Anonymous De-centralized Ephemeral Chat Application using Interplanetary File System

Faraz Khan[1], *Niraj* Mantri[2], *Sagar* Rajput[3], *Dhananjay* Dhakane[4], *Puja* Padiya[5,*]

[1]Department of Computer Engineering, Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai, India
[2]Department of Computer Engineering, Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai, India
[3]Department of Computer Engineering, Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai, India
[4]Department of Computer Engineering, Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai, India
[5]Department of Computer Engineering, Ramrao Adik Institute Of Technology, Nerul, Navi Mumbai, India

Abstract— Communication is essential for human beings and we communicate globally with the means of internet every day. Internet is an interconnected mesh of networks where our data is transferred through hundreds of nodes before reaching its destination. As the intermediary network node increases, the risk of losing confidentiality and integrity is also affected. Decentralized Chat (DChat) is a chat service on the Interplanetary File System (IPFS) peer-to-peer protocol where users can communicate with ephemeral chats under any anonymous alias. The users are not aware of real identity of each other and the chats are lost from the service once the node is disconnected. The data is tamper-resistant because to alter it would change the hash and invalidate it from the network. Here we aim to develop a secure chat service that provides anonymity and ephemeral chats using cost-effective IPFS technology.

Keywords— decentralized, anonymous, peer-to-peer, tamper-resistant, ephemeral, chat.

1. Introduction

We use internet a lot, maily for communication. We rely on applications like Facebook, Twitter, Whatsapp. We use them to connect with our family, friends and colleagues but unfortunately these applications are not ephemeral, meaning they leave an electronic trace of ours online which can be easily tracked down to us by a proper cyber forensic team or some skilled individual.

We use chat applications often without knowing that we could under surveillance which could back fire us in an unexpected way in the future. Privacy has value to democracy, liberty and basic human rights. This has to be solved by voluntarily safeguarding and making the conversations ephemeral.

Today when we visit a website, browser sends a GET request to the server and connects to a system that hosts website. The request is routed through the internet and if the servers are at far away distance, the process may take a really longtime and requires intermediate nodes to be involved in it.

Hackers are becoming more prominent today making internet security a major issue. Open and free Wi-Fi may be a threat to one's personal data. It is easier for the hacker to enter into the system and access personal information or other devices connected via open Wi-Fi. Research suggests some of the ways to protect from online threats. One must turn off file sharing before using free public networks. One must avoid signing any site that requires password. Another public but distributed technology that prevents data from being modified is blockchain technology [1].

A blockchain is a database accessed over a computer netw ork. It is very difficult to change when a record has been attached to the chain. The data approved by the network is attached to a chain. A unique code called a hash is contained in each node. It also includes the hash of the chain's previous node.

IPFS [2] is a modern peer-to-peer hypermedia protocol intended at supplementing the Hypertext Transfer Protocol now controlling the Network, or perhaps even replacement. An unique fingerprint, called a cryptographic hash, is given in IPFS to each file and to all blocks. IPFS prevents network-wide duplicates. Each network node only stores content it needs and some indexing information helps find out who stores what. You ask the network to find nodes that store content behind a specific hash while searching data.

* Corresponding author: puja.padiya05@gmail.com

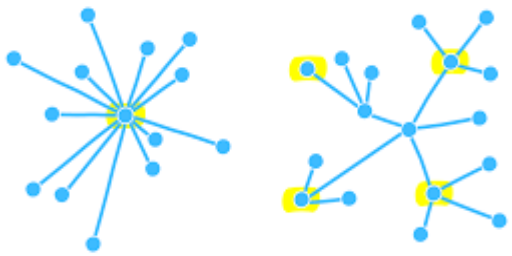

Fig.1 Centralized and Decentralized nature

The focus of our research is to build a decentralized anonymous and tamper-proof cross platform communication system with user friendly interface, that provides integrity and availability and to overcome the demerits of having a central server which loses access to data on failure of single point.

The paper is organized as follows: in section 2 the motivation and approach towards the research is described, section 3 describes the literature survey, problem definition is stated in section 4, and section 5 describes the proposed system followed by results in section 6. Section 7 concludes the paper along with section 8 which describes the future work.

2. Motivation

Everyone likes their own personal space and likewise some people likes being anonymous on the internet. Anonymity has certain benefits for individuals and the environment, such as creating a sense of protection. If they are anonymous, some people may feel safer online. Anonymity is preferred when someone gives their opinion on controversial topics. Anonymity ensures privacy, facilitates freedom of speech, preserves the identity of the individual from public and decreases self-awareness. In addition to anonymity, it is necessary to provide ephemeral chat to prevent those records from haunting us in future. This violates the basics of cyber security, i.e. integrity of the messages are getting intercepted and manipulated during the transmission. To resolve this, there is a need of trustworthy mechanism to disallow validation and acceptance of intercepted and manipulated messages. The concept of key value is something that can bridge the gap. This mechanism uses the concept of a key-value data store. If the value of the hash changes then we can say that the data is invalid.

3. Literature Survey

Most popular online chat sites used by millions of users are Whatsapp [3] and Snapchat [4]. As per recent news of August 2018, WhatsApp was vulnerable to let hackers intercept personal and group messages and manipulate messages.

Here are the few takeaways from the article:

1. The vulnerability concerns WhatsApp's encryption process, which is meant to protect every 2message, picture, call, video or other content sent in chats.

2. However when decrypted, the Check Point team realized that the protocols being used by WhatsApp could be converted and accessed, allowing them to see exactly what rules were being used, and also to change them to their liking.

3. This may allow hackers to modify a group chat text by putting words or using the quote feature in a chat group discus sion to modify the sender's identity.

4. Hackers could also send a personal message to another group participant posing as a public message for all so that wh en the person in question answers, he is visible to all.

The similarities of the system can be related to how Snapchat works on the frontend. By default upon the chat window is closed everyone message in the conversation is deleted from the user's device. This makes the idea rather confusing to naive users. This idea makes more sense in a scenario where the privacy of the conversation is really important. The message is deleted from the conversation the companies claim that the information is deleted off the companies' servers unless the conversation is reported for violating the policies of the application. In that case the conversation is reviewed before it is deleted from the company servers. In either case the integrity of privacy is often affected in some way of the other.

These messaging systems never function on a peer-to-peer basis. There is no relation to each computer of your friends (from your device). You attach your computer to your server instead. You can then use a custom TCP protocol to send your communications to the server, or perhaps to HTTP.

The procedure of visiting a website is firstly your browser requests the server upon which the web service is running on. Even in case in which these servers are far remotely across the world. This is location based reference. This process is bandwidth heavy and thus making it a disadvantage relatively. Also the contents are retrieved from a single data source this is prone to attacks as the availability of the content is at risk. In comparison IPFS downloads the content from multiple sources.

Having a centralized server means the data access to the content can very well be easily blocked by governments and etc. Browser data may expose your device to virtual threats. This information can be the name of your computer, your IP address, the operating system you use, and any other details you request from your website.

All the existing systems [5], [6], [7], suffer from the drawback of centralization of information. They still rely on

* Corresponding author: puja.padiya05@gmail.com

traditional centralized technologies exposing them to attacks concentrated on the central server. Our research aims to overcome this drawback of centralization by using decentralized storage for storing the chat messages securely on IPFS network. Some of the surveys related to IPFS tecnology are as follows:

Youn Chen in [1] introduced blockchain to combine IPFS with the zig-zag storage model. To facilitate permanence and collaboration in web archives, Salwood Alam Mat in [2] had built Interplanetary Wayback to disseminate the contents of WARC files into the IPFS network. S. Muralidharann and Heedong Ko in [8] proposed IoT framework in a P2P decentralized storage infrastructure using IPFS. From the survey we conclude that IPFS technology will be the future for decentralized communication reducing the burden of centralized system [9].

The focus of our research is to build a secure communication application with respect to concepts of security, demolishing the centralized monopoly built by tech giants, having more control over our data as we have clear transparent information on how it is stored and passed on, maintaining integrity of transferred data and anonymity without gathering any user personal data.

4. Proposed System

We are proposing a Secure Distributed Chat application for users that can be used as an alternative to the current Centralized server chat applications. The proposed system uses the advantages of IPFS [9] technology to improve the reliability of the communication applications respecting the privacy of customers.

The user communicates under a fake alias which can be changed anytime during the conversation in the chatroom. This gives complete anonymity and flexibility to the users of the Dchat application. Our system not only provides a means of anonymous communicating, but also follows the cybersecurity basics and promotes them. Also the messages during the conversation are ephemeral [10] messages and are destroyed upon disconnect of the user.

IPFS uses the concept of pinning. Since IPFS is a file system the data may be needed to store for a long time. You can pin your own information or use some third party services to pin it for a small amount of monthly fee depending on the service used. Since we do not want our chat to be persisted, we are transmitting the communicational information only in real time and since we do not pin these information the information gets lost and this achieves ephemerality.

Security in this implementation is IPFS dependent, meaning every information can be accessed by anyone if they're the hash of the information this can be seen as a security risk at first but IPFS hashes are of 32 bytes hash with SHA256. So it is impossible for anyone to guess the hash of any information exchanged and even if they manage to guess it correctly. It is only one message out of the many from the conversation and since the chat is ephemeral the hash must be referred to, as the communication is taking place as the information will be wiped from the IPFS File system by not pinning it. The only way for a third party to intercept the communication is by knowing the chat room ID of the communication which is taking place and actively being listening in real time. So it is recommended to use long and complicated chatroom names to avoid security breaches.

4.1 Interplanetary File System (IPFS):

IPFS establishes a permanent distributed network by using content-based reference. This is different as compared to the usual location based reference of traditional protocols like HTTP.

To compare the structure of a request of HTTP with IPFS.

HTTP request

https://192.168.0.125/files/resume.pdf

IPFS request

/ipfs/QmjY8F0C3Onu/files/resume.pdf

IPFS [11], [12], [13], [14] uses the hash of the file itself to be used as a reference. This hash is the result of a cryptographic cipher which makes sure that only one copy of the file exists on the IPFS network which in results avoids duplications across the network.

IPFS uses peer to peer technology. Hence making a direct communication of two peers possible. This is possible due to the ipfs pubsub-room. Upon receiving a connection request the browser initiates an IPFS node in the client's browser and connects it to a room. LibP2P protocol is used is to emit membership events, listen for incoming messages and broadcasts and directly messaging to the peers on the network. Upon sending a message the message gets routed through the IPFS network to the receiver with the correct PeerID. Likewise upon receiving a text-message the network(IPFS) checks the peerID from the metadata of the message it is specified for and thus completing the communication process.

A broadcast room is a chatroom where multiple people are communicating at the same time therefore broadcasting messages to everyone connected in the IPFS room. Users have to visit the DChat web application for the first time The IPFS Server initializes a new node for the current user. Upon initialization is completed the user is now connected to the IPFS server chat room. The chat room has a new unique name on which the clients send and listen for new messages

User selects an alias name for the messages on the application Throughout the conversation the user has the flexibility to change his alias to any other name When the chat

* Corresponding author: puja.padiya05@gmail.com

room detects a new message event the message is returned to all connected nodes Someone can choose to either connect to someone from the chat room for a private peer to peer chat or create their own custom chat room.

The browser uses ipfs-js package for instantiating a node in the browser, the node of ipfs-js is then passed on to a ipfs-pubsub service which allows the possibility of using IPFS as a potential chat application with web sockets like functionalities to connect and subscribe to messages in real time.

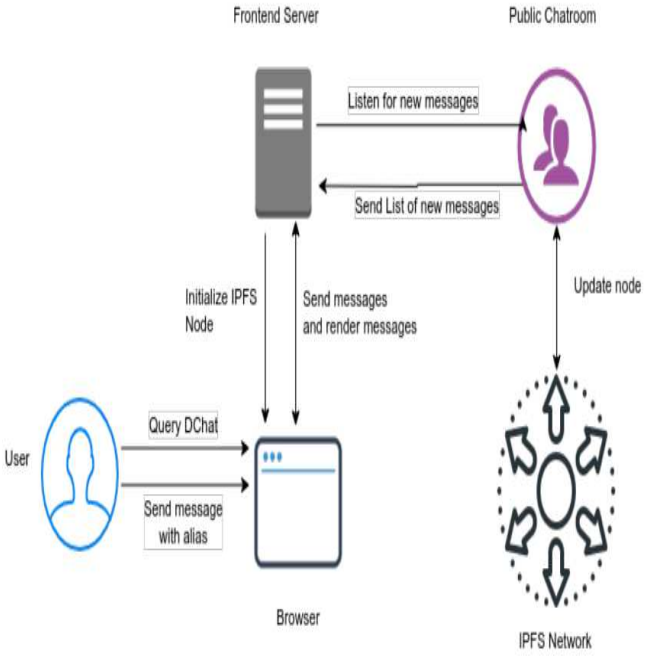

Fig.2. System Architecture

Users have to visit the DChatwebapp for the first time The IPFS Server initializes a new node for the current user. Upon initialization is completed the user is now connected to the IPFS 7server chatroom. The chatroom has a new unique name on which the clients send and listen for new messages.

4.2 Design of the System:

User selects an alias name for the messages on the application. Throughout the conversation the user has the flexibility to change his alias to any other name When the chatroom detects a new message event the message is returned to all connected nodes. Someone can choose to either connect to someone from the chatroom for a private peer to peer chat or create their own custom chat room. When the connection to the IPFS node is lost, the connection is dropped and the addresses to the previous messages are lost.

The user initializes an IPFS node and once the initialization is completed user gets connected to the chatroom using IPFS technology and if not it throws a error “try again”.

Once the user is connected to the chatroom it broadcasts a message to all the users in the chatroom under an alias. The alias as is, is anonymous. Everyone in the chatroom receives the message.

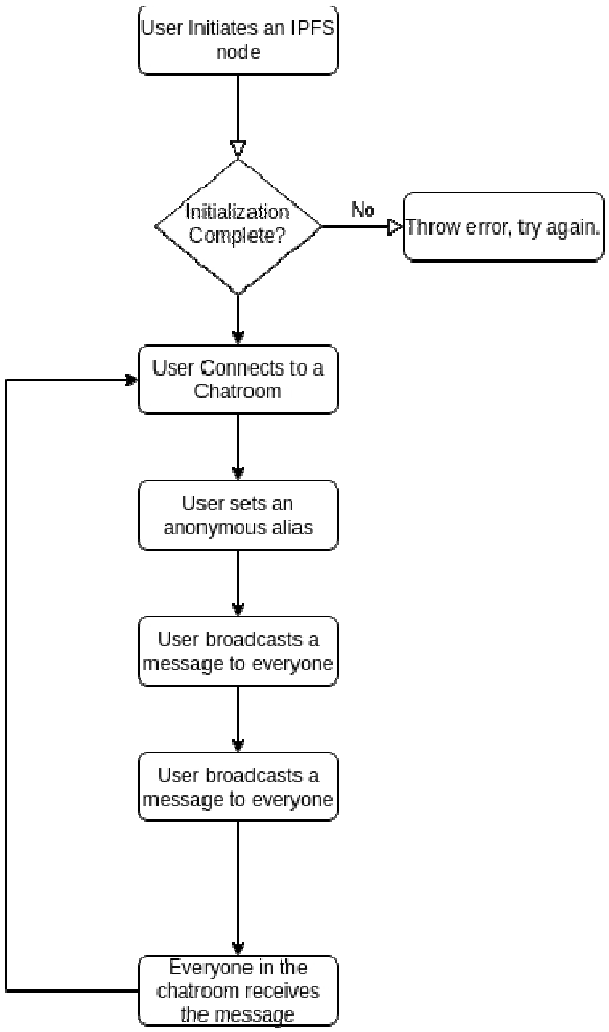

Fig. 3. Flow Diagram

The particular person who wants to communicate with the user sends a message back and after some verification they can communicate secretly or one can create their own custom chat room. Once the chat ends and they exit the chat gets deleted permanently and as there is no record of chat it is completely secure.

The major components of the system consist of the core blocks:

* Corresponding author: puja.padiya05@gmail.com

1. User Interface - User Interface Design is important because it can make or break your customer base. It creates fewer problems, increases user involvement, perfects functionality and creates a strong link between your customers and your application. The user interface for the DChat application is a simple responsive Chat interface with options for user to send a message under a random and flexible alias name.

2. Storage the new list of messages received on the Chatroom are temporarily stored in the volatile storage object of the React server which upon reload or refresh is lost

3. IPFS node each user on the network connected to the website gets their own instance of an IPFS node through which they can send and receive messages

4.Chatroom IPFS can store all type of information, In this case we store a chatroom data which consist of the name of the chatroom and the hashes of user connected, hashes of messages and etc.

5. Results

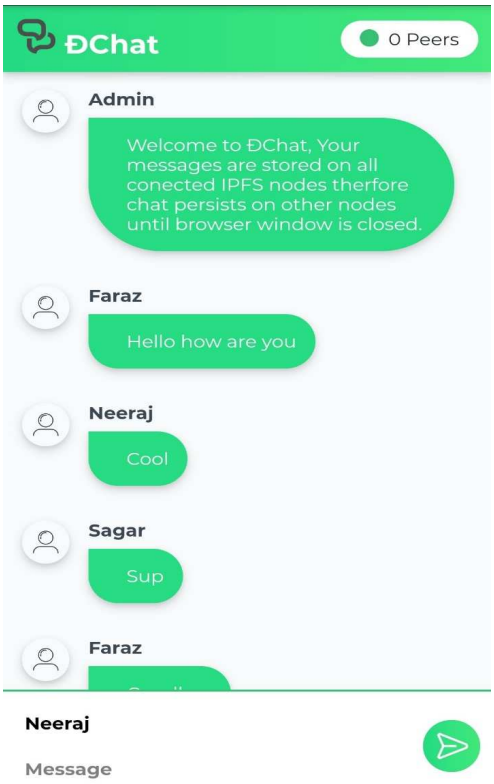

Fig. 4. Snapshot of the developed DChat application

Users have to visit the webapp.

2. The IPFS Server initializes a new node for the current user.

3. Upon initialization is completed the user is now connected to the IPFS server chatroom.

4. The chatroom has a new unique name on which the clients send and listen for new messages.

5. User selects an alias name for the messages on the application.

6. Throughout the conversation the user has the flexibility to change his alias to any other name.

7. When the public chatroom detects a new message event the message is displayed onto all the 9 nodes which are connected to the public chatroom.

8. When the connection to the IPFS node is lost, the connection is dropped and the address to the previous messages is lost.

The new proposed system uses the advantages of IPFS technology to improve the reliability of the communication applications respecting the privacy of customers. Confidentiality refers to protecting information from being accessed by unauthorized parties. Proposed Dchat does not disclose the identity of the user and the only way user is recognized on the network is their IPFS node hash. Integrity refers to ensuring the authenticity of information that information is not altered. Dchat uses technology of IPFS where the data is tamper-resistant as to alter any information it would change the hash. Availability means that information is accessible by authorized users. We achieve it through the help of IPFS peer to peer architecture where the same data is stored on each node connected on the network. Therefore the data is always available until at least one node is available on the network. Dchat provides anonymity as throughout the conversation the user has the flexibility to change his alias to any other name. When the connection to the IPFS node is lost, the connection is dropped and the addresses to the previous messages are lost and all the chat are cleared. The chat communications provided by Dchat are ephemeral.

6. Conclusion

We conclude that the Decentralized Chat (Dchat) is a cross-platform application, an anonymous and tamper-proof communication system with user friendly interface which follows integrity and availability concepts of cyber security, with ephemeral communication and overcomes the demerits of having a central chat server. Thus, redefining the concept of secure chat app on the internet.

7. Future Work

Proposed Dchat is a text messaging application that uses IPFS technology for decentralized anonymous and tamper-proof cross platform communication system with user friendly interface. It provides integrity and makes sure that the

* Corresponding author: puja.padiya05@gmail.com

communication is ephemeral communication. In future, newer version of Dchat application will provide images and videos to be communicated along with the text messages.

References

1. Y. Chen, H. Li, K. Li and J. Zhang, "An improved P2P file system scheme based on IPFS and Blockchain," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, pp. 2652-2657, (2007)
2. S. Alam, M. Kelly and M. L. Nelson, "Interplanetary Wayback: The permanent web archive," 2016 IEEE/ACM Joint Conference on Digital Libraries (JCDL), Newark, NJ, pp. 273-274, (2016)
3. S. Patmanthara, D. Febiharsa and F. A. Dwiyanto, "Social Media as a Learning Media: A Comparative Analysis of Youtube, WhatsApp, Facebook and Instagram Utillization," 2019 International Conference on Electrical, Electronics and Information Engineering (ICEEIE), Denpasar, Bali, Indonesia, pp. 183-186, (2019)
4. N. S. Al-Saqer and M. E. Seliaman, "The Impact of Privacy Policies Awareness on Snapchat Saudi users Discontinuous Usage Intention," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, pp. 1-6, (2018)
5. D. Henriyan, Devie Pratama Subiyanti, R. Fauzian, D. Anggraini, M. Vicky Ghani Aziz and Ary Setijadi Prihatmanto, "Design and implementation of web based real time chat interfacing server," 2016 6th International Conference on System Engineering and Technology (ICSET), Bandung, pp. 83-87, (2016)
6. I. Karabey and G. Akman, "A cryptographic approach for secure client - server chat application using public key infrastructure (PKI)," 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, 2016, pp. 442-446, (2016)
7. R. Sanjaya and A. S. Girsang, "Implementation application internal chat messenger using android system," 2017 International Conference on Applied Computer and Communication Technologies (ComCom), Jakarta, pp. 1-4, (2017)
8. S. Muralidharan and H. Ko, "An InterPlanetary File System (IPFS) based IoT framework," 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 1-2, (2019)
9. R. Kumar and R. Tripathi, "Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain," 2019 Fifth International Conference on Image Information Processing (ICIIP), Shimla, India, pp. 246-251, (2019)
10. A. Malhotra, V. Sharma, P. Gandhi and N. Purohit, "UDP based chat application," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, pp. V6-374-V6-377, (2010)
11. Teixeira Pedro, "*Professional Node.js: Building Javascript Based Scalable Software Kindle Edition*", (Wrox, 2012)
12. Online: https://ipfs.io/ [Accessed: 15-09-2019]
13. Online: https://github.com/ipfs-shipyard/ipfs-pubsub-room [Accessed: 27-09-2019]
14. Online: https://github.com/ipfs-shipyard/ipfs-pubsub-1on1 [Accessed: 04-10-2019]

* Corresponding author: puja.padiya05@gmail.com