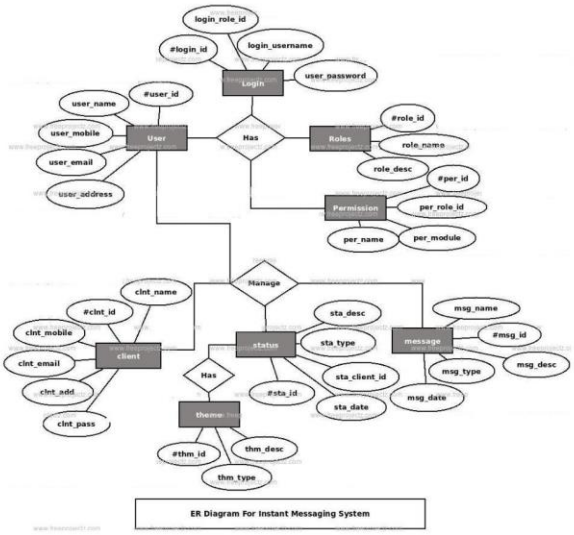
collaboration that realizes an operation.

- Either model generic interactions (showing all doable methods through the interaction) or specific instances of an interaction (showing only one path through the interaction)

Sequence of the system:

a) User login to the system using username and password.
b) System checks the login detail of user.
c) System valid the details of the user.
d) It checks the details of user in the blockchain.
e) If details is present in database then only user can access the pages of the system.
f) If all the details are correct then only user can successfully login to the system otherwise it shows the invalid login and system destroy the session.

G. ER Diagram



Entity Relationship Diagram, additionally called ERD, ER Diagram or ER model, could be a variety of structural diagram to be used in information style. associate ERD contains completely different symbols and connectors that visualize 2 vital information: the key entities inside the system scope, and therefore the inter-relationships among these entities. And that's why it's referred to as "Entity" "Relationship" diagram (ERD).

ER Diagram in information engineering guarantees you to provide high-quality information style to use in information creation, management, and maintenance. associate ER model additionally provides a way for communication.

Our system has following entities and their attributes:

a. User: It has attributes like phone number, username, email id etc.
b. User can login to the system with the help of username or password.
c. User has roles like id, name etc.
d. User can sends messages in the form of text, videos or images.

5. Project Plan

A. Project Estimates

Time Estimators:

The initial time estimate for the complete implementation of the primary objectives is 40-45 days depending on the schedule of the developers. The secondary objectives require an additional of 25 days to be completed. Also, depending on the stage of development, the testing and debugging would require an additional of 15 days.

Project Resources:

- *People*
  1. Prashant Sonawane (Developer)
  2. Shruti Hiremath (Developer)
  3. Rohit Rathod (Tester)
- *Hardware*
  1. RAM 2 GB
  2. Processor - i5 8th Gen, 2.0 GHz
  3. Mobile Phone
- *Software*
  1. Android OS
  2. Java
  3. Hyperledger

B. Risk Management

Risk Identification:

1. Hardware failure
2. Zero Speed of Internet Connection

Risk Analysis:

- *Hardware failure:* Any of the hardware component may or may not work because of unforeseeable or unavoidable reasons.
- *Reduced or zero speed of Internet connection:* System requires an Internet con- nection which has good speed

Table 2
Risk table

Sr. No.	Risk Description	Probability	impact		
			Quality	Overall	
1	Hardware Failure	Low	Low	high	Medium
2	Zero Speed of Internet Connection	Medium	Low	high	High

Table 3
Risk Probability definitions

Probability	Value	Description
High	Probability of occurrence is	> 75%
Medium	Probability of occurrence is	26-75%
Low	Probability of occurrence is	< 26%

Table 4
Risk Impact definitions

Risk ID	1
Risk Description	Hardware failure
Category	Development Environment
Source	Software requirement specification document
Probability	Low
Impact	High
Response	Mitigate
Strategy	Replace the failed piece hardware
Risk Status	Identified
Risk ID	2
Risk Description	Reduced or zero speed of Internet connection
Category	Requirements
Source	Software requirement specification document
Probability	Medium
Impact	High
Response	Mitigate
Strategy	Connect to High Speed Internet Connection WiFi
Risk Status	Identified

C. Project Schedule

Project task Set

Major tasks in the project stages are:

- Task 1: Finalization of Domain
- Task 2: Literature Survey
- Task 3: Application and objectives
- Task 4: Platform/Technology Selection
- Task 5: Internal Presentation 1
- Task 6: Study of Algorithms
- Task 7: Mathematical Model
- Task 8: Software Requirements Specifications
- Task 9: UML Diagrams
- Task 10: Problem Definition using Blockchain
- Task 11: System Architecture
- Task 12: Testing Phase
- Task 13: Internal Presentation 2
- Task 14: Report Preparation

D. Team Organization

Team Organization/Team Structure:

Our Strategy is to divide the tasks equally amongst four of us. We decide a deadline for each task. In the end we combine the results of individuals into one single outcome.

Management reporting and communication:

We report progress of our project to our project guide once a week. We show our weekly status to our guide and incorporate the necessary changes. The project members communicate among themselves in case any suggestions are required while performing or executing any tasks.

6. Project Implementation

A. Overview of Project Modules

The traditional navigation system consists of three main modules as discussed earlier.

1. Registration 2. Communication 3. System

1) Registration

- User have to be compelled to registered on the applying.
- When registration distinctive public and personal secret's generated for every user.

2) Communication

- Every user has distinctive non-public and public key.
- The general public secret's shared with alternative user and personal secret's command with user. it's not shared with others.
- During this project we tend to victimisation RSA algorithmic program for encoding and cryptography

B. RSA algorithm

1. Generate the RSA modulus The initial procedure begins with choice of 2 prime numbers specifically p and letter, then conniving their product N, as shown − N=p*q Here, let N be the desired sizable amount.
2. Derived range (e) take into account range e as a derived range that ought to be larger than one and fewer than (p-1) and (q1). the first condition are going to be that there ought to be no divisor of (p-1) and (q-1) except one.
3. Public key the desired combine of numbers n and e forms the RSA public key and it's created public.
4. Non-public Key non-public Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows − erectile dysfunction = one mod (p-1) (q-1) The on top of formula is that the basic formula for Extended geometrician algorithmic program, that takes p and letter because the input parameters

C. Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax − C = Pe mod n

D. Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as − Plaintext = Cd mod n

3) System

- Consider a sender who send a message to receiver then the message is first encrypted using public key.
- The encrypted data send over the blockchain network.
- The blockchain network verify and validate the sender and the receiver.
- After the validating the message is stored in block.

- After validation data is send to the receiver.
- The receiver decrypt using his private key.

E. Tools and Technologies used

1) Blockchain

Blockchain may be a localised, distributed, public ledger. Blockchain is outlined as assortment of blocks. Block is the tiniest unit of blockchain that records recent transactions. each transactions ar classified and hold on on a public ledger. In blockchain, the first block is termed as genesis block. when genesis block the block is else consequently by victimization hash of genesis block. Blockchain technology the newest word in monetary service has the capability to store, share and affect the transactions during a totally different manner. The Satoshi Nakamoto bought Bitcoin and Blockchain over paper in July 2009, the primary blockchain was introduced and have become standard. Blockchain technology is that the one UN agency builds a trust between 2 member or 2 entities. once there's a digital dealing between 2 persons then no a 3rd party concerned in dealing system. Blockchain provides additional security to the info. The aim of blockchain is to make trust among the humans. The trust ought to be ride each the perimeters in dealing as between producer and shopper. The blockchain system is built for rising the society, by reducing the frauds as prohibited accessing to information and hacking the system. The blockchain is employed to make the primary crypto currency that is Bit coin. There are numerous applications on wherever we will have blockchain technology addressing the dealing system. The blockchain is updated by itself in every 10 minutes.

2) Distribited Ledger

A distributed ledger (also referred to as a shared ledger or distributed ledger technology or DLT) may be a agreement of replicated, shared, and synchronised digital knowledge geographically unfold across multiple sites, countries, or establishments. there's no central administrator or centralized knowledge storage.

3) Peer to peer network

Peer-to-peer network is blockchain is employed to possess a distributed ledger. So that every person in blockchain is connected to different by means that of network that is peer to look. The peer provides disk storage and network information measure on the market to every node. Therefore, all the information is shared by exploitation the network. Distributed machines on peer to look network helps to keep up consistency of their public ledger. This network uses digital signature to validate the transactions.

4) Storage system within the blockchain

Blockchain technology creates redistributed information storage and provides the selection to the user to use it. Decentralization of blockchain offers numerous edges like enable the user to hold on and downloads the file from multiple nodes rather than one server. information is hold on on multiple nodes that area unit distributed globally; there's no central authority to manage these nodes. Also, it will increase security and reduces the value thanks to redistributed file storage. information is hold on by the licensed user in encrypted and therefore the user World Health Organization has the key will solely decipher it and access.

F. Blockchain Working

The blockchain provides higher security to the storage system. the info once inserted within the block can't be modified or deleted. Additionally, the info can't be updated within the system. A ledger could be a list of transactions right from the beginning of blockchain. Block holds recent copy of ledger that is shared with every member of blockchain over the distributed network. Once the block is verified it becomes a relentless a part of blockchain. mistreatment the scientific discipline functions the info is valid and keep on ledger within the block. To confirm the all transactions responsibility. Block time is outlined because the time taken by the network to feature a block into the blockchain. The block time for bitcoin is ten minutes. In cryptography the info in encrypted and a hash code is formed for each single dealings. Blockchain technology is formed for industrial transactions. the primary suburbanised cryptocurrency that is formed mistreatment blockchain is Bitcoin. nowadays varied establishments area unit dynamical their transactions systems into blockchain based mostly system. this is often thanks to the reliable and versatile nature of the blockchain. The blockchain technology involves dealings to keep up server networks referred to as 'nodes'. the pc system that holds blockchain area unit referred to as nodes. The copy of the ledger is distributed to the peer-to-peer network off the blockchain. each system has Associate in Nursing updated duplicate of the ledger on the system. The transactions of the blockchain area unit valid by nodes. If the transactions area unit valid then the block is added to the ledger. The blockchain makes it simple to use good contracts like embedded contracts in pc codes that will implement themselves mechanically on the incidence of assorted events. The blockchain provides high security to private information by mistreatment hashing technique. the most advantage of blockchain area unit

G. Data Ownership:

The Blockchain framework mainly ensures that the user can control and own their data. This system makes the user, the owner of their own data with permissions.

H. Data Transparency

The user is made completely transportable to know where her/his data is being collected and accessed.

I. Android Studio

Android Things permits you to experiment with building devices on a trustworthy platform, while not previous information of embedded system design:

- Develop mistreatment the mechanical man SDK and mechanical man Studio.
- Access hardware like displays and cameras natively

through the mechanical man framework.

- Connect your apps with Google services.
- Integrate further peripherals through the Peripheral I/O arthropod genus (GPIO, I2C, SPI, UART, PWM) Use the mechanical man Things Console to push over-the-air feature and security updates

Android Things extends the core mechanical man framework with further arthropod genus provided by the items Support Library, that permits you to integrate with new varieties of hardware not found on mobile devices.

Developing apps for embedded devices is completely different from mobile during a few necessary ways that such as:

More versatile access to hardware peripherals and drivers than mobile devices

- System apps don't seem to be gift to optimize startup and storage necessities.
- Apps square measure launched mechanically on startup to immerse your users within the app expertise.
- Devices expose only 1 app to users, rather than multiple like with mobile devices.

J. Server Socket

Socket programming facilitates association of 2 nodes on a network that will communicate with one another. One socket that conjointly called (node) listens on a selected port at AN science, whereas alternative socket reaches bent the opposite to make an association. Server develops the auditor socket whereas shopper reaches bent the server. they're the important backbones behind net browsing. In easy words there's a server and a shopper. Socket programming at first starts by commerce the socket library and creating a straightforward socket. Sockets offer the communication mechanism required for communication between 2 computers victimization communications protocol. A shopper program creates a socket at its facet and tries to attach that socket to a server. once the association is formed, the server creates a socket object on its facet. The shopper and therefore the server will currently communicate by writing to and reading from the socket. A socket is one end of a two-way communication link between the server and shopper programs running on the network. A socket range to a port variety in order that the communications protocol layer will establish the applying that information is destined to be sent to. A protocol stack, these days typically provided by the package may be a set of services that permit pro- cesses to speak over a network victimization the protocols that the stack implements. the applying programming interface (API) that programs use to speak with the pro- tocol stack, victimization network sockets, is termed a socket API. A server includes a bind() methodology that binds it to a selected science and port in order that it will hear incoming requests on it science and port. A server conjointly implements a listen() methodology that permits the listen mode on the server. The server listens to incoming connections. ultimately the server implements AN accept() and close() methodology. The settle for methodology initiates a reference to the shopper and therefore the shut methodology closes the reference to the shopper.

7. Software Testing

A. Types of Testing

We use software package testing methodologies whereas execution program or application with the intent of finding the software package bugs. it's conjointly necessary method of verifying and validating that the software package program or application or product have met the business and technical demand that target-hunting it's style and development.

B. Goals and Objective

Finding defects which can get created by the coder whereas developing the An- droid application. Gaining confidence in and providing data concerning the extent of quality. to forestall defects. to form certain that the top result meets demand. to make sure that it satisfies the SRS that's System demand Specification. to achieve confidence of shoppers by providing them quality product.

C. Types of Testing

a) Integration testing: code integration testing is that the progressive integration testing of 2 or a lot of integrated code parts on one platform to supply failure caused by interface defects. The task of the combination check is to ascertain that parts or code applications, e.g. parts in an exceedingly code or - one maximize - code applications at the corporate level - move while not error.

b) Functional Testing: useful tests offer systematic demonstrations that functions tested area unit on the market as such that by business and technical necessities, system documen- tation and user manuals. Organization and preparations of useful tests is targeted on necessities, key functions, or special check cases. additionally, systeatic coverage prede- punished processes, and consecutive method should be thought-about for testing. Before useful testing is complete, extra tests area unit known and also the effective worth of current tests is decided.

c) Black Box Testing: Black-box testing could be a technique of code testing that examines the practicality of Associate in Nursing application while not peering into its internal structures or workings. This technique of check will be applied just about to each level of code testing: unit, inte- gration, system and acceptance. it's generally observed as specification-based testing.

D. Test case and test result

Table 5
Test cases

Sr.	Test	Expected result	Actual result	Status
1	Registration of user	User must be successfully registered	User is successfully registerd	Pass
2	Sign in of user	After the correct information user must ne sign in	User is sign in to app	Pass
3	Chat	Minimum 2 user is available for chat	Message is sent between 2 user	Pass
4	Group	Group can be created between multiple user	Group is created	Pass
5	Chat history	User can able to see his old chat	User can access the old chat	Pass
6	Chat delete	User can able to delete his own chat	Chat is deleted	Pass
7	Image	Image can be sent	Image is sent	Pass
8	Profile picture	User can set his profile picture	Profile picture is set	Pass
9	Emoji	User can send the emoji	Emoji is sent	Pass

8. Conclusion

A. Conclusion

In each centralized system the user information square measure accessed by organizing system. These information square measure keep in information of system and they're not secured. Anyone will simply hack the system and access the personal details of members within the system. The blockchain system provides the answer on this downside. It collects data of user and permits the user to possess management on their own information. Each user has his own non-public and public keys for group action. Each user shares his public key over the suburbanized, distributed, public ledger on blockchain therefore nobody will access the main points of anyone simply because it is in key kind. Since whereas transactions the hash code square measure generated and supplemental on ledgers. Blockchain provides a high security to the non-public information of user and also as on the general public network of user. Since, the details square measure extremely secured on blockchain. The laws and regulation systems may be coded into blockchain. In some things the ledger act as a legal proof just in case of unauthorized transactions.

In a conclusion, hash formula is in a position to assist secure speech communication at intervals computer network by its application of hashing formula and personal nature. the applying primarily ‘disguises’ the text before it's send across the network creating it protected against the read of attackers. Most of knowledge sent by users is confidential.

In this case, security in transmission information or data is required to shield from unauthorized person. during this analysis hashing formula was applied associate degreed enforced by developing an IM application. This IM application additionally was tested and information transmission safer compared to information transmission while not hashing formula.

B. Future Work

- The system may be extended to share every type of documents videos and pictures.
- The users will audio and video decision to every alternative.
- The cluster admin will have authoriries to send the message on the cluster chat.
- The stickers may be extract and shared on the chat.
- Mistreatment this application payment may be done.

C. Application

The projected system can perform these tasks:

- Folk will simply access the appliance.
- This application is often used for varied institutes and organizations.

References

[1] B-money. (1998). Retrieved from http://www.weidai.com/bmoney.txt
[2] Big data, for better or worse: 90% of world’s data generated over last two years. (2013). ScienceDaily.
[3] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From Bitcoin to Cybersecurity: A Comparative Study of Blockchain Application and Security Issues, (61471129), 975–979.
[4] Double-spending. (n.d.). https://en.bitcoin.it/wiki/Double-spendingKharif, O. (n.d.). CryptoKitties Mania Overwhelms Ethereum Networks Processing.
[5] Ali, M. (2017). Blockstack Token Whitepaper.
[6] Ali, M., & Freedman, M. J. (2017). Blockstack Technical Whitepaper.
[7] Ali, M., Nelson, J., Labs, B., Shea, R., Labs, B., Freedman, M. J. Freedman, M. J. (2016). Blockstack: A Global Naming and Storage System Secured by Blockchains.