PREVENTING THE SPREAD OF MISINFORMATION IN WHATSAPP USING HASH INFO FEATURE IN BLOCKCHAIN WITH ENHANCED USER EXPERIENCE

[1] *Mr. M. Shanmugam,* [2] *Hemachandran G,* [3] Ragul *S,* [4] *Trijun M,* [5] *Vishal T*

Department Of Computer Science and Engineering
Sri ManakulaVinayagar Engineering College

ABSTRACT

Fake news spreads like a virus these days. Mindless and incessant forwarding of WhatsApp messages without verifying the correctness of such messages is leading to the spread of fake news, and many a time, such messages assume racial and religious overtones. Therefore, dealing with these in real-time and in an accurate scale is a critical issue. Whatsapp made a few changes in the app for Indian users, like labeling forwarded messages, removing the quick forward button, and limiting the number of allowed forwards to five people or five groups at a time [1]. It did stop the individual forwards carrying nonsense messages and fake news but it continues to revel in Whatsapp groups. Complete anonymity is one of the biggest problems with this menace of fake news. WhatsApp needs to take more concrete steps to ensure that each time a message is sent, it must have some indication of the sender's identity. This would make it easier for the law enforcement agencies to get hold of the person who actually created the message [2]. Our proposed system creates accountability for every user who shares a forwarded message, so as to make them think twice before sending an abusive message or forwarding fake news [5]. Forwarded messages don't have accountability, which leads to the problem of forwarding them too many times. So to stop this from happening, we have created a way of identifying the senders through a hash code, which can be found by selecting the message and clicking on the hash info option. This displays the hash code as well as the hash pointer for that message. By using this feature, every user knows that they will be held accountable whenever they forward a message [6]. This can stop people from sending fake news and helps us to identify every person to which it

has been sent as well as easy identification of the source. This feature also helps users to have a better overall user experience, as providing users with the ability to stop the propagation of fake news helps them to trustthe app more easily.

Keywords: WhatsApp , Fake News, Hash Info, Security, Context aware, Intelligence, Progressive, Accountability.

1. INTRODUCTION

1.1 Whatsapp

Whatsapp is a simple messaging application that was designed to be much less intrusive on people's privacy than Facebook, which also happens to own Whatsapp. Facebook knows much more about its users, has greater capability to combat fake news, and more means to handle the issue [1]. On the other hand, WhatsApp's administrators reportedly have no access to the content of messages, they are encrypted unless specifically reported. This is one of the dilemmas of the modern, electronic world: The more a social medium or a messaging application knows about its users, the more it can do to limit malicious behavior, but the more it knows, the more it can be used to spy on people's lives (and thus be misused in equally evil ways). Any regulation of social media may impinge on free speech and the right to privacy.

1.2 Whatsapp Features

WhatsApp has helped tackle misinformation through product changes to reduce bulk and viral messaging, which have yielded a 70% decrease in highly forwarded messages on WhatsApp. Some of these features include

1.2.1 Whatsapp Forwarded Message Labels:

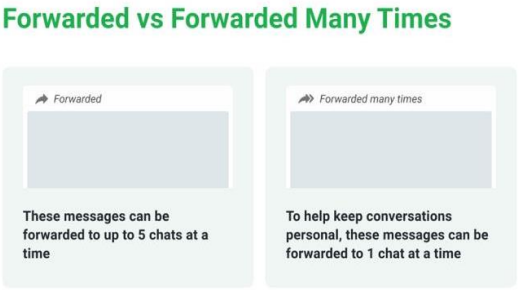


FIG 1.1 : Forwarded labels Messages with the "Forwarded" label helpyou determine if your friend or familymember wrote the message or if it originallycame from someone else. When a message isforwarded through a chain of five or morechats, meaning it's at least five forwards away from its original sender, a double arrowicon and the "Forwarded many times" labelwill be displayed

1.2.2 Whatsapp Forwarding Limits:

You can forward a message to up to five chats at a time. If a message has already been forwarded, you can forward it to up to five chats, including a maximum of one group [6]. However, when a message is forwarded through a chain of five or more chats, meaning it's at least five forwards away from its original sender, then it can only be

forwarded to one chat at a time, as a way to help keep conversations on WhatsApp intimate and personal. This also helps slow down the spread of rumors, viral messages, and fake news.

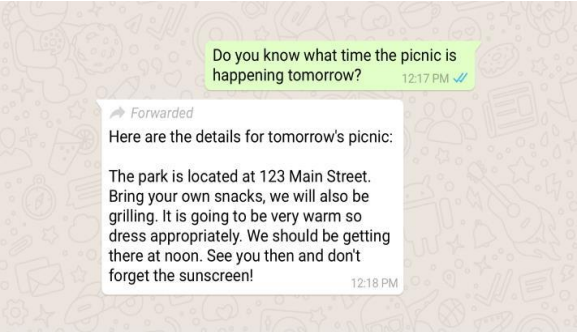


FIG 1.2 : Forwarding Limits

Forwarded messages contain a counter that keeps track of how many times a message is forwarded. For your privacy, WhatsApp doesn't know how many times a message is forwarded and can't see the content of any of your messages in end-to-end encrypted chats.

1.2.3 Whatsapp "Search The Web" Feature:

The new WhatsApp feature provides a simple way to search messages that have been forwarded many times, which may help people find news results or other sources of information about the content they have received [6]. This feature works by allowing users to upload the message via their browser without WhatsApp ever seeing the message itself.

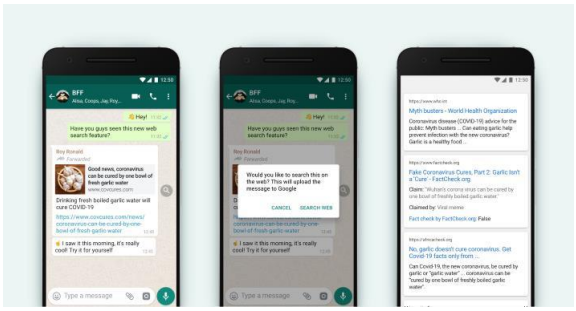


FIG 1.3 : "Search the web " Feature

With the "search the web" feature, users will be able to see a magnifying glass button next to a forwarded message. On clicking the magnifying glass, users will be taken to a Google search with results showing whether the message is fake or true.

1.2.4 Whatsapp Report:

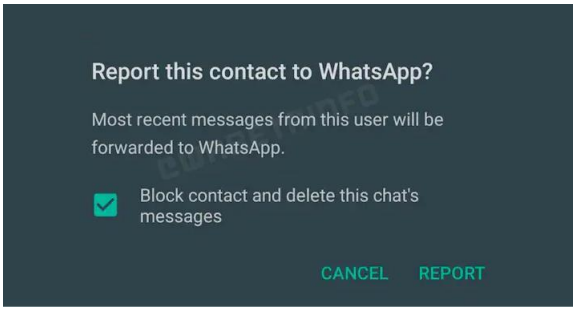


FIG 1.4 : Whatsapp Reeport

You can also choose to report an account by long pressing a single message and clicking on the report option. When you report someone, WhatsApp receives the last five messages sent to you by the reported user or group, and they won't be notified. WhatsApp also receives the reported group or user ID, information on when the message was sent, and the type of message sent (image, video,text, etc.) [1].

1.3 Threat Of Traceability In Brazil And How It Erodes Privacy

The Brazilian National Congress is actively considering legislation that would force companies to add a permanent identity stamp to the private messages people send. The proposal is called "traceability." If passed, private messaging services like WhatsApp would have to trace "who said what" and "who shared what" for the billions of messages sent every day. The proposal inverts law enforcement investigations by forcing private companies to turn over the names of people who say or share something. This could include information about people who forwarded something along just to comment on it.

As we conduct more of our lives online, especially in the middle of this pandemic, protecting our private conversations with friends, family, doctors, and clients is more important than ever. That is why Whatsapp built end-to-end encryption into their app. This security technology protects users by making sure only the sender and the people they are talking to can see the content of their messages, not criminals, not hackers, not authoritarian governments, and not even WhatsApp. Viral misinformation is a widespread societal problem that exists in every form of communication, including email, letters, and in-person conversations. Weakening privacy for all and putting innocent people at risk is not the solution.

2. LITERATURE SURVEY

2.1 How To Stop Spread Of Misinformation On Social Media: Facebook Plans Vs. Right-Click Authenticate Approach

AUTHORS: Pardis Pourghomi, Fadi Safieddine, Wassim Masri, Milan Dordevic

DESCRIPTION: To combat the spread of misinformation and to verify the interrelationship between actors and artifacts from the social media applications ecosystem for suggesting improvements in the development of these tools.This paper didn't make new efforts made by social media application developers to provide tools to mitigate misinformation, although necessary,are not successful.

2.2 Developing More Reliable News Sources By Utilizing The Blockchain Technology To Combat Fake News

Authors: Panayiotis Christodoulou, Klitos Christodoulou

Description: The decentralised application presented in this paper was created using Solidity and deployed to the Ethereum

blockchain. The purpose of the proposed application is to assist the government's communication and media agencies in their fight against false information. More specifically, we suggest a regulating mechanism for registering trustworthy news sources that is managed by a smart contract. This makes it possible for people to confirm an article's veracity for themselves. By incorporating new attributes like an article's URL or its hash, which is created by analysing the text and header metadata, they didn't worry about enhancing the expressivity of the information that is governed by the smart contract.

2.3 Comparison Of Various Machine Learning Models For Accurate Detection Of

Fake News

Authors: KarishnuPoddar, Geraldine Bessie Amali D, Umadevi K S

Description: Fake news consists of news that is not well researched or deliberate steps have been taken to spread misinformation or hoaxes via different forms of news distribution networks. This paper aims to tackle this issue using a computational model of probabilistic and geometric machine learning models. Moreover, the scores of two different vectorizers namely count and Term Frequency Inverse Document Format(TF- IDF) will be compared to find the appropriate vectorizer for fake news detection. English stop words have been used to improve the scores. Various classifiers like Naive Bayes, Support Vector Machine(SVM), Logistic regression and decision tree classifier were used to predict the fake news. Simulation results indicate Support Vector Machine (SVM) with the TF-IDF gave the most accurate prediction.

2.4 Whistleblower: Towards A Decentralized And Open Platform For Spotting Fake News

Authors: Gowri Ramachandran, Daniel Nemeth, David Neville, DimitriiZhelezov, Ahmet Yalc¸in, and OliverFohrmann, BhaskarKrishnamachari

Description: WhistleBlower enables the developers of machine learning and AI algorithms to integrate their work into a platform for user-driven fake news identification. On public nodes donated by members of the community, a framework for verifiable computation has been used to carry out the computation. They didn't use HelixNetwork, which has a native HLX coin, HelixMesh, and a double consensus protocol. It enables versatility and includes both an on- chain and an off-chain consensus mechanism.

2.5 Online Misinformation: From The Deceiver To The Victim

Authors: Anu Shrestha, Francesca Spezzano.

Description: This report included a summaryof our ongoing investigations into the misinformation-spreading actors and our outreach efforts to the most helpless victims. We demonstrated a link between the believability of false news and the bias of its publishers, discovered that network properties aid in identifying active fake news spreaders, and discussed our senior outreach experience. By taking into account the revelations made in this research, they failed to create algorithms for automatically determining news, source, and user reliability.

2.6 Unsupervised Whatsapp Fake News Detection Using Semantic Search

Authors : Jaynil Gaglani, Yash Gandhi,Shubham Gogate, Aparna Halbe **Description**: Using machine learningapproaches, we have proposed an unsupervised and distinctive method for categorising false claims made over WhatsApp. By utilising the capabilities of natural language processing, this method notonly determines if the sent message isfraudulent or not, but also takes into accountthe contextual resemblance between claimsand news articles. This work aids in the fightagainst false information that spreads widelyon social media sites like

WhatsApp. Theydidn't use the deep learning idea to translatethe message and read its context to determineif it was phoney or not. Multimedia Fakenews is increasingly being disseminated using messages like photos and videos. Using a Deep Learning method, the veracity of sentphotos and videos may be examined.

3. SYSTEM STUDY

3.1 Existing System

A similar method which is used for preventing spread of misinformation uses a method called the 'Right-click Authenticate' that would review, rank, and identify misinformation by combining several tools already found online. However, these tools have never been put together in an easily accessible way that would help online users in their pursuit of authentication of the information they view. In this approach, three categories of authentication have been identified textual, imagery, and video misinformation, yet the research focused on the first two, Textual and imagery authentication. In that process, users who are unsure about the content could rightclick and select authenticate as conceptualized. This approach does not prohibit sharing or trending of misinformation approach, thus satisfying critics who are concerned about suppression of freedom of speech. Instead, this approach provides a presentation of facts together with editorial in the same format of Wikipedia. This approach would also represent an important step to analyze and predict the dynamic trend of misinformation propagation.

3.2 Limitations Of Existing Systems: There are some important limitations to be noted though. The approach does not contain a filtering process to stop abuse of this system and possibly slowing down to a point of denial of service. Unlike Facebook whodecides if the item reported is worth reporting, users could abuse this service toauthenticate holiday photos, works of literature, or any work that is not in essence news. Another consideration is the effort toauthenticate. The Facebook approach suggests that the news will be tagged as fake news without the need to right-click and authenticate. This will be visible for everyone. Moreover, this approach will be restricted to one or few browsers only. Users adamant to follow fake news will simply switch browsers and some countries may go as far as banning such browsers. Finally, both approaches will remain limited in their ability to verify live reporting and breaking news. However, it is evident from this review that the Facebook approach to combating spread of misinformation has some important failings and inefficiencies that the social media needs to address.

3.3 Proposed System

3.3.1 Proposed Solution:

The system aims to prevent the spread of misinformation as early as possible. This is achieved by introducing a private blockchain architecture in the existing system along with a slight modification of the right-click authentication method. The current features in Whatsapp don't provide users the ability to stop the spread of a misinformation once it is identified. A clear example is, when a user finds out that a message is misleading using the find the web feature, the only

next step they can take is to ask the person who sent them to not share the information anymore. This doesn't stop the spread since the person who sent the user is not the origin of the misinformation.

3.3.2 Proposed Architecture:

Thus by applying the concepts of blockchain, we are able to create links between the forwarded messages using hash code and hash pointers. This can help us trace back to the origin of the message without having to compromise on privacy. When a user finds a message to be misinformation, they can simply long press the message and click on the report hash pointer option, which will then give them the ability to see the hash pointer of the message and report it.

When the threshold for the number of reports for that particular chain exceeds, it automatically hides every message in the chain and sends it for verification similar to the right-click authentication method. If the message is reviewed and found out to be fake, the data is then sent to a dataset model and the person who sent the message in the first

place will be notified. If the count for the number of times a person gets notified exceeds, then their account gets banned from Whatsapp. This helps prevent users from forwarding misinformation as well as stopping the spread of fake news in the network.

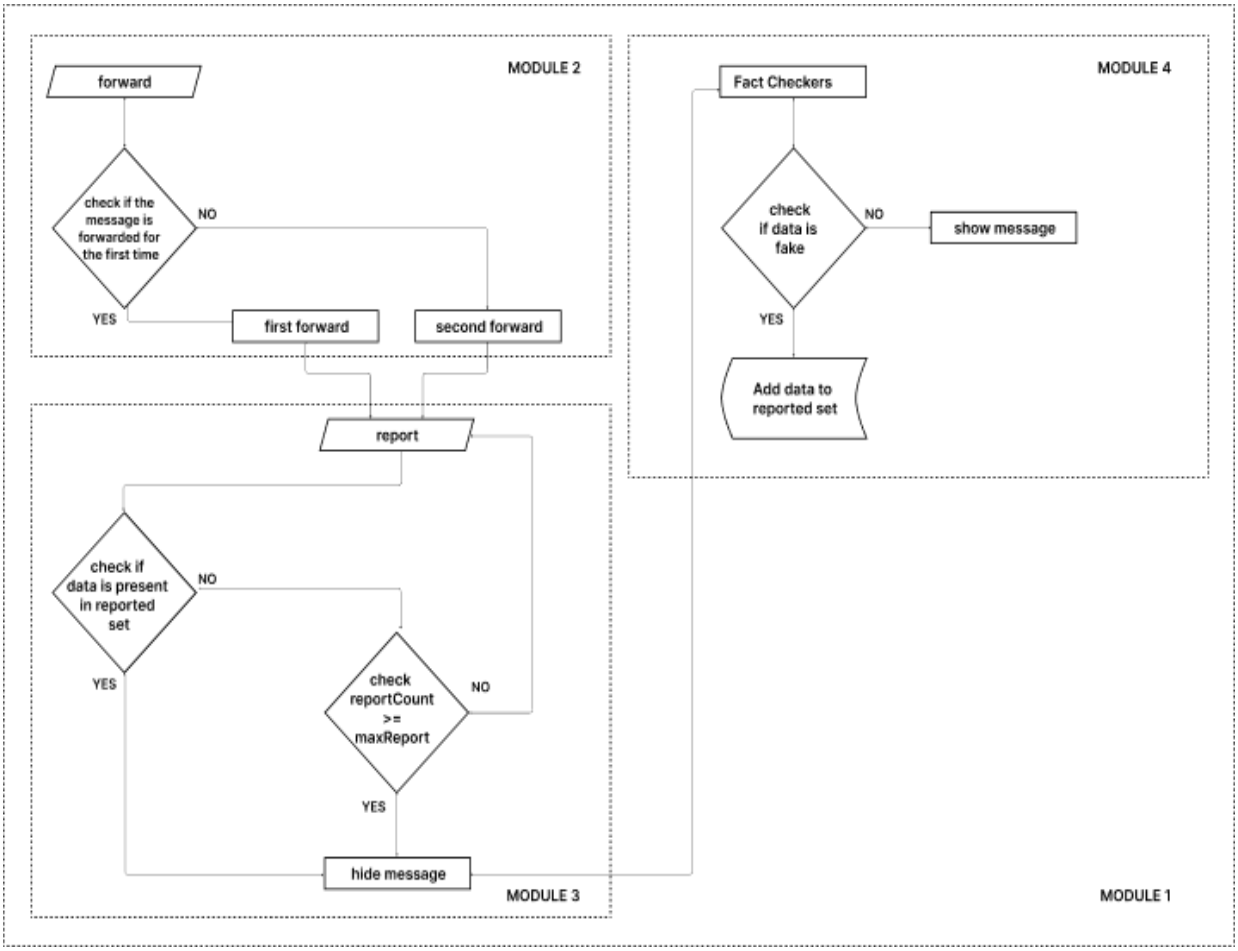


Fig 3.1: Proposed Architecture

SYSTEM REQUIREMENTS

4.1 Software Requirements:

Larvel:

Laravel is a back-end PHP-based and open- source framework used for building a wide range of custom web applications. It's an entirely server-side framework that manages data with the help of Model-View-Controller

(MVC) design which breaks an application back-end architecture into logical parts.

Features of Laravel:

Authentication:

It is the most important factor in a web application, and developers need to spend a lot of time writing the authentication code. Laravel contains an inbuilt authentication system, you only need to configure models,

views, and controllers to make the application work.

Innovative Template Engine:

Laravel provides an innovative template engine which allows the developers to create the dynamic website. The available widgets in Laravel can be used to create solid structures for an application.

MVC Architecture Support:

Laravel supports MVC architecture. It provides faster development process as in MVC one programmer can work on the view while other is working on the controller to create the business logic for the web application.

PostgreSQL:

PostgreSQL is the open-source relational database software that runs on the Linux platform and functions with objects as a relational component in the database management system. It uses Structured Query Language (SQL) for accessing the data in the tables of the database, and hence it is also called Postgres. Some of this database's prominent features are that it is

highly robust and reliable the recovering process is effortless, and maintenance costs less cost and manual efforts. It is developed and maintained by the PostgreSQL Global Development Group, which is a group ofPostgreSQL developers.

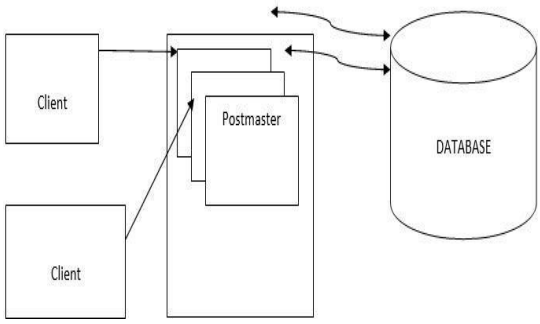


FIG 4.1: Architecture of PostgreSQL

Features of PostgreSQL:

- This supports the lockingmechanism.
- It has high availability.
- It is free and open-source software.
- This is ACID compliant.
- It has the capacity for fault tolerance.
- It also supports image, video storage.

4. IMPLEMENTATION

To implement the system, we require four tables that are added upon the existing database architecture. They are

id	from	to	message	m
1	Trij	Hema	Argentina lost the world cup final to France	http://127.0.0.1 ages/DK6yjR4S MO
2	Trij	Sam	Reminder to participate in the upcoming event	

FIG 5.1 Message Table

4.1 Message Table:

This is the table that contains all the messages that are sent by the user to others. This table helps us to understand the existing architecture that is being used in Whatsapp when users send message to one another. Thetable contains of 8 columns:

i. **id** – This is a column that keeps track of all the unique id that is required for identifying the message in the database.

ii. **from** – This is a column that contains data about the sender of a message. **to** – This is a column that contains data about the receiver of the message.

iii. **message** – This column contains the actual message that is sent by the user.

iv. **messageImage** – This column keeps track of all the image links that are shared by the user as a part of the message.

4.2 Forwards Table:

id	message_id	report_count	max_report	created_at	updated_at
1	1	0	3	16-01-2023 11:27	16-01-2023 11:27
2	1	0	3	16-01-2023 11:27	16-01-2023 11:27
3	1	2	3	16-01-2023 11:27	16-01-2023 11:30
4	1	3	3	16-01-2023 11:31	16-01-2023 11:31

FIG 5.2: Structure of Forwards Table This table helps us to map the messages oncethey are forwarded for the first time, thus creating new chains which will then further be mapped by the Hash Info table. This table consist of 6 columns:

i**.id** – This is a column that keeps track of all the unique id that is required for identifying the forwarded messages in the database and the properties of the starting message of a single chain.

ii. **message_id** – This is a column that maps the forwarded message with the original message to

avoid redundancy..

iii. **report_count** – This is a column that contains data about the number of users who have reported the messages in that specific chain.

iv. **max_report** – This column contains the threshold value for that specific chain to get triggered resulting in the activation of smart contract that will change all the hidden property of all the forwarded messages of that specific chain in the hash info table to True.

4.3 Hash Info Table:

This table consist of every forwarded message of every chain and consist of properties that are used for determining when to hide the message. It consists of 8 columns:

forward_id	hash_code	hash_pointer	reported	forwarded	hidden	created_at	updated_at
1	$2y$10$NnoQFG95BDb.G/W3RL6ue..8zYLppXD3jxujbgTmdDocRd2E3Rk2u	$2y$10$I2vIfv/SJx8EIlYf2mPqi.h2SiFUlTIxKzzDWmuVU7dN.qA6blYAy	FALSE	FALSE	TRUE	16-01-2023 11:27	16-01-2023 11:31
2	$2y$10$boCSFdkHML2HNUlWItiWNeE8qljmlEt7tdXSNMKSQBAo2r7NB2hqK	$2y$10$I2vIfv/SJx8EIlYf2mPqi.h2SiFUlTIxKzzDWmuVU7dN.qA6blYAy	FALSE	FALSE	TRUE	16-01-2023 11:27	16-01-2023 11:31
3	$2y$10$h/hBSFaIELK2JFyoo7jsMeu0VczsAC4WrsBO6Vof6jQ2kifYRQ38W	$2y$10$I2vIfv/SJx8EIlYf2mPqi.h2SiFUlTIxKzzDWmuVU7dN.qA6blYAy	TRUE	TRUE	TRUE	16-01-2023 11:27	16-01-2023 11:31
3	$2y$10$07jXAvQXXuChBwGaYPNRmOyDMxZiZOT/.rvZhA0a7rcwwbMvIvvOq	$2y$10$h/hBSFaIELK2JFyoo7jsMeu0VczsAC4WrsBO6Vof6jQ2kifYRQ38W	FALSE	TRUE	TRUE	16-01-2023 11:27	16-01-2023 11:31
3	$2y$10$2BsE.48WB2bf0OUu4On4ouHU1U1KyAVmazHa2j8c/GvAEqM1Oq43m	$2y$10$07jXAvQXXuChBwGaYPNRmOyDMxZiZOT/.rvZhA0a7rcwwbMvIvvOq	TRUE	FALSE	TRUE	16-01-2023 11:28	16-01-2023 11:31
3	$2y$10$BlCCGxLqo/Z4YCpZ3FcFPO1zisK.GzJd0Hauvb2jnCgs23VDmckqa	$2y$10$07jXAvQXXuChBwGaYPNRmOyDMxZiZOT/.rvZhA0a7rcwwbMvIvvOq	FALSE	FALSE	TRUE	16-01-2023 11:30	16-01-2023 11:31
4	$2y$10$ZelcQtwQfVlUm.GD.yXgd.ovZZG/eIs1Vu8a3ncoZdJ04YeY8ONSi	$2y$10$I2vIfv/SJx8EIlYf2mPqi.h2SiFUlTIxKzzDWmuVU7dN.qA6blYAy	TRUE	TRUE	TRUE	16-01-2023 11:31	16-01-2023 11:31
4	$2y$10$Av7TvlyGLBGHcihvoBOH2OXt2QxIdZvHmH1.pKZPCmzhXRWu5UE8i	$2y$10$ZelcQtwQfVlUm.GD.yXgd.ovZZG/eIs1Vu8a3ncoZdJ04YeY8ONSi	TRUE	TRUE	TRUE	16-01-2023 11:31	16-01-2023 11:31
4	$2y$10$sHihxGDjfO47SgGCFAoTdea0m3COCXUMAvpOZhiE1rW8.gC2MCcpK	$2y$10$Av7TvlyGLBGHcihvoBOH2OXt2QxIdZvHmH1.pKZPCmzhXRWu5UE8i	TRUE	FALSE	TRUE	16-01-2023 11:31	16-01-2023 11:31

FIG 5.3: Hash Info Table

i. **forward_id** – This is a column that helps us determine on which chain the forwarded message exist by linking it with the Forwards Table.

ii. **hash_code**– This is a column that consist of all the hash codes of every forwarded message and is used for uniquely identifying any forwarded message in the chain

iii. **hash_pointer**– This is a column that consist of all the hash pointers of every forwarded message and is used for identifying the previous block of any given forwarded message.

iv. **reported**– This is a boolean property that is used for determining whether the message has been reported by the user or not.

v. **forwarded** – This is a boolean property that is used for determining whether the message has been forwarded by the user or not.

vi. **hidden**– This is a boolean property that is used for determining whether to display the message to

the user or not.

4.4 Verification Table:

id	forward_id	verified	created_at	updated_at
1	4	FALSE	16-01-2023 11:31	16-01-2023 11:31

FIG 5.4: Structure of Verification Table

This table is used for verification and data modelling. After a message gets hidden, it will then be added to this table to be verified by machine learning algorithms. The result is then converted into a Boolean value which will then be used for determining whether or not to display every message in every chain. This table consist of 5 columns:

i. **id** – This is a column that keeps track of all the unique id that is required for identifying the messages that are added into the Verification table.

ii. **forward_id** – This column is used for mapping the Forwards table which will help determine the chain from which it was reported.

iii. **verified** – This is a boolean property that is used for determining whether the reported message has been officially verified by the organization.

4.5 Working:

When a user sends a message to another user, it gets stored in the Message table with a unique id. This message_id is what we will use to keep track of the original message throughout the other tables.

When a user does forward a message for the first time, two things happen:

1) A new chain is created which can be tracked using the Forwards table as it only stores the chain_id (or forward_id). The message_id is passed to the Forwards table to link the forward message back to the original sender and contains the necessary information about the chain such as report_count and max_report.

2) The information about that specific block will be stored in the Hash Info Table with properties such as hash_code, hash_pointer,

reported, forwarded, hidden along with the chain_id (or forward_id) to map it back to the Forward table.

When a user does forward a message that has been already forwarded, then we don't need to create a new chain but instead find the existing chain in

which the forwarded message exist and store the new block in the Hash Info table along with that chain_id (or forward_id). When a user reports a message,three things happen:

1) The reported property of that block in the Hash Info Table gets updated to True.

2) The report_count of that chain is updated by tracing back the specific chain using the chain_id (or forward_id) of that block.

3) The report_count and max_report values of that chain are checked to be equal.

If they are equal, then the hidden property of every block in that chain gets updated to True and the chain_id (or forward_id) gets added to the Verification Table with a verified property added to it. This results in the hiding of every message that has been sent to different users in the application.

If they are not equal, the process ends.When a chain_id (or forward_id) gets added to the Verification Table, the organization starts tracking the original message by combining the Message, Forward and Verification table and verifies whether the message is fake.

If the message is fake, it is updated in the Verification Table and is permanently hidden from the users. The message is then added to a data model for future purpose of identifying fake news instantly.

If the message is found out to be true, then the verified property of that chain in the Verification table gets updated to True. This will result in updating all the hidden property of that chain in the Hash Info table to True, thus allowing the messages to become visibleto the users once again.

5. ANALYSIS AND REPORT

The Right Click Authenticate method focuses more on verifying the information that is propagated which doesn't help in preventing the spread of misinformation. Our technique solves the problem by focusing more on containing the spread, after which it will be verified by the International Fact Checking Organization for authentication of the message. Moreover the system that we propose can work in end to end encrypted applications such as Whatsapp, Signal, etc. It also ensure that the accountability is maintained whenever a user sends a message, as each and every message that is forwarded

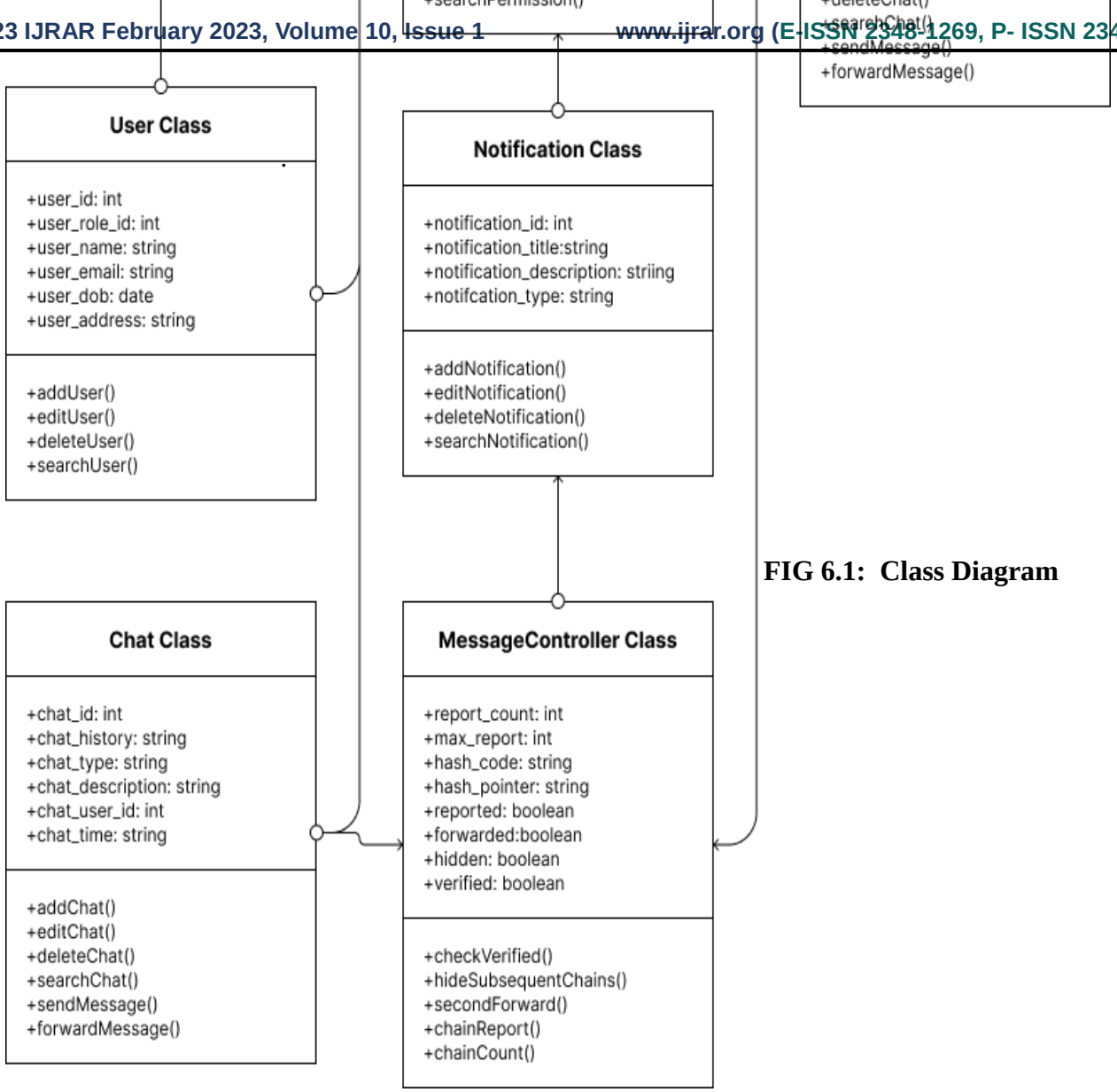


FIG 6.1: Class Diagram

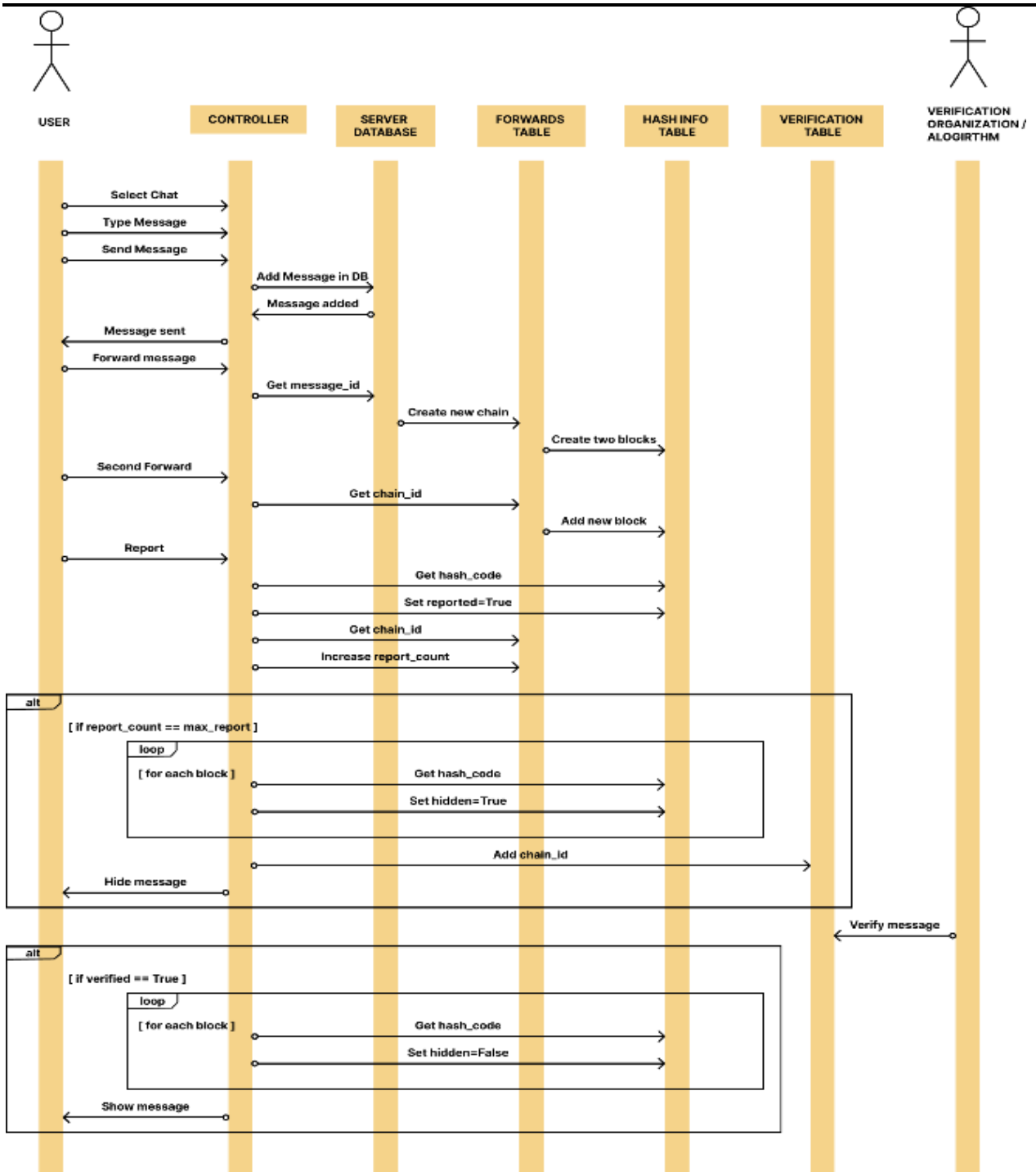


FIG 6.2 Sequence Diagram

Enhanced UX Factors	Right Click Authenticate	Value	Hash Info Feature	Value
Security	This method cannot be applied to end to end encrypted applications, therefore lacking security	0	This method can be used in end to end encrypted applications, providing security for users	1
Context Aware	In this method, we won't be able to know the previous user who shared a similar post	0	In this method, we can easily keep track of all the forwarded messages by finding the chain_id	1
Intelligence	This method doesn't use any Machine Learning models,	0	This method currently doesn't include any ML models but the results can be used to train a ML model for early tracking of fake messages	0
Progressive	This technique is built on top of the current system	1	This technique allows scalability which can be achieved by adding 3 tables in the the current system	1
Non Human Interaction	The report generated by this method doesn't require any human Intreraction	1	The hiding and displaying of message once verified is automatically performed without the need for human interaction	1

FIG 6.3: Enhanced UX factors

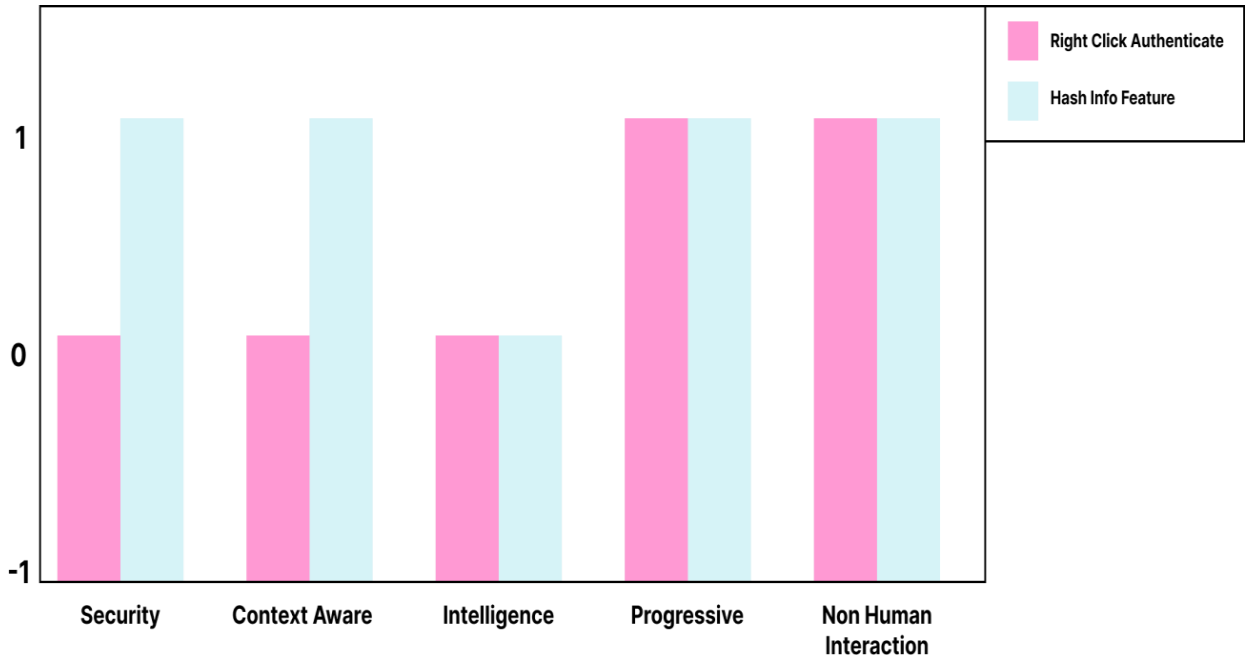


FIG 6.4: Performance of Right Click Authenticate vs Hash Info Feature

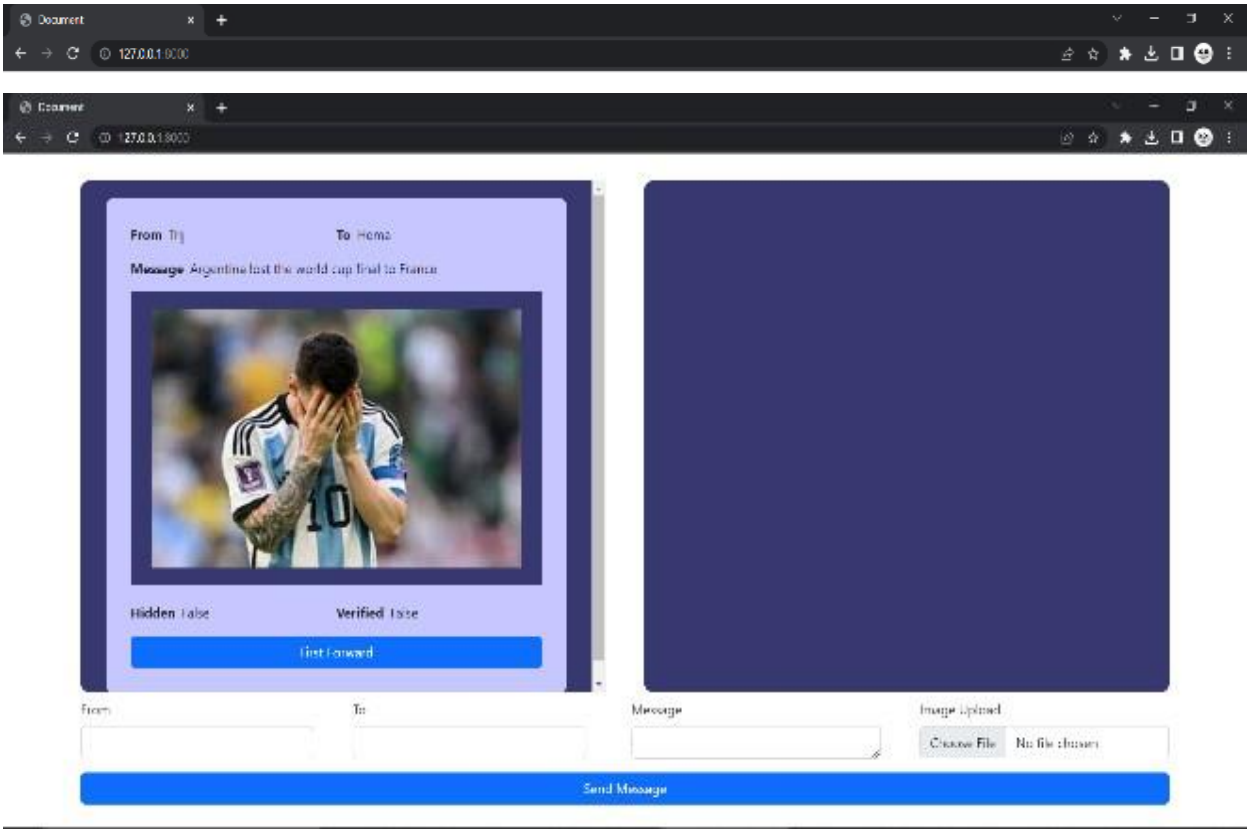
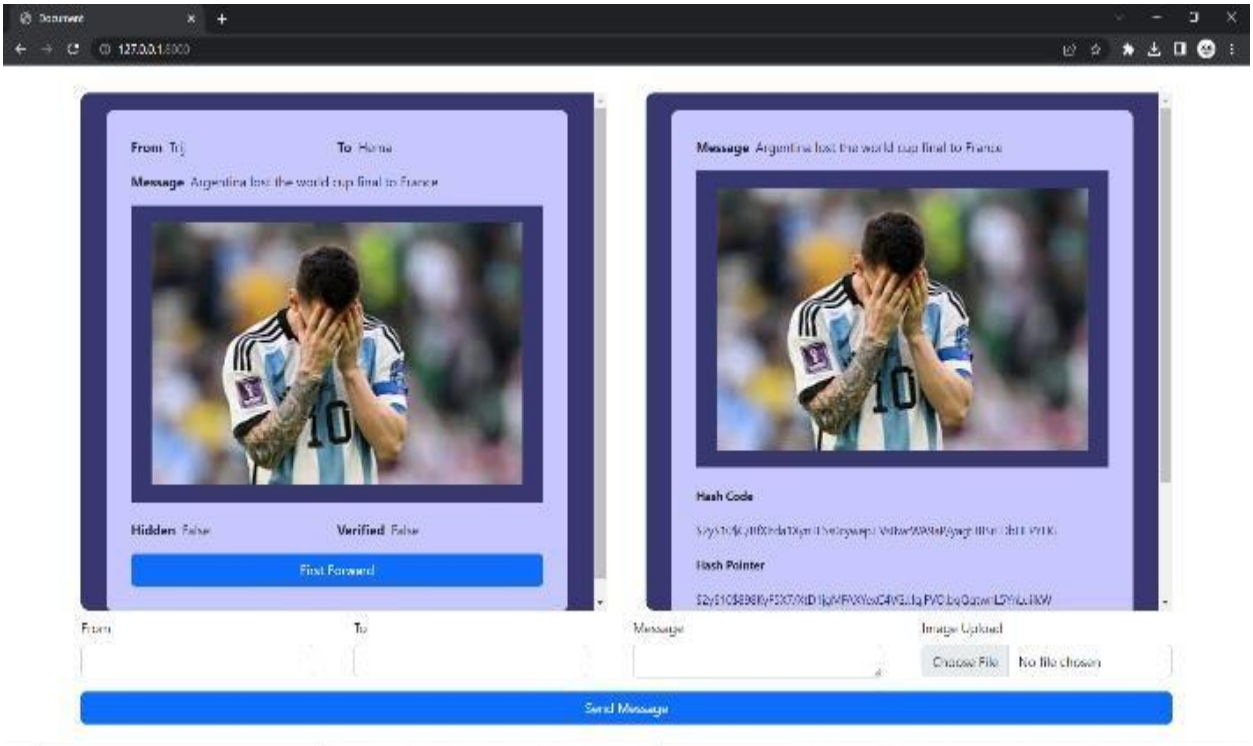


FIG 7. 1: Interface to send message:

6. SCREEN SHOTS:

FIG 7.2: Message sent by a user to another user:



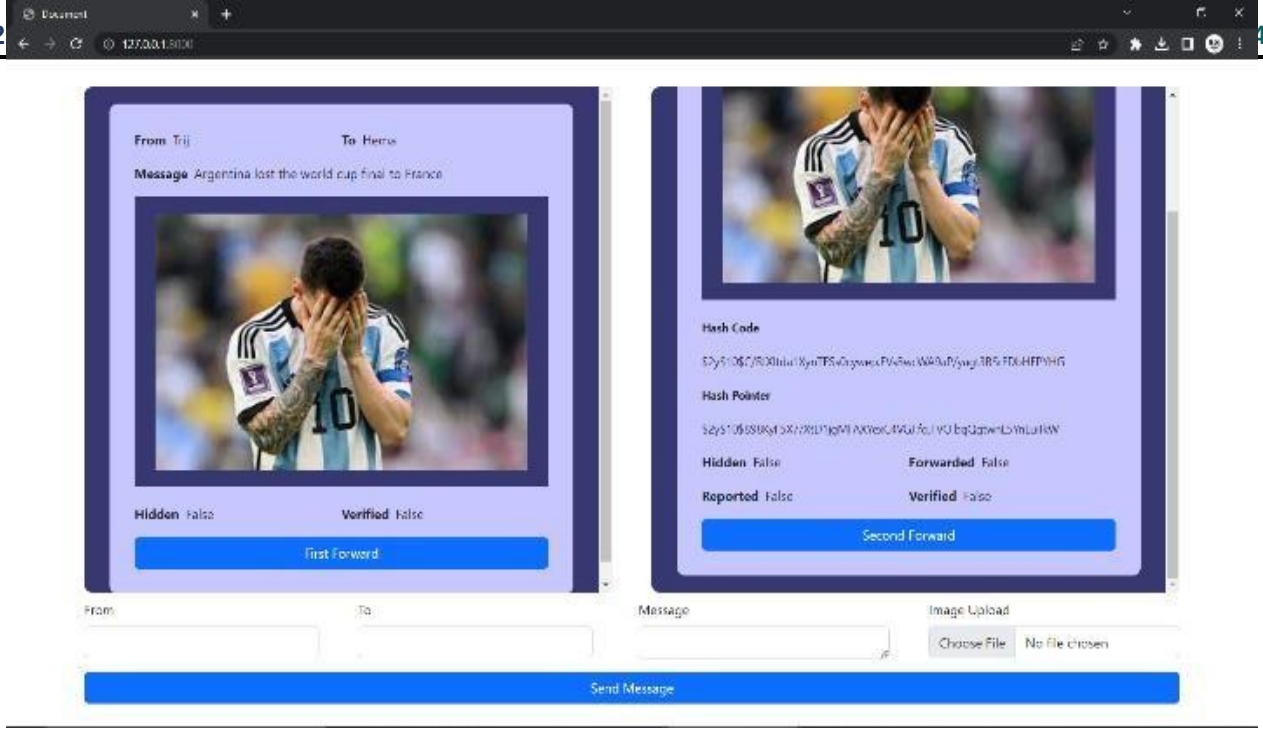


FIG 7.3: Forwarding the message for the first time by the user

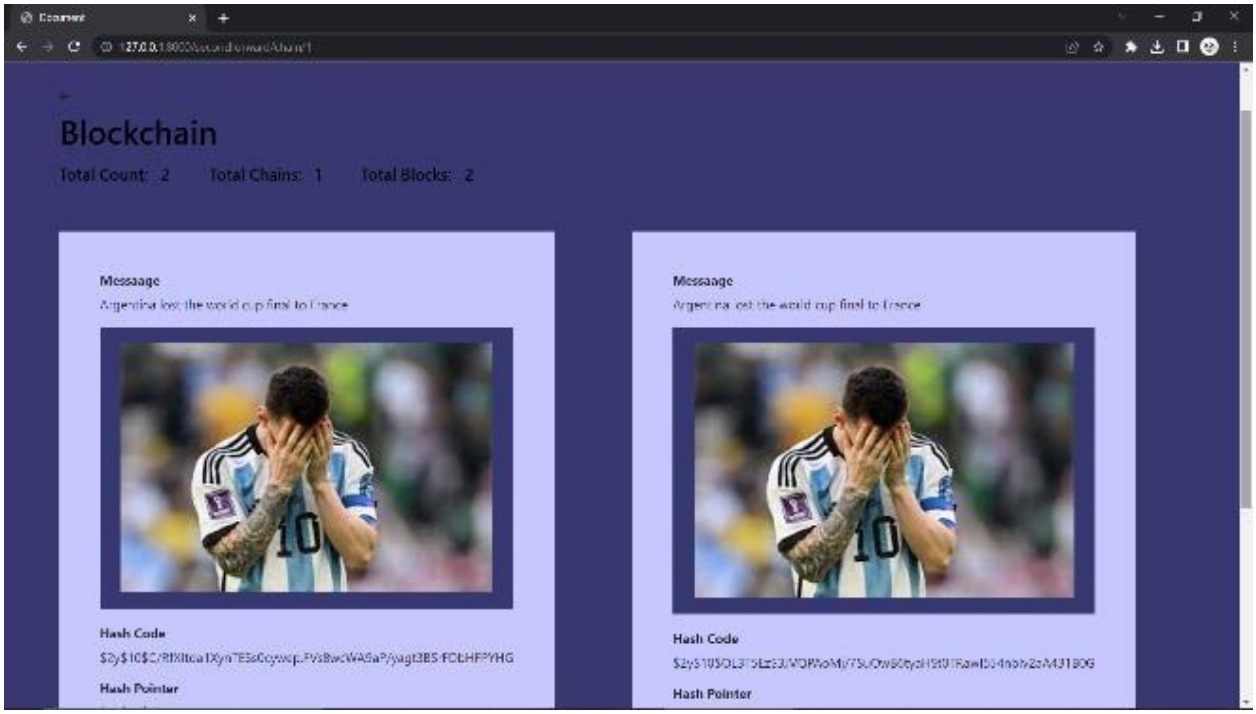


FIG 7.4: Second forward done by the user

FIG 7.5: A new chain with two blocks added to it

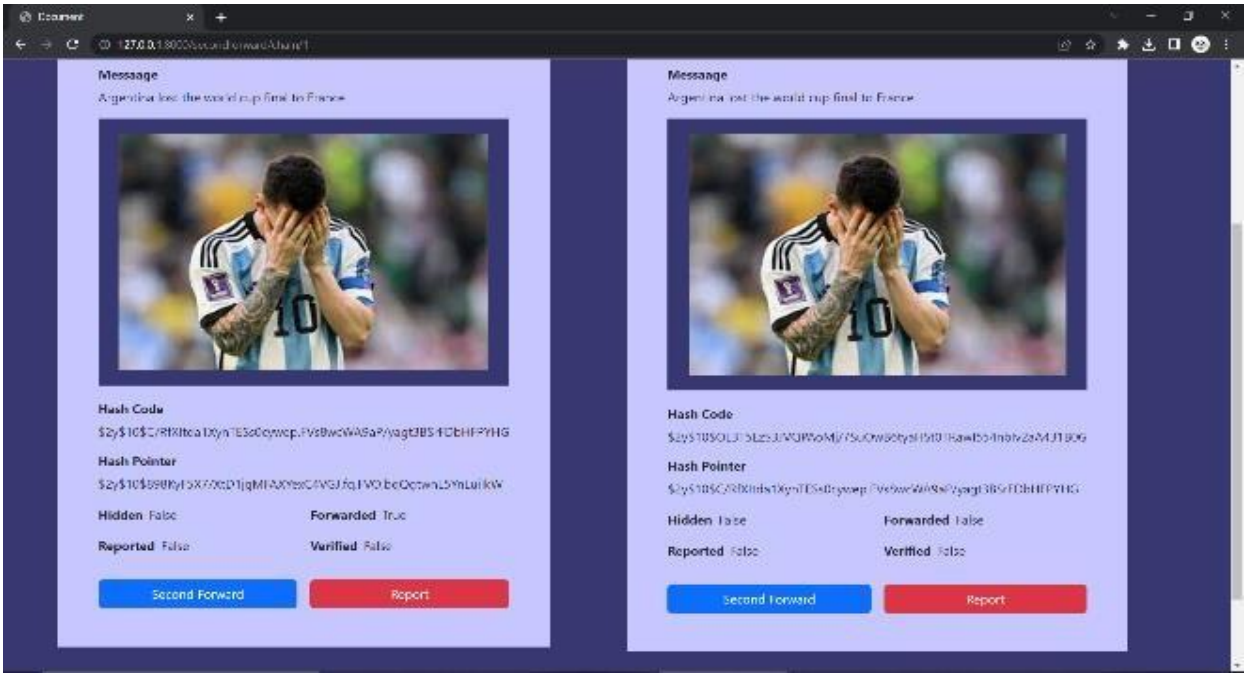
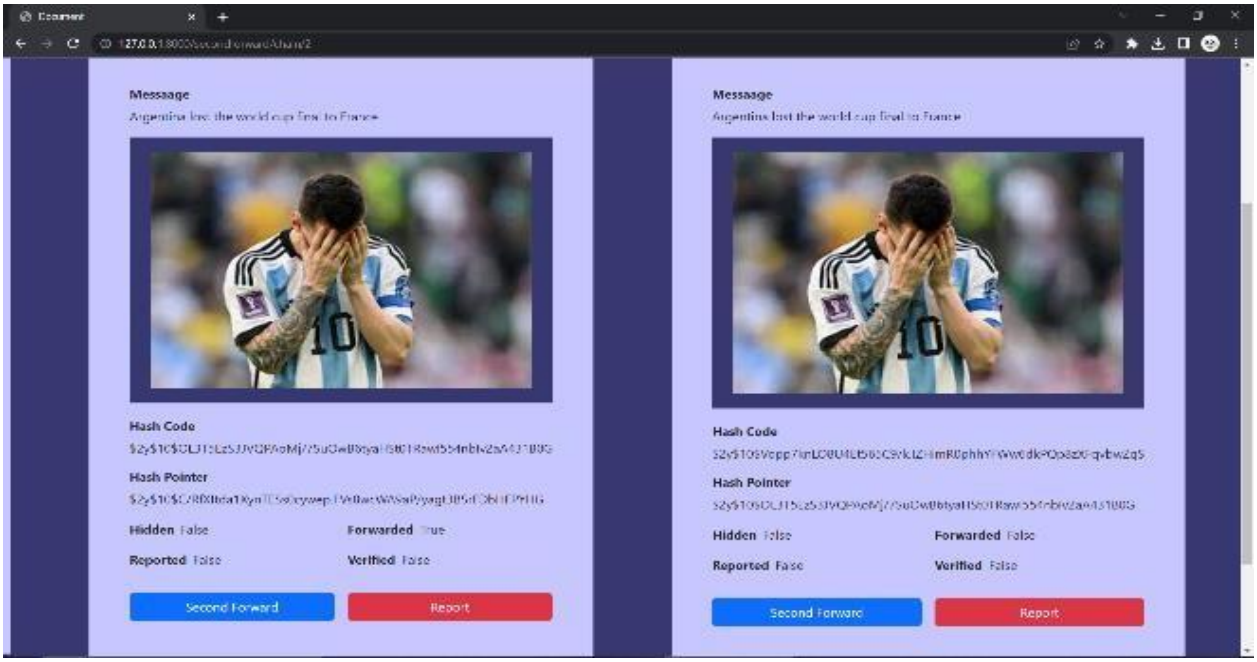


FIG 7.6: Ability for the user to report as well as forward to another user



chain

FIG 7.7: Another block added to the exisitng

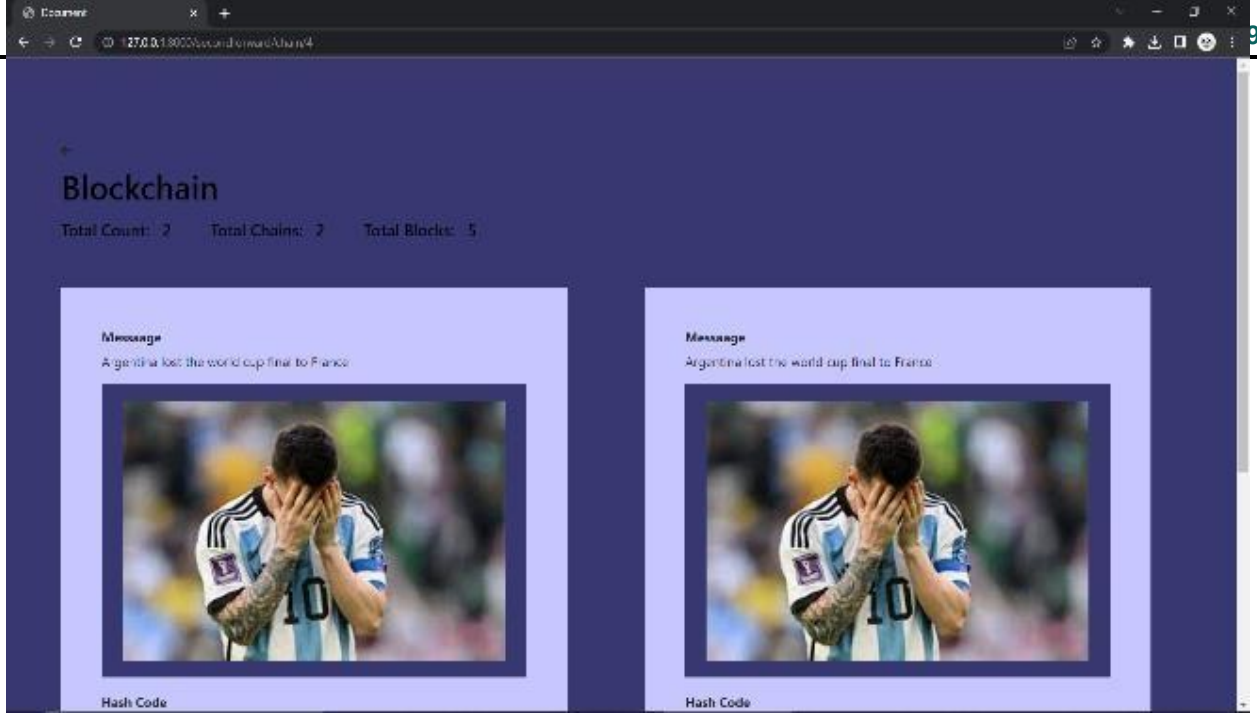


FIG 7.8: Details of the number of chains and blocks in the chains

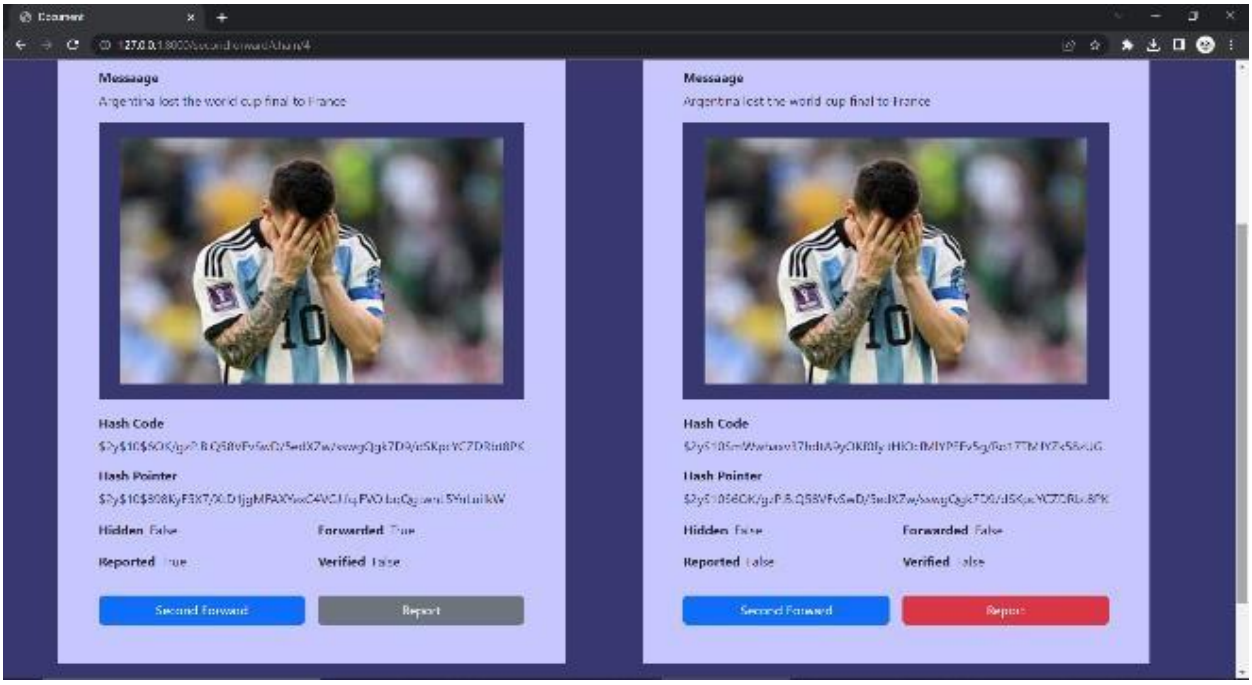


FIG 7.9: Reported blocks cannot be reported again

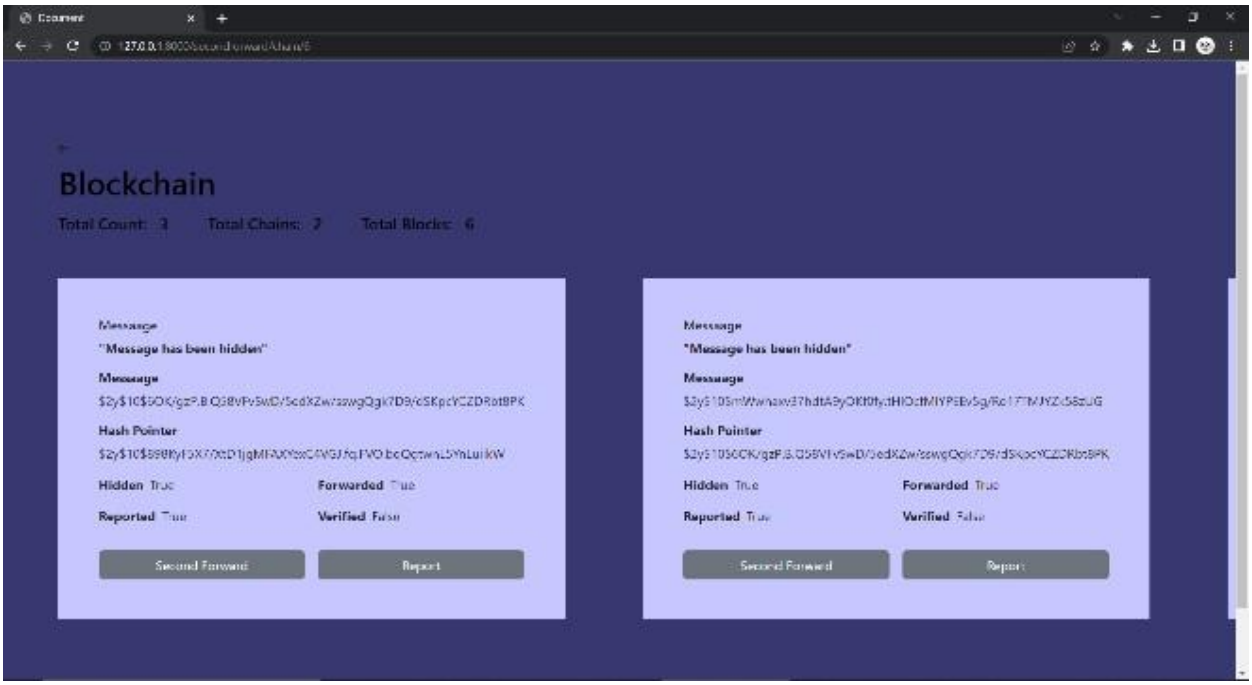


FIG 7.10: Blocks in the chain getting hidden

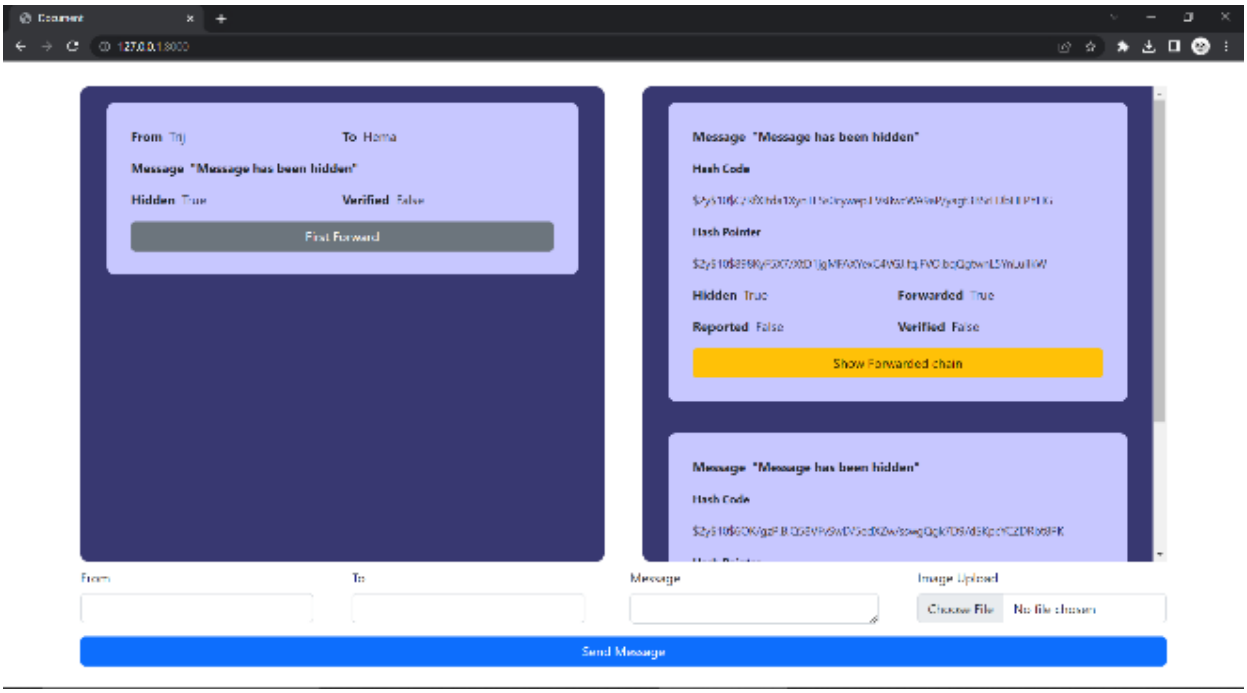


FIG 7.11: Message forwarded by the original sender gets hidden

displayed again

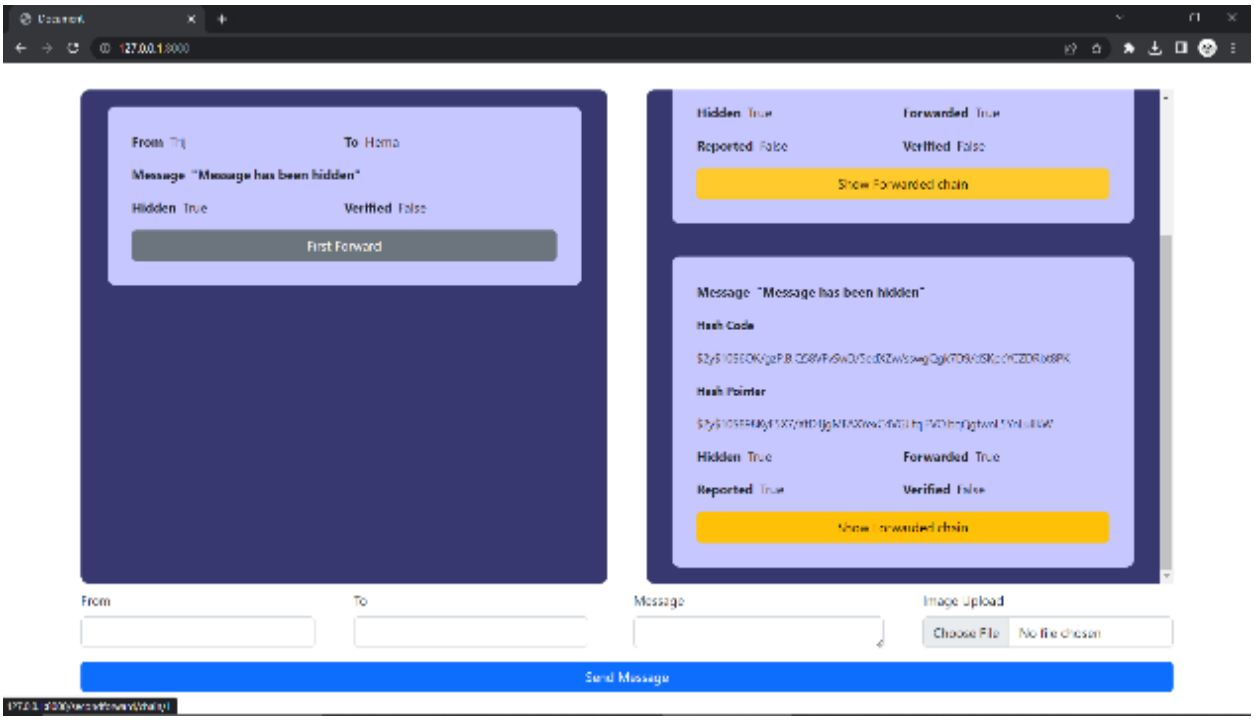


FIG 7.12: Subsequent chains getting hidden

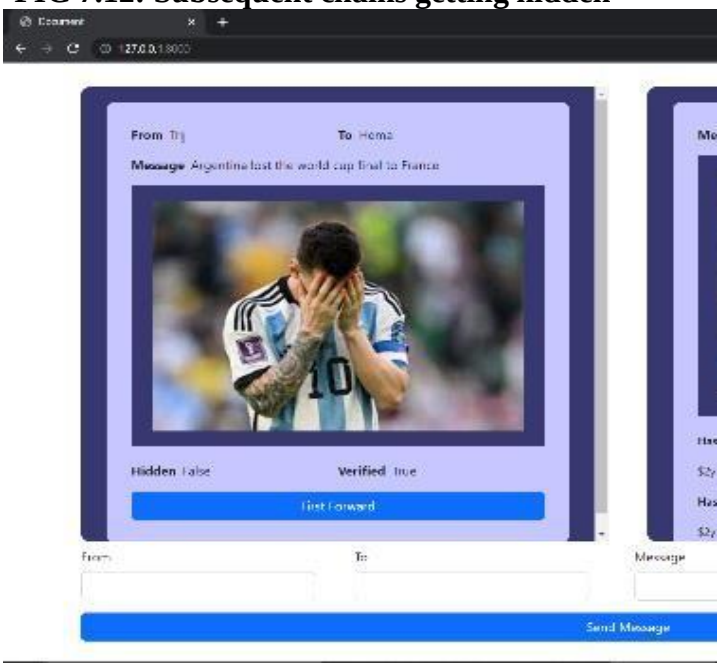


FIG 7.13: Verified messages getting

displayed as well

FIG 7.14: Subsequent chains getting

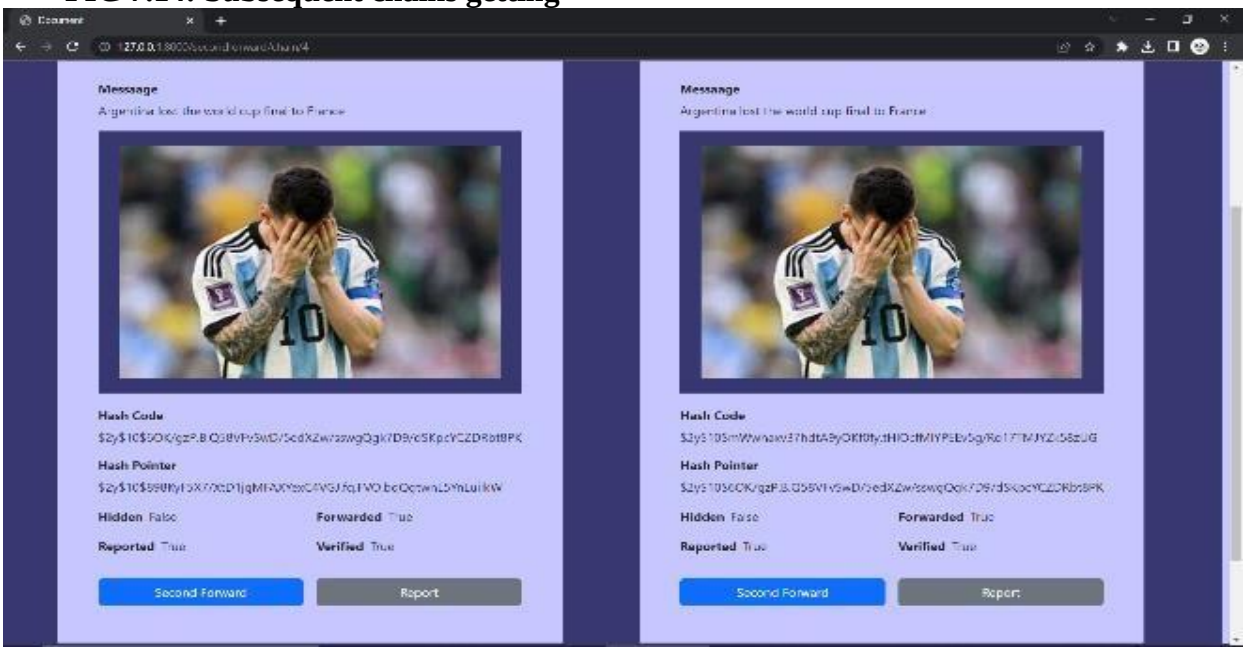


FIG 7.15: Verified blocks cannot be reported

7. CONCLUSION

The system that we proposed has shown significant improvement in the ability for users to stop the spread of misinformation. Unique ids for messages are created only when it is forwarded, which further increases efficiency as messages sent between two users don't need this hash info feature. Previous studies as shown that it is difficult to verify whether a message is real or fake but by reducing the count of people forwarding fake messages, we will be able to trust the messages that are being forwarded as every user will know that they are accountable whenever they forward a message

In future, we would be able to use the data collected from the proposed system to train a machine learning model that can then be used to identify fake news as soon as a message is reported which will reduce the chances of hiding genuine messages. Along with which a credibility system can be implemented to reward users who identify fake news after it is verified by the organization. This will prompt users to actively check for fake news within the community groups and improve the overall user experience of the application.

REFERENCES:

[1] Pardis Pourghomi, Fadi Safieddine, Wassim Masri, Milan Dordevic, How to stop spread of misinformation on social media: facebook plans vs. right-click authenticate approach.

[2] Deblina Kar, spotting misinformation to limit the impact of disruption on society by using machine learning.

[3] Panayiotis Christodoulou ,Klitos Christodoulou, Developing more reliable news sources by utilizing the blockchain technology to combat fake news.

[4] Karishnu Poddar, Geraldine Bessie Amali D, Umadevi K S, comparison of various machine learning models for accurate detection of fake news.

[5] Ranojoy Barua, Rajdeep Maity, Dipankar Minj,Tarang Barua, Ashish Kumar Layek, F- nad: an application for fake news article detection using machine learning techniques.

[6] Gowri Ramachandran, Daniel Nemeth, David Neville, Dimitrii Zhelezov, Ahmet Yalc¸in and Oliver Fohrmann, Bhaskar Krishnamachari, whistleblower : towards a decentralized and open

platform for spottingfake news.

[7] Anu Shrestha, Francesca Spezzano, online misinformation: from the deceiver to the victim.

[8] Jaynil Gaglani, Yash Gandhi, ShubhamGogate, Aparna Halbe, unsupervised whatsapp fake news detection using semantic search

[9] M. F. Mridha; Ashfia JannatKeya; Md. Abdul Hamid; Muhammad Mostafa Monowar; Md. SaifurRahman,A Comprehensive Review on Fake News Detection With Deep Learning

[10] Hager Saleh, Abdullah Alharbi, SaeedHamood Alsamhi, OPCNN-FAKE: Optimized Convolutional Neural Network for Fake News Detection.

[11] Matthew Carter; Michail Tsikerdekis; Sherali Zeadally,Approaches for Fake Content Detection: Strengths and Weaknesses to Adversarial Attacks.

[12] Tao Jiang; Jian Ping Li; Amin UlHaq; Abdus Saboor; AmjadAliA Novel Stacking Approach for Accurate Detection of Fake News.

[13] Shiwen Ni; Jiawen Li; Hung-Yu Kao, MVAN: Multi-View Attention N

[14] Khubaib Ahmed Qureshi; Rauf Ahmed Shams Malick; Muhammad Sabih; HocineCherifi,Complex Network and Source Inspired COVID-19 Fake News Classification on Twitter.

[15] Muhammad Umer; Zainab Imtiaz; SaleemUllah; ArifMehmood; Gyu Sang Choi; ByungWon On,Fake News Stance Detection Using Deep Learning Architecture(CNN-LSTM).

[16] Estée Van Der Walt; Jan Eloff, Using Machine Learning to Detect Fake Identities: Bots vs Humans.

[17] Mohamed K. Elhadad; Kin Fun Li; Fayez Gebali,Detecting Misleading Information on COVID-1

[18] Hyewon Choi; Youngjoong Ko, Using Adversarial Learning and Biterm Topic Model for an Effective Fake News Video Detection System on Heterogeneous Topics and Short Texts

[19] AnkurGupta, NeerajKumar; Purnendu Prabhat; Rajesh Gupta; SudeepTanwar; Gulshan Sharma, Pitshou N. Bokoro, Ravi Sharma,Combating Fake News: Stakeholder Interventions and Potential Solutions.

[20] DhirenRohera , HarshalShethna, Keyur Patel, UrvishThakker , SudeepTanwar, Rajesh Gupta, Wei-Chiang Hong, Ravi Sharma ,A Taxonomy of Fake News Classification Techniques: Survey and Implementation Aspects.

[21] Wesam Shishah, JointBert for Detecting Arabic Fake News.

[22] Myunghoon Kang; JaehyungSeo; Chanjun Park; HeuiseokLim,Utilization Strategy of User Engagements in Korean Fake News Detection.

[23] Abdullah Tariq,AbidMehmood; MouradElhadef, Muhammad Usman Ghani Khan, Adversarial Training for Fake News Classification