Department of Computer Science and Business Systems

F-CHAT: Decentralized End to End Encrypted Chat System

THE TRULY FREE CHAT

F-CHAT

Submission By:

Aditya Adiga – 01JST19CB001

Guided By:

Dr. Manju N Dept of ISE , JSSSTU Mysuru

Table of contents

Abstract

This is the implementation of the concept of Decentralization in its true form.

Here we use a Chat System which is built on top of a database which is distributed across a number of devices and uses resources provided by those devices and uses that to run the application thus removing the need of a centralized database.The real reason to use decentralized database is because it provides security in the best form when it is paired with end to end encryption making it very tedious for an attack to disintegrate the system.

Introduction

Integrity of data and security of a product is considered to be the top priority.

Considering the recent developments in the field of blockchains and decentralized ledger technology, security and data integrity of a system can be maintained feasibly.

The Chat system which is in use now uses a centralized database to store the all the data

which is used for the purpose of communication between the two parties.Even though the data is stored securely by encrypting the data using modern cryptography.In case the database is compromised on exposure to some external factors, then the whole database is at a risk of being compromised.This product solves the problem by storing the data on a decentralized system and also providing the end-to-end encryption thus making the chat system more secure.

Literature Survey

In our quest to better understand network traffic dynamics,we examine Internet chat systems. Although chat as an application does not contribute huge amounts of traffic, chat systems are known to be habit-forming[1].WhatsApp messaging service has emerged as the most popular messaging app on mobile devices today. It uses end-to-end encryption which makes government and secret services efforts to combat organized crime, terrorists, and child pornographers technically impossible. Governments would like a “backdoor” into such apps, to use in accessing messages and have emphasized that they will only use the “backdoor” if there is a credible threat to national security. Users of WhatsApp have however, argued against a “backdoor”; they claim a “backdoor” would not only be an infringement of their privacy, but that hackers could also take advantage of it.[2]

Fast SHA-256 [1] is one member of a family of cryptographic hash functions that together are known as SHA-2. The basic computation for the algorithm takes a block of input data that is 512 bits (64 bytes) and a state vector that is 256 bits (32 bytes) in size, and it produces a modified state vector.[3]FAST SHA256 is used to check the integrity of the sent message.

Blockchain technology (aka Distributed Ledger Technology or DLT) is a novel configuration of Peer-to-Peer, cryptographic and distributed computing technologies that have the potential to shift the internet from an internet of information to an internet of value network, with significant disruptive potential. To date, the cryptocurrency ‘bitcoin’ is the application of DLT that has attracted most attention, not all of it favorable. However, DLTs are about much more than cryptocurrencies[4].

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network[5].We use the same idea to host the chat system on a decentralized chat system.

Drawbacks

- **The costs of centralized storage are high**, including employee wages, accounting costs, legal fees, management burdens, data center rents, etc. These costs are even gradually increasing, making the prices of centralized cloud service higher. In addition, the cost of data migration between different centralized cloud storage platforms is also high.
- **The data transmission speed of the centralized storage is slow.** Since the centralized cloud server is usually located in a remote area, which is far away from the users, making its data transmission speed quite slow.
- **The centralized storage is low in security.** In terms of location, centralized cloud servers are concentrated in one or several places. In the event of a power outage or other failure, a large number of related services are often paralyzed, or even have the risk of losing the data for good.
- **The centralized storage is prone to privacy leaks.** The hosts can monitor, censor or disclose data to third parties and your data could be lost, altered or scrambled.

Requirements

Constraints and guidelines :

Software constraints :

1. Operating system: Windows 2000 and above/Linux.

2. Browser:Google Chrome/Mozilla Firefox/Brave/etc.

3.npm has to installed on the device to run on localhost.

Software guidelines: The code is kept tidy and straightforward to ease future program upgrades and maintenance.

Functional Requirements :

- Users should be able to send messages to others.
- Users Should be able to read the messages shared by others.
- Data should be stored on a Decentralized Database and should be easily available.
- Data Should have End-to-End encrypted in place to protect the given data.

Non Functional Requirements:

- Users should be able to create an account.
- Users can Login and Logout as wishes to do.

Problem Statement

Develop a chat system which uses the decentralized ledger technology to store the available data and the chat system should provide end to end encryption to all the information which is being shared amongst the involved parties, chat system should also have authentication in place to allow only legit users to have access to their account.

Satisfying these requirements results in a chat system which is highly secure and data integrity of which cannot be easily exploited.

Methodology

Here we have used Svelte along with HTML and CSS in order to develop the frontend interface of the project.Svelte allows us to interact with APIs and other dependencies as it is also a module of javascript.

For the backend we use GUN API which is, Open Source Firebase, Decentralized Dropbox,GunJS is a module of javascript which lets us use an API to directly interact with a certain live firebase.By using the SEA API by GUN the authentication for the project is created using which users can login and signup.

We use Firebase inorder to host our project online so that users can interact with each other from different places in the world.

HTML

The HyperText Markup Language, or 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 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.[9]

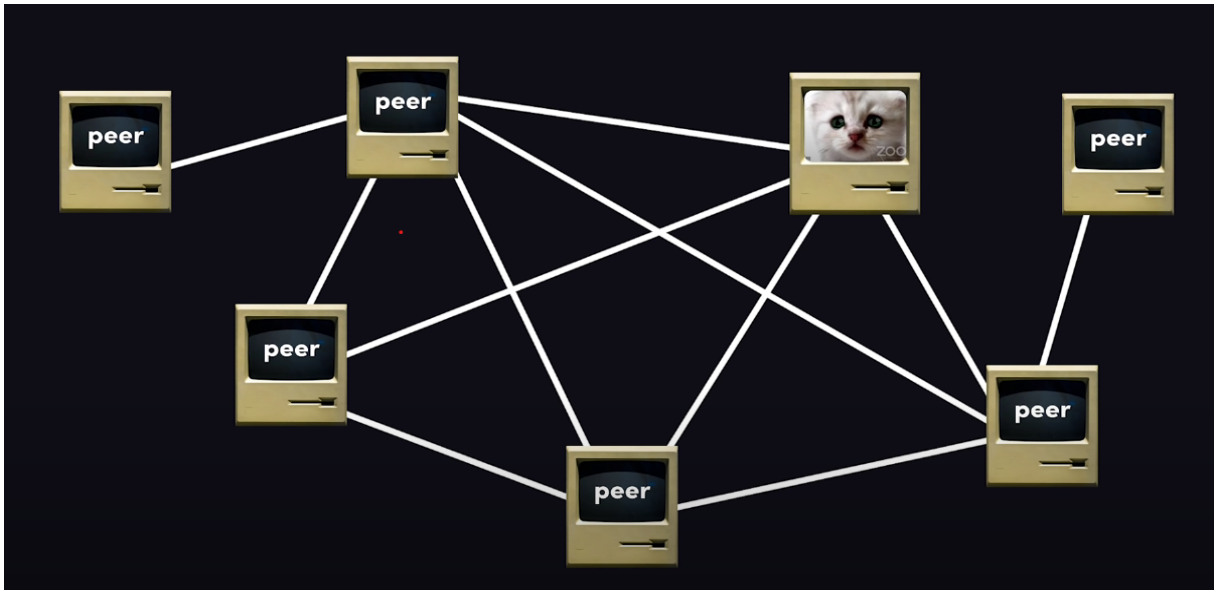
CSS

Cascading Style Sheets is a style sheet language used for describing the presentation of a document written in a markup language such as HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts.[10]

GUN API

GUN is an ecosystem of modular tools. Graphs take you beyond just immutable hashes, they let you do real time multiplayer updates on any type of data. SEA gives you the best local-first secure user accounts, but with normal logins and even p2p password resets using 3FA!

AXE will let you deploy without clouds to a decentralized edge CDN for your JAMstack apps. It runs everywhere, even via browsers with WebRTC, using the simple yet powerful HAM "CRDT" conflict resolution algorithm. Meanwhile, DAM let's you do offline mesh networking and RAD stores your data.[6]



The above picture depicts the way data is stored in the backend when we use GunJS thus by doing this we can be sure that the database will be truly decentralized and when combined with end-to-end encryption makes it comparatively more secure than the traditional chat systems.

SEA API

Security, Encryption, & Authorization - SEA:

SEA is split into two parts, the gun.user() chain and Gun.SEA utility. This page focuses on documentation for the utility library.

SEA is an easy API for the cryptographic primitives explained in the 1min animated explainer cartoon series, that wraps painful ones like the browser native WebCrypto API. We hope to have it swappable with WASM libsodium and/or local proxies to Electron/NodeJS or browser extensions.[6]We use this to create authentication for our users so that no outsider can login as the said user.

FIREBASE

Firebase Hosting provides fast and secure hosting for your web app, static and dynamic content, and microservices.

Firebase Hosting is production-grade web content hosting for developers. With a single command, you can quickly deploy web apps and serve both static and dynamic content to a global CDN (content delivery network).[7]We use this service to publish our website to the internet,So that users can use it from any part of the world.

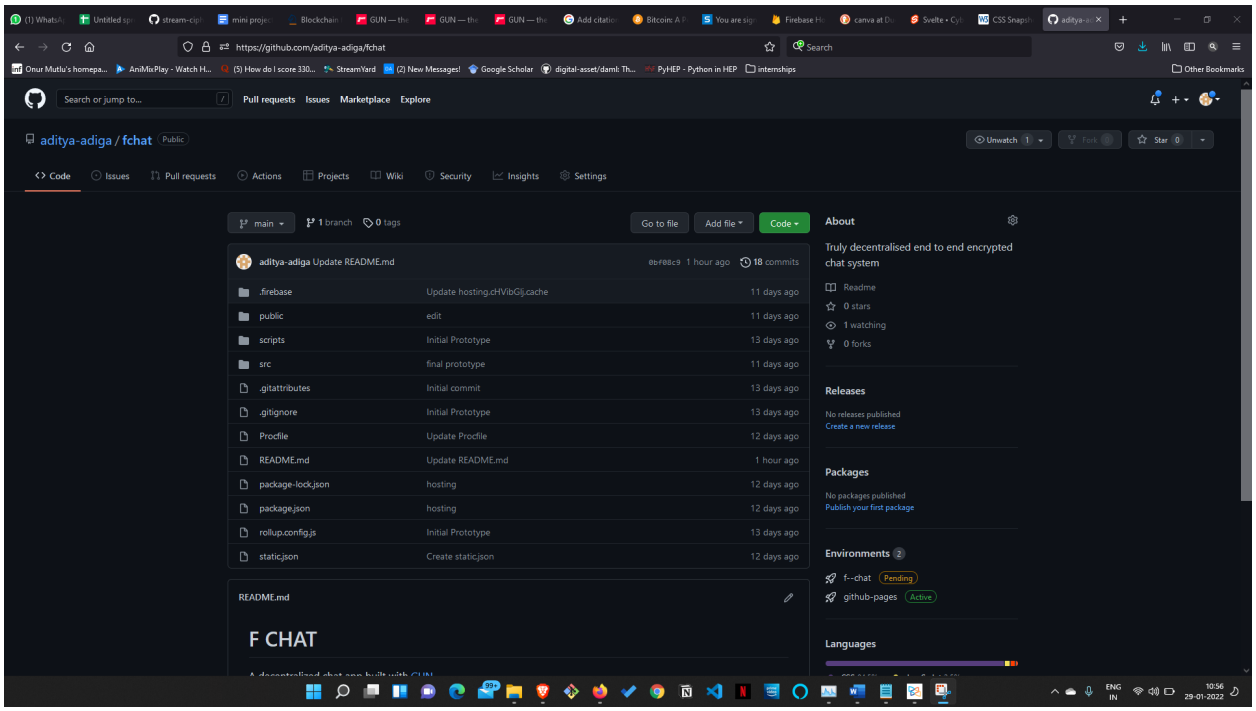
Results

To Run the Application:

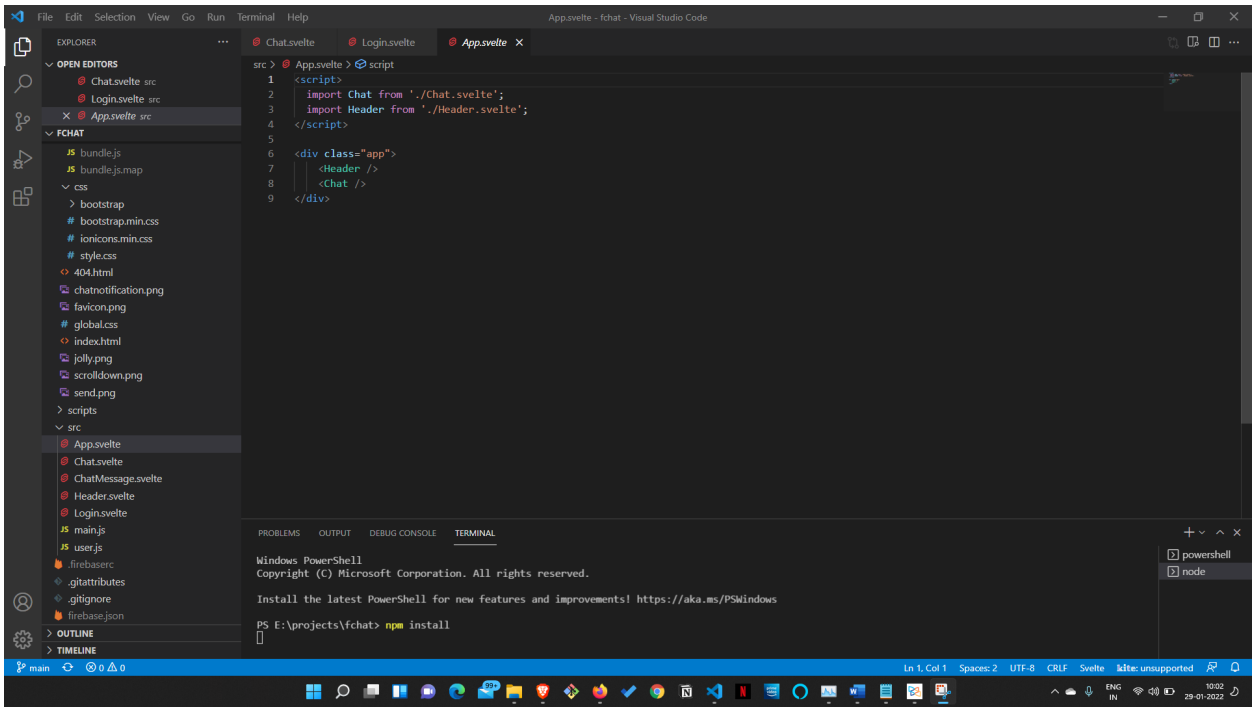
1)Clone the github repo which has the code using the command git clone after navigating to the place where you want to copy the files.

git clone https://github.com/aditya-adiga/fchat

On typing the above command the files are copied to the desired location.

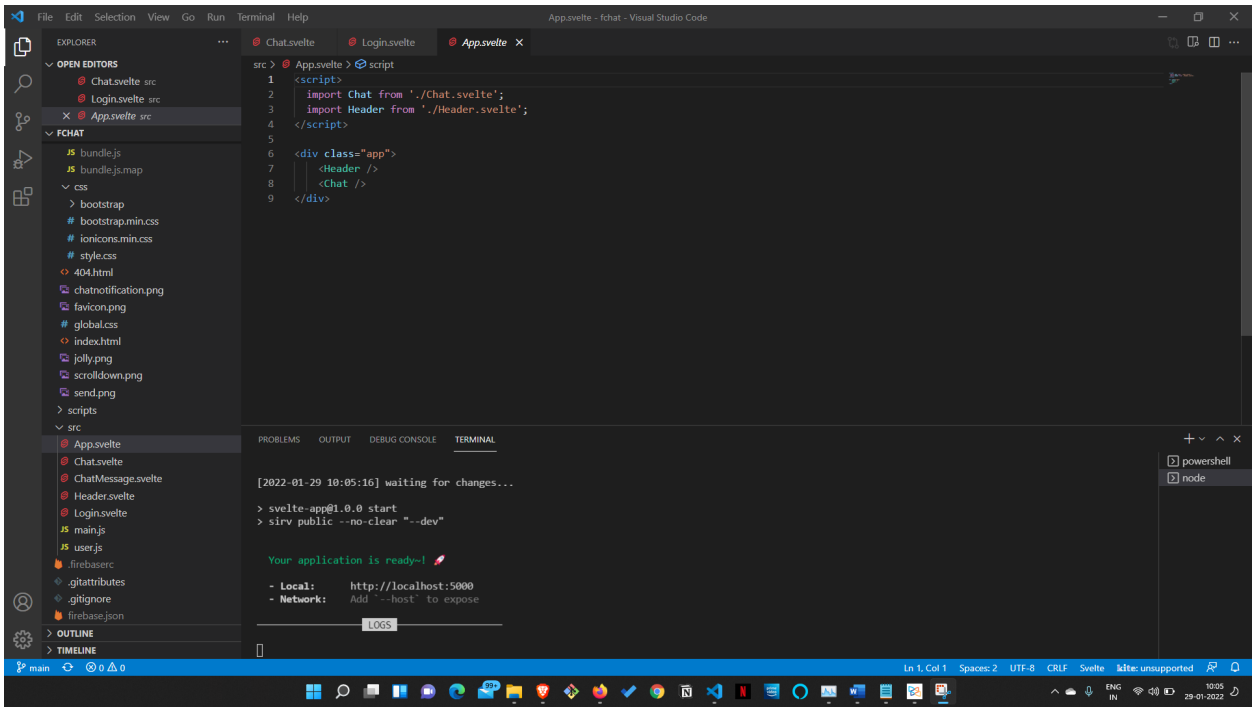


2)Now in order to install all the dependencies we navigate to the root folder that we copied and type the following command:npm install



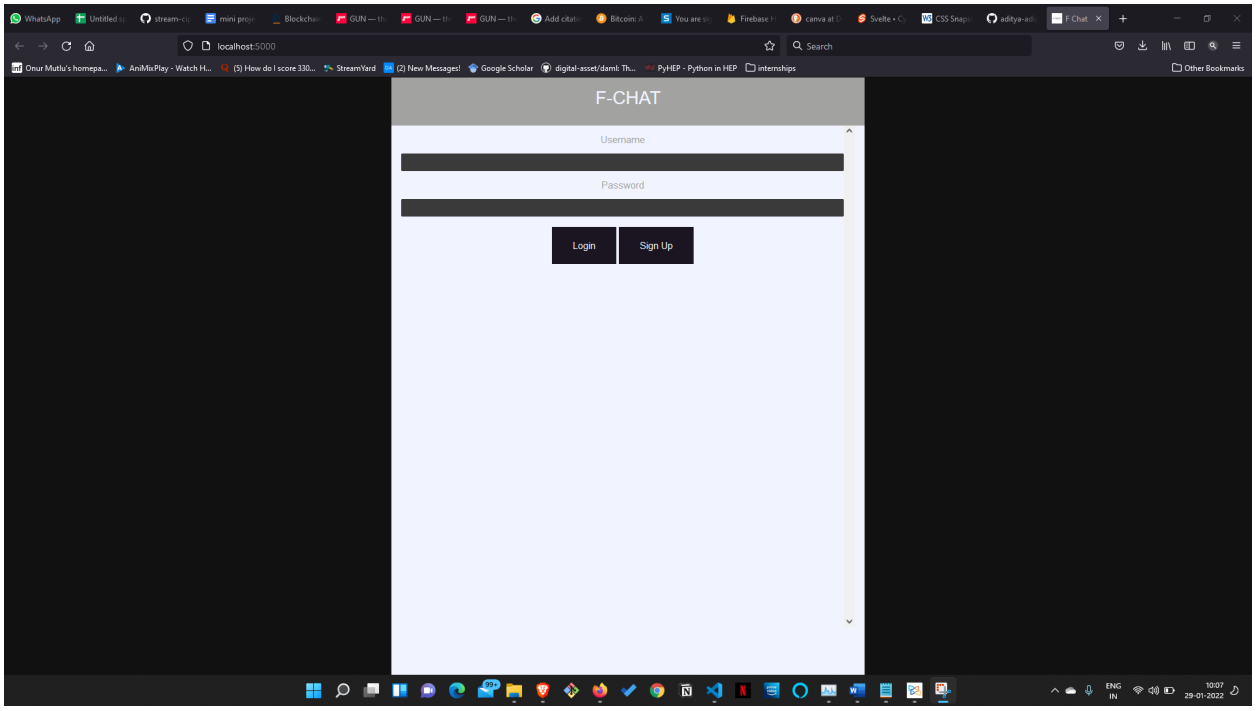
3)Now we can run the application as all the dependencies are already installed.

npm run dev



On running the above command we get the output as shown in above image thus the website will be hosted on: http://localhost:5000/

4)If we go to http://localhost:5000/ we get to see our application.



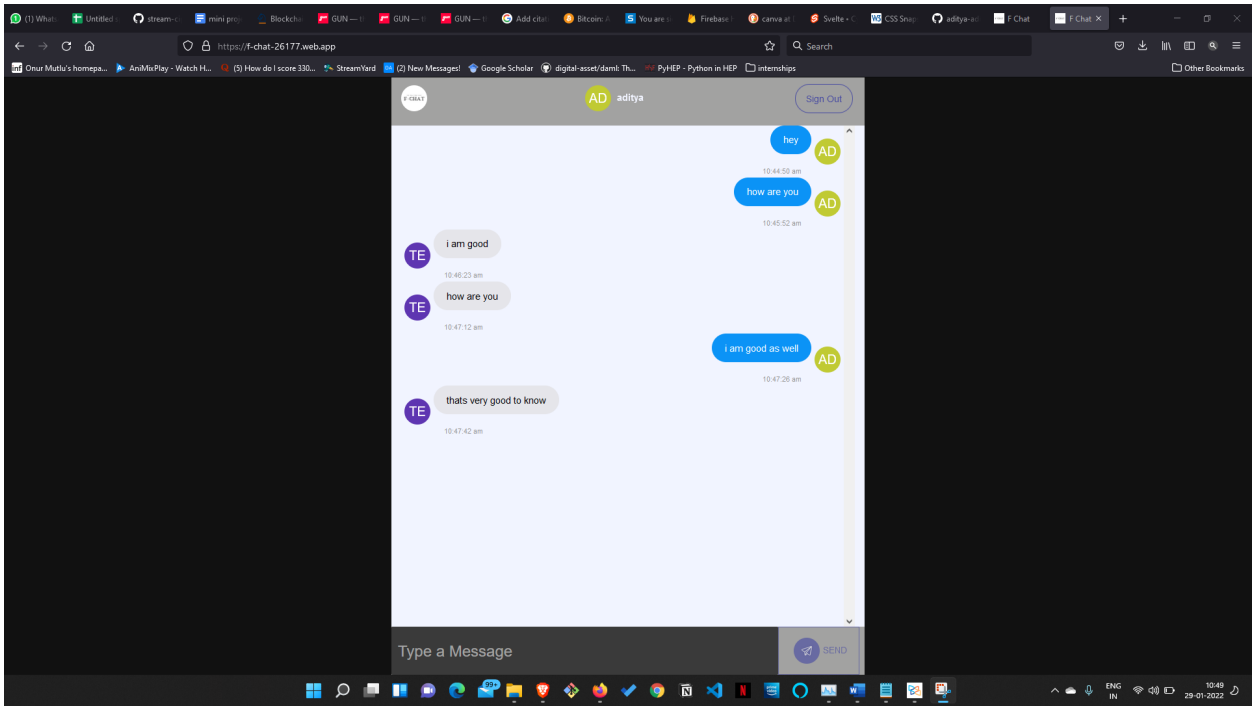
Thus we can access the application on the local server.

Hosted Website on Firebase:

The application can be hosted on the firebase directly by following the docs and using the commands after installing firebase on the device.

Hosted website:https://f-chat-26177.web.app/

Github Link:https://github.com/aditya-adiga/fchat

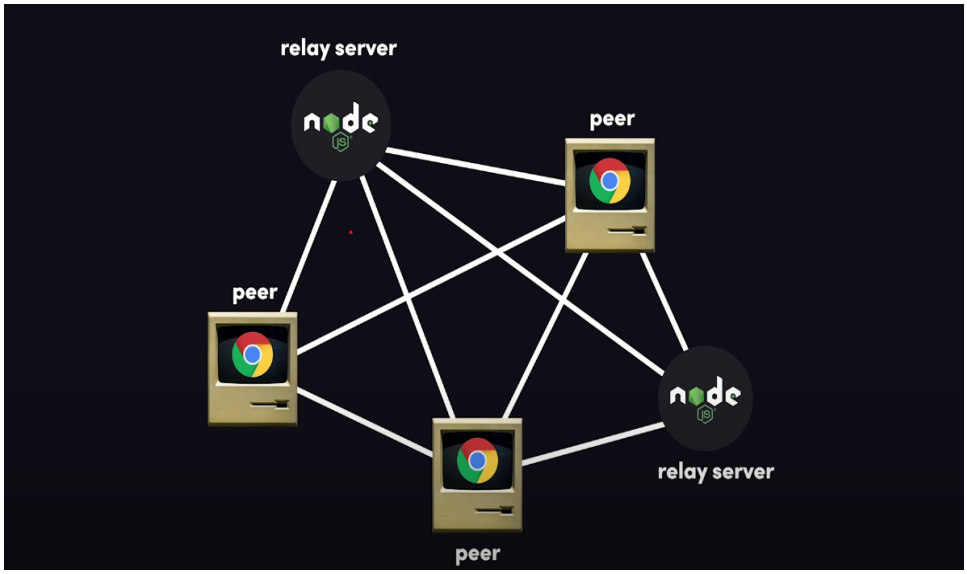


Conclusion and Future Scope

Thus we can conclude that by using decentralized databases along with the end-to-end encryption the security and data integrity of the chat system can be increased by a huge magnitude.But also has its drawbacks as more than a certain amount of nodes need to be active for the website to to function at all times.End-to-end encryption also here is done statically thus the security of the system is still open to Questioning.

Thus in the future modules the focus will be based on the key distribution between the parties to enhance the security of the data being transferred.

In order to keep the distributed database live we can add relay servers in case the amount the nodes available is not enough to keep the data live,thus solving the problems discovered during testing the current release.



Reference

[1]Christian Dewes, Arne Wichmann, and Anja Feldmann. 2003. An analysis of Internet chat systems. In Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement. Association for Computing Machinery, New York, NY, USA, 51–64. DOI:https://doi.org/10.1145/948205.948214

[2]Endeley, R.E. (2018) End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. Journal of Information Security, 9, 95-99. https://doi.org/10.4236/jis.2018.91008

[3]Fast SHA-256 Implementations on Intel® Architecture Processors https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/sha-256-implementations-paper.pdf

[4]Adams R., Kewell B., Parry G. (2018) Blockchain for Good? Digital Ledger Technology and Sustainable Development Goals. In: Leal Filho W., Marans R., Callewaert J. (eds) Handbook of Sustainability and Social Science Research. World Sustainability Series. Springer, Cham. https://doi.org/10.1007/978-3-319-67122-2_7

[5]Bitcoin white paper-https://bitcoin.org/bitcoin.pdf

[6]GunJS Docs-https://gun.eco/docs/API

[7]Firebase Docs-https://firebase.google.com/docs

[8]Svelte-https://svelte.dev/

[9]HTML-https://html.spec.whatwg.org/

[10]CSS-https://www.w3.org/TR/CSS/#css