



*DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,  
SHARDA SCHOOL OF ENGINEERING AND TECHNOLOGY,  
SHARDA UNIVERSITY, GREATER NOIDA*

## **FAKE NEWS DETECTION USING BLOCKCHAIN**

*A project submitted in partial fulfillment of the requirements for the degree of  
Bachelor of Technology in Computer Science & Engineering*

**SUBMITTED BY:**

**Jai Sanger(2019628545)  
Taslim Raza Ahmad (2019635844)  
Veetu Kaushik (2019628545)**

**SUPERVISED BY:**

**Dr. Renu Mishra  
Associate Professor  
Department of Computer Science & Engineering  
SET**

**May, 2023**

## **CERTIFICATE**

This is to certify that the report entitled “Fake News Detection Using Blockchain” submitted by Jai sanger(2019628545), Taslim Raza Ahmad(2019635844), Veetu Kaushik(2019521381) to Sharda University, towards the fulfillment of requirements of the degree of Bachelor of Technology is record of bonafide final year Project work carried out by him/her in the Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University. The results/findings contained in this Project have not been submitted in part or full to any other University/Institute for award of any other Degree/Diploma.

Signature of Supervisor

**Dr Renu Mishra**

Associate Professor

Signature of Head of Department

**Prof. (Dr.) Nitin Rakesh**

(Office seal)

Place:Sharda University

Date:

**Signature of External Examiner**

## **ACKNOWLEDGEMENT**

A major project is a golden opportunity for learning and self-development. We consider our self very lucky and honored to have so many wonderful people lead us through in completion of this project. First and foremost we would like to thank Dr. Nitin Rakesh, HOD, CSE who gave us an opportunity to undertake this project. My grateful thanks to Dr Renu Mishra for her guidance in our project work who in spite of being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where we would have been without her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Name and signature of Students

Jai Sanger (2019628545)

Taslim Raza Ahmad (2019635844)

Veetu Kaushik (2019521381)

## **ABSTRACT**

The online social networks facilitate to share information among the users based on their interests. The specific information being shared by a user may be legitimate or fake. Often, misinformation propagated by users and groups can create chaos and riots in the worst circumstances. Social media network is one of the important parts of human life based on the recent technologies and developments in terms of computer science area. This environment has become a famous platform for sharing information and news on any topics and daily reports, which is the main era for collecting data and data transmission. There are various advantages of this environment, but in another point of view there are lots of fake news and information that mislead the reader and user for the information needed. Lack of trust-able information and real news of social media information is one of the huge problems of this system. Therefore, there is a need to establish a new robust system to check the information authenticity within the network . Nowadays, a third party like ALT news and Cobrapost check the authenticity of the information, but it takes too much time to validate it. Going through the different model proposed by different authors using various technology such as Artificial intelligence , machine learning, blockchain, polygraph, natural language processing etc . the main problem with the Prevailing model available are as follows Traceability, credibility, new user authentication, Trust model, Ledger design, credible peer , authenticity . To overcome this problem, We have proposed a machine learning-based system that integrates various blockchain and natural language processing (NLP) components to identify fake news and make better predictions about fake user accounts and posts. The Reinforcement Learning technique is applied for this process. To improve this platform in terms of security, the decentralized blockchain framework applied, which provides the outline of digital contents authority proof. More specifically, the concept of this system is developing a secure platform to predict and identify fake news in social media networks.

# CONTENTS

<b>TITLE .....</b>	<b>i</b>
<b>CERTIFICATE.....</b>	<b>ii</b>
<b>ACKNOWLEDGEMENT.....</b>	<b>iii</b>
<b>ABSTRACT.....</b>	<b>iv</b>
<b>LISTOF FIGURES .....</b>	<b>vi</b>
<b>LISTOF TABLES .....</b>	<b>vii</b>
<b>CHAPTER1: INTRODUCTION.....</b>	<b>1</b>
1.1 Project Overview .....	1
1.2 Expected Outcome .....	2
1.3 Blockchain Technology Overview .....	2
1.4 Reinforcement Learning Overview .....	4
<b>CHAPTER2: LITERATURE REVIEW .....</b>	<b>8</b>
2.1 Existing Work .....	8
2.2 Research Gap .....	11
2.3 Problem Statement.....	11
<b>CHAPTER3: PROPOSED METHODOLOGY.....</b>	<b>12</b>
3.1 System Architecture .....	12
3.2 System Design .....	14
3.2.1 Use Case .....	14
3.2.2 Class Diagram .....	15
3.2.3 Activity Diagram .....	17
3.2.4 Sequence Diagram.....	18
3.2.5 Collaboration Diagram .....	19
3.2.6 Component Diagram .....	19
3.2.7 Deployment Diagram .....	20
<b>CHAPTER4: IMPLEMENTATION .....</b>	<b>21</b>
4.1 Implementation.....	21
4.2 Software Environment.....	25
<b>CHAPTER5: TESTING .....</b>	<b>30</b>
5.1 Testing.....	30
5.2 Test Cases.....	33

<b>CHAPTER6: RESULT AND OUTPUT .....</b>	<b>35</b>
6.1 Output .....	35
6.2 Analysis .....	43
<b>CHAPTER 7: CONCLUSION.....</b>	<b>44</b>
<b>CHAPTER 8: REFERENCES.....</b>	<b>45</b>
<b>ANNEXURE:LIST OF PUBLISHED PAPER.....</b>	<b>47</b>

## LIST OF FIGURES

Fig.3.1.1 System Architecture .....	12
Fig.3.1.2 Data Flow Diagram .....	13
Fig.3.2.1 Usecase Diagram.....	15
Fig.3.2.2 Class Diagram .....	16
Fig.3.2.3 Activity Diagram.....	17
Fig.3.2.4 Sequence Diagram.....	18
Fig.3.2.5 Collaboration Diagram.....	19
Fig.3.2.6 Component Diagram .....	20
Fig.3.2.7 Deployment Diagram .....	20
Fig.4.1.1 Dataset Value .....	22
Fig.4.1.2 Smart Contract Function .....	22
Fig.4.1.3 Generation Of Private Key And Account.....	23
Fig.4.1.4 Blockchain Deployment.....	24
Fig.4.1.5 Blockchain Function .....	24
Fig.5.1.1Static Testing.....	31
Fig.5.1.2 Structural Testing .....	32
Fig.5.1.3 Blackbox Testing .....	33
Fig.6.1.1 IPFS Server .....	35
Fig.6.1.2 IPFS Server Started .....	36
Fig.6.1.3 User Interface .....	36
Fig.6.1.4 New User Sign-up .....	37
Fig.6.1.5 Sign-up Process Completed .....	37
Fig.6.1.6 User login Screen .....	38
Fig.6.1.7 Load Buzz Feed Dataset.....	39
Fig.6.1.8 Data-Set.....	39
Fig.6.1.9 Trained Dataset with Algorithm.....	40

Fig.6.1.10 Post News Screen .....	41
Fig.6.1.11 Post News Screen With File.....	42
Fig.6.1.12 Detection Result .....	43

## **List of Tables**

Table.2.1.1 Existing Work .....	9
Table.5.2.1 Test Cases .....	33

# CHAPTER 1

## INTRODUCTION

### 1.1 Project Overview

Information has been propagated in mass from ancient times to modern times. But since last one Decade news has been propagated digitally. Digital propagation has its own benefit like widespread of news in very less time and to Maximum Population coverage But later in the decade this feature has given rise to big problem. A growing number of People uses social network in todays era to stay informed and share article, Post, Video, News etc . With the increasing number of people in social media platform it has become easy to spread misinformation or false news to mass in very less time. We propose a combination of blockchain and natural language processing (NLP) to use machine learning techniques to detect fake news and better predict counterfeiters and advertisers. Reinforcement learning techniques are used for this process. To secure the platform, a distributed blockchain framework is used that provides proof of rights to digital content. More specifically, the idea of the system is to create a secure platform for predicting and detecting fake news on the social media network. Using Reinforcement Deep Learning algorithm to detect fake news and then applying Blockchain technology to provide security to NEWS data. Reinforcement algorithm will match similarity between old news and current news and if news contains more similarity then it will detect as Fake news and penalized the user and if news is REAL then algorithm will reward user and then store NEWS in Blockchain. Blockchain store each news as block/transaction and associate each block with unique hashcode and then store this block in multiple nodes as Decentralized storage and if one node is down then Blockchain will access News from other working nodes.



## **1.2 Expected Outcome**

The expected outcome after the completion of project is expected to detect the news which is given to the system is Fake or True news, by taking input from the user and using its algorithm it should be able to detect whether the news is genuine or fake news in efficient manner.

## **1.3 Blockchain Technology Overview**

We created the two methodologies as simulations in this project, one is blockchain and another in reinforcement learning. Thus we will first give detailed description of the these two technologies. Then we will go further into the system design and working.

Blockchain technology is a decentralized, distributed ledger that records transactions in a secure, transparent, and tamper-proof way. It was first introduced in 2008 as the underlying technology behind the digital currency Bitcoin, but has since been applied to various industries beyond just finance. At its core, a blockchain is essentially a chain of blocks containing information. Each block contains a hash (a unique identifier), a timestamp, and a set of transactions. When a new transaction is added to the blockchain, it is first verified by a network of nodes (or computers) in the network. These nodes compete to solve complex mathematical puzzles to validate transactions, and once a transaction is validated, it is added to the blockchain as a new block. Once a block is added to the blockchain, it is immutable, meaning that it cannot be altered or deleted. This is because each block contains a reference to the previous block in the chain, creating a chain of blocks that is resistant to tampering. This makes the blockchain a highly secure and reliable way to record transactions, as it is virtually impossible to alter any data without it being detected by the network. Blockchain technology is designed to be transparent, meaning that anyone can view the contents of the blockchain. However, the identity of the participants in a transaction can be kept private using various cryptographic techniques. This allows for a high degree of privacy and confidentiality in transactions, while still ensuring that the underlying data is transparent and accessible to all parties involved. In addition to Bitcoin, blockchain technology has been applied to a variety of other industries, including healthcare, supply chain management, and real estate. It has the potential to revolutionize how data is stored, shared, and verified, creating a more secure and efficient global economy. The technical details of blockchain technology:

**Hash Functions:** A hash function is a mathematical algorithm that takes input data of any size and outputs a fixed-size alphanumeric string. This string is unique to the input data and is used as a digital fingerprint. In blockchain, every block is assigned a hash function that represents the block's contents. The hash function is used to verify the integrity of the data in the block.

**Distributed Ledgers:** A distributed ledger is a database that is spread across a network of nodes. Each node has a copy of the ledger, which is updated whenever a new block is added to the blockchain. This creates a decentralized system where there is no central authority controlling the network. Instead, transactions are verified and validated by a network of nodes, making it highly resistant to hacking or data breaches.

**Consensus Mechanisms:** Consensus mechanisms are used in blockchain technology to ensure that all nodes in the network agree on the validity of transactions. There are several consensus mechanisms used in blockchain, including Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). These mechanisms rely on a network of nodes competing to solve complex mathematical puzzles to validate transactions and add them to the blockchain.

**Smart Contracts:** Smart contracts are self-executing contracts that automatically execute when certain conditions are met. They are coded in a programming language and run on the blockchain. Smart contracts can be used to automate a wide range of processes, such as payment processing, supply chain management, and insurance claims processing. They can also reduce the need for intermediaries, such as lawyers or financial institutions, which can save time and reduce costs for businesses.

Blockchain is a decentralised (save data at numerous nodes rather than a single centralised node) server that records information about products as blocks of transactions and generates hash codes for those details for each block. The current block and its corresponding hash code are then maintained at several nodes (decentralised). Blockchain verifies all of the nodes' hash codes prior to storage any new transactions; if block data is not altered, all nodes' hash code verifications are successful, and new transactions are stored; if confirmation fails-at-any node, however, Blockchain considers that-node to have been attacked and instructs it to recover with lawful blocks. By using these techniques, which we refer to as "PROOF of Work," we can guarantee that customers will obtain accurate product information. With POW customers will become more reliable on the

supply chain because they don't have to be worry about the quality of the product they receive. Within the blockchain there is hash function with the help of which verification process carries out. The generation algorithm is described in the below paragraph. A hash function converts an information string (numeric, letter sets, or multimedia items) of arbitrary length to a single line of a particular length. The acceptable piece length might differ depending on the hashing algorithm calculation used (for example, 32 bits, 64 bits, 128 bits, or 256 bits). The outcome is a hash that is of respectable length. The cryptography outcome of a hash computation is also this hash. The demarcation below aids in our comprehension. The characteristics of the hash algorithm are as follows: It produces a unique output, also known as a hash. There is only one way it can be used. In the context of cryptocurrencies like Bitcoin, this cryptographic hash function is utilized by the consensus process on the blockchain. A computerized unique fingerprint impression or condensation of a cluster of info is a cryptographic hash. Cryptographic hash functions take transactions as input and process them through a hashing process to produce a fixed-size output. Since the hashing function is one-way, the resulted hash cannot be utilised to get the complete text. This differs from conventional cryptographic processes like encoding, where you encode anything using the key and then decode it to restore it back to its initial state.

## **1.4 Reinforcement Learning Overview**

Reinforcement learning (RL) is a subset of machine learning that involves training an agent to make decisions by rewarding or punishing it for its actions. The goal of RL is to develop intelligent systems that can learn from their experiences to make better decisions in the future. The basic idea behind RL is to create an environment in which an agent can interact with its surroundings and learn from its actions. The environment provides feedback in the form of rewards or punishments for each action the agent takes. The agent's goal is to maximize its cumulative reward over time by learning from its experiences. In RL, an agent makes a decision by selecting an action from a set of possible actions. The environment responds to the action with a reward, which is a numerical value that reflects the quality of the action taken. The agent's goal is to maximize the cumulative reward it receives over time. The RL framework consists of three key components: the agent, the environment, and the reward function. The agent is the decision-making entity that interacts with the environment. The environment is the system in which the agent operates. The reward function is the function that assigns a numerical value to each action the agent takes. The RL algorithm

works by repeatedly exposing the agent to the environment and updating its decision-making process based on the feedback it receives. The agent learns to make better decisions by exploring the environment and adjusting its actions based on the rewards it receives.

One common RL algorithm is called Q-learning. Q-learning is a model-free RL algorithm, which means that it does not require prior knowledge of the environment. In Q-learning, the agent learns a Q-function, which is a mapping between states and actions and their expected rewards. The Q-function is updated using the Bellman equation, which is a recursive formula that computes the expected reward for taking an action in a given state. Another common RL algorithm is called policy gradient. Policy gradient is a model-based RL algorithm, which means that it requires knowledge of the environment. In policy gradient, the agent learns a policy, which is a mapping between states and actions. The policy is updated using gradient descent, which is a technique for optimizing functions. RL has many applications in fields such as robotics, finance, and gaming. For example, RL can be used to train robots to perform complex tasks, such as navigating through a cluttered environment. RL can also be used to develop trading algorithms that can learn to make better investment decisions based on market data. In gaming, RL can be used to train agents to play complex games, such as chess or Go. Despite its potential, RL still faces many challenges. One major challenge is the problem of exploration vs. exploitation. The agent must balance the desire to explore new actions with the need to exploit actions that have already been shown to be successful. Another challenge is the problem of credit assignment. The agent must determine which actions led to a particular reward, which can be difficult in complex environments. Another challenge of RL is the issue of generalization. The agent needs to be able to apply what it has learned in one environment to new, similar environments. This requires the agent to abstract away from specific details of the environment and learn more general rules and concepts. RL also requires a large amount of data to train an agent effectively. This is because the agent needs to explore a wide range of actions and receive feedback on those actions to learn from them. Collecting this data can be time-consuming and expensive, especially in complex environments. One way to address the challenge of data efficiency is through the use of simulation. By creating a simulated environment, the agent can be trained on a larger and more diverse dataset than would be possible in the real world. However, the use of simulation also introduces the problem of the "sim-to-real" gap, where the agent's performance in the simulated environment does not transfer well to the real world. Another area of active research in RL is the development

of more advanced algorithms that can handle more complex environments and tasks. For example, deep reinforcement learning (DRL) uses neural networks to represent the Q-function or policy, allowing for the representation of more complex functions. DRL has been successfully applied to a wide range of tasks, such as playing Atari games, mastering the game of Go, and controlling humanoid robots. In addition to algorithmic advances, there is also ongoing research in RL around topics such as multi-agent RL, where multiple agents must learn to cooperate or compete with each other, and inverse reinforcement learning, where the goal is to learn the reward function from expert demonstrations.

In-depth learning through reinforcement this deep learning algorithm mimics how the human brain makes choices by taking into account three processes.

- 1) Environment: The working space where Agent and State are present is the surroundings.
- 2) Agent: Agent is regarded as an act that will be carried out in accordance with the state.
- 3) State: refers to the situation at hand. People, for instance, perform or act in response to their environment and state when watching television.

If a viewer feels that a currently running channel on TV isn't good, he or she could choose to alter the channel or the programme, and this act or choice could go on until the viewer finds a good show and receives incentives. Asynchronous: This approach employs numerous agents, every one of which has a network of its own settings and an exact replica of the environment. In contrast to other well-known DRL algorithms like Deep Q-Learning, that utilizes just one agent and a single environment. These agents engage in asynchronous interactions with the settings in which they operate, learning from each encounter. A global system controls each agent. Each agent adds to the overall understanding of the global system as it increases its understanding. Since there is a global the system, each of the agents can access a wider variety of training information. This configuration closely resembles the environment in which people actually live, where each person learns from the observations of others, improving the "global network" as a whole. As an extension, we have now included an asynchronous multi-agent system that continuously learns from the model in order to maximise efficiency. We employed a single agent in the proposed study and, as an extension, many agents, which will aid in obtaining higher reward values. Multi agents will keep getting knowledge from training model and optimize performance. It's similar to human

where multiple peoples gain knowledge and then apply that knowledge to get better result. Numerous applications, such as those in agriculture and food supply chains, can benefit from the usage of multi-agent systems. For instance, in a supply chain management system, agents might be trained to track the quantity of stock, the quality of the product, and logistics of transportation. They may jointly improve the effectiveness of the supply chain by decreasing waste, increasing efficiency, and raising product quality by exchanging information with other agents.

## CHAPTER 2

### LITERATURE SURVEY

#### 2.1 Existing work

With the advance utilization of social media applications in daily life, fake posting cause a mess in various platforms. This problem is identified and addressed by various authors to find a proper and suitable news on the topic searched. They all explored and found that, machine learning and blockchain can be combine together to overcome fake news sharing issue.

Author Name	Advantages	Disadvantages	Methodology
Nicollas R. [2]	computational expressive examination in light of NLP	It has 86% exactness and 94% accuracy	It Uses NLP and ML Calculations for calculating the exactness of the report.
Guanfeng Liu, [3]	Idea of Quality of Trust (QoT) is used to show the level of reliability	better but not 100% accurate.	Monte Carlo-based estimate calculation.
Maria Nefeli Nikiforos, [4]	gives a spic and span informational index of 2,366 English- tweets	Covers only particular event not all and still in Research stage	Two ML models were utilized in preliminaries
Adline Rajasenah [5]	different exemplary ML and deep learning systems	better than the other wokrs but not 100% accurate.	This research is completely based on deep learning models.

Xishuang Dong [6]	This paper is also effective even with limited labeled data.	very limited labeled data is available, which is inadequate for the supervised model	proposed a deep semisupervised learning model of limited labeled data.
S. Kumar, [7]	achieved accuracy of 88.78%.	Tested 1356 instances so not a fully tested model.	Used(CNNs), (LSTMs), ensemble methods, and attention mechanisms.
P. Bahad, [8]	Bi-directional LSTM model	2 publicly available unstructured news articles datasets used	Bi-directional LSTM-recurrent neural network.
G. Sansonetti, [9]	used two approaches online and offline analysis. online content	offline analysis is completely dependent on individual	Used deep learning for offline and online is done through classification

Table2.1.1 Existing work

The review [1] takes a gander at the extreme changes in proficient political correspondences that are occurring in the computerized age. The heuristic possibilities of framework humanistic system, intuitive methodology, and hypothesis of informative activity can be generally integrated into the examinations on account of the multiparadigm approach's capability as the strategic establishment.. Correspondence innovation for "fake news" has the accompanying elements: rate with which these messages are spread, wide allure, and trouble finding .They have additionally started to "blockcade" political and correspondence between genuine political players. To ensure the veracity of the data that is circulated and the shortfall of sham disinformation, specialists should apply extra exertion in dissecting web reports.In [2], to distinguish counterfeit news in virtual entertainment posts, they utilize a computational expressive examination in light of natural



language processing and ML calculations are utilized. As far as identification quality, even with a layered decrease to one-sixth of the quantity of unique elements, 86% exactness and 94% accuracy stick out. While our strategy can give a high certainty file to deciding if news is real or fake, it has a low above. As a part of various improving exercises in [3], they first present an original complex informal organization structure and a pristine idea of Quality of Trust (QoT) to show the ability to ensure a specific level of reliability in trust evaluation. The ideal social trust course decision is in this manner exhibited as a NP-Complete Multi-Constrained Optimal Path (MCOP) assurance issue. To resolve this issue, they present MONTE K, a proficient Monte Carlo-based estimate calculation. Our examination on a genuine world dataset of interpersonal organizations shows that our proposed calculation beats existing ones as far as proficiency as well as the nature of the social trust channels picked. In [4], The quantity of individuals who utilize virtual entertainment and online data has soar as an immediate consequence of the quick improvement of organization administrations. These stages are utilized by pernicious records to spread misleading data and publicity across enormous client organizations. Thusly, a computerized framework for recognizing trickery and misleading data is required. This study gives a spic and span informational index of 2,366 English-language tweets about Hong Kong's occasions in August 2019 and a clear cut calculation for etymological and network-based misleading news recognition. Two ML models were utilized in preliminaries to approve our strategy, and it performed better compared to past examinations. In [5], Machine learning is especially important when it comes to fake social media posts because of the scope of ecological and social challenges. A false or true message that goes viral can be created by anyone. During general elections, political parties in nations like India use social media groups to spread fake messages across the nation. While some of the messages might be genuine, many of them are fakes. Social media groups can be used to send spam messages and fake messages with false information. Policymakers and private residents alike face a serious problem like this. Utilizing numerous AI draws near, specialists recognize spam interchanges and fake news. A subset of machine learning known as "deep learning" mimics the human brain in its ability to solve numerous challenging issues. As a matter of fact, deep learning techniques are right now utilized by society since they can effectively tackle text acknowledgment issues like recognizing fake news and spam. These models work rapidly on crude information by concentrating on undeniable level qualities all alone. To recognize deceitful and spam correspondences, different exemplary ML approaches as well as deep learning systems are

talked about in this article. An outline of a few examinations on the distinguishing proof of phony news utilizing conventional ML techniques and Deep Neural Networks is likewise remembered for this review.

## **2.2 Research Gap**

Researcher have proposed different algorithms and Technique to Identify Fake news and to Stop the dissemination of fake news, all those algorithms are based on traditional machine learning algorithms such as SVM or Random Forest. These algorithms lack of security and authorization. There is need of robust system and algorithm which can detect fake news which can provide security to the news and data as well as less time complexity in identification of fake news.

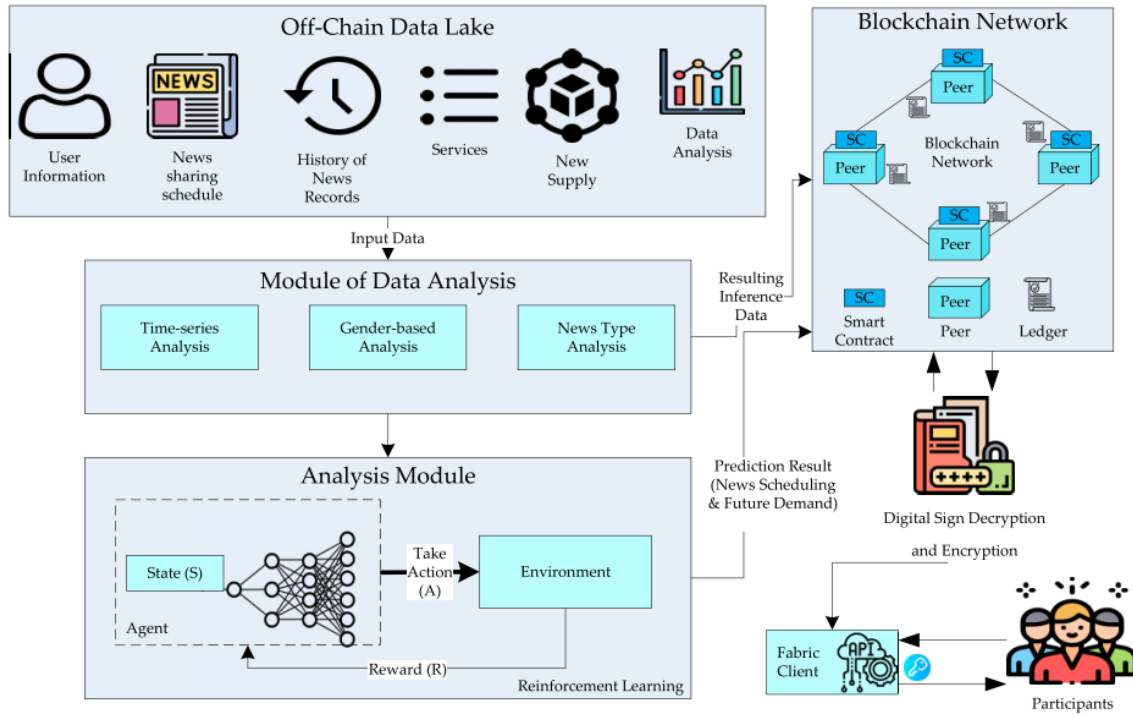
## **2.3 Problem Statement**

The fake news spread is part of social media failing to check the authenticity of the news spread in the platform to the mass or the people. Fake news has been skillfully prepared in the form of article, post images, audio, video such that it seems real one. Fake news is mostly used to manipulate the mass or public opinion for the political or commercial purpose. Fake news is spread by the social media user only who post, comment, share the news. The spreading of the fake news has its own consequences while some are minor or relatively harmless other can cause the damage to the society as it causes change in demographic thinking or opinion. Fake news can hamper the peace in the society and political, economical, societal aspect of the state. There has been many cases of the fake news spread in the last ten year which was propagated and causes severe damage or change in the public opinion. The news later verified found to be faked such as Fake news of immigration crisis. In February 2017 British newspaper posted an article claiming that Germany hoped to carry in twelve million immigrant. This news later when checked came out to be fake news. There has been riot because of spread of Fake news such as London Riot 2011 happened due to mass spread of fake news. During the covid-19 vaccination period false information got spread among people that vaccine is not safe as a result people were not taking the vaccine which causes even death due to misinformation propagation.

## CHAPTER 3

### PROPOSED METHODOLOGY

#### 3.1 System Architecture

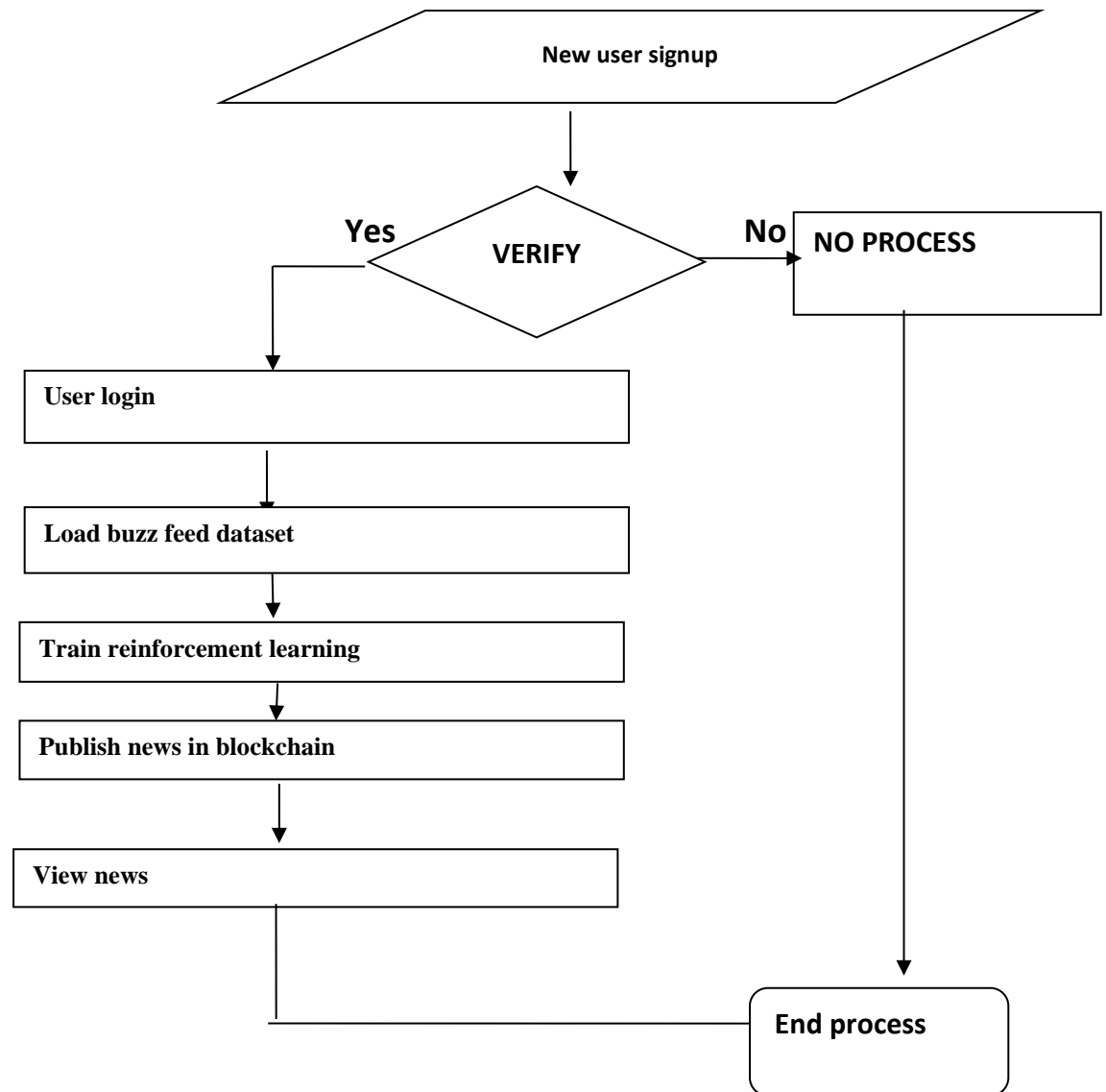


**Fig.3.1.1 System Architecture**

#### DATA FLOW DIAGRAM:

1. A DFD, which is also known as a bubble chart, is a graphical representation of a system's input data, the operations performed on it, and the resulting data. This simple notation allows for a visual representation of these elements.
2. The data flow diagram (DFD) is a critical modeling tool used to create models of a system's components. These components include the system's functionality, the data it uses, the entities that interact with it, and the path that data takes through the system.

3. DFDs illustrate the flow of information throughout a system and the various transformations that occur. They use visual elements to demonstrate how data is transformed and moved within the system



**Fig.3.1.2**Dataflow diagram

## **3.2 SYSTEM DESIGN**

UML stands for Unified Modeling Language. UML is a general-purpose modelling language that has been standardised for use in the area of object-oriented software engineering. The standard was created and is supervised by the Object Management Group. The goal is for UML to become a standard language for creating models of item-centered computer programming. A notation and a meta-model are two significant components of UML's continuous structure. In the future, further steps or methods may be added, or they could be connected to UML, a standard language for describing, visualising, creating, and documenting software system artefacts. UML is also used for business modelling and other non-software systems. The UML is a collection of the most effective engineering practices for modeling large and complicated systems. The software development process and the development of objects-oriented software both rely heavily on the UML. The UML mostly uses graphical notations to describe how software projects are designed.

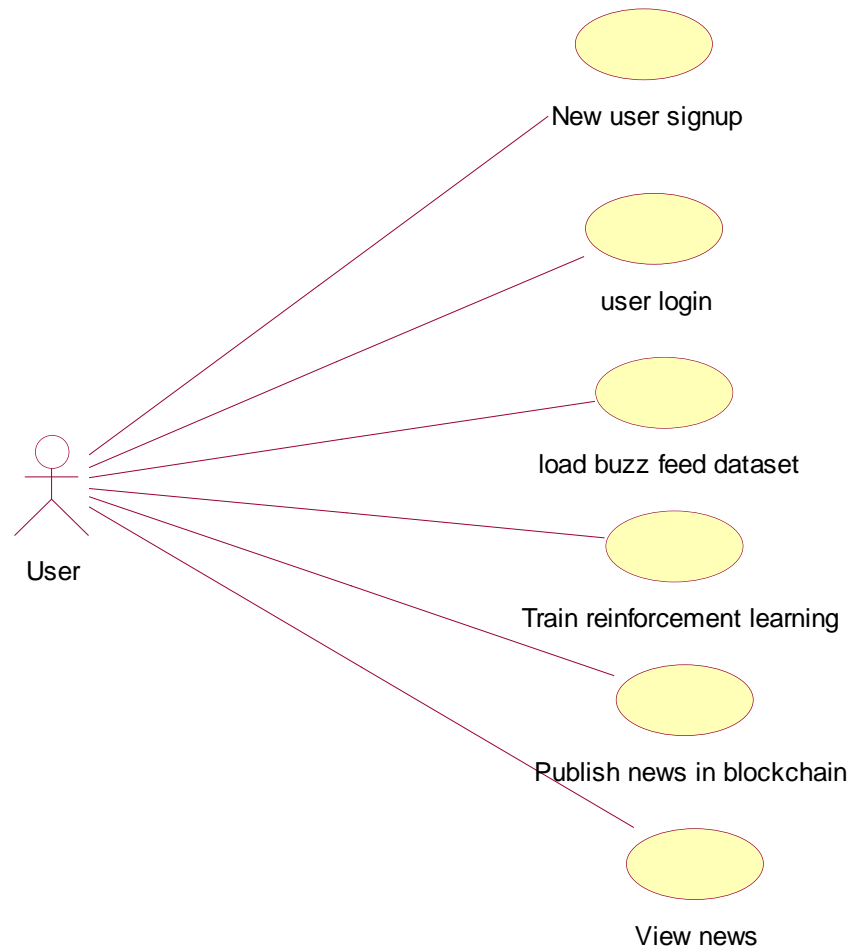
### **GOALS:**

The Essential objectives in the plan of the UML are as per the following:

1. Provide users with a visual modeling language that is ready-to-use and expressive so that they can create and exchange meaningful models.
2. Provide mechanisms for extendibility and specialization to extend the fundamental ideas.
3. Be independent of particular development methods and programming languages.
4. Establish a formal foundation for modeling language comprehension.
5. Encourage the market for OO tools to expand.
6. Help develop higher-level ideas like collaborations, frameworks, patterns, and components.
7. Make use of best practices.

### **3.2.1 Use case diagram:**

A use case diagram is a type of behavioural diagram in the Unified Modelling Language (UML) that is derived from and described by a use-case study. The purpose of a use case diagram is to provide a visual representation of a system's functionality, in terms of the actors involved, their objectives (represented as use cases), and any relationships between those use cases.

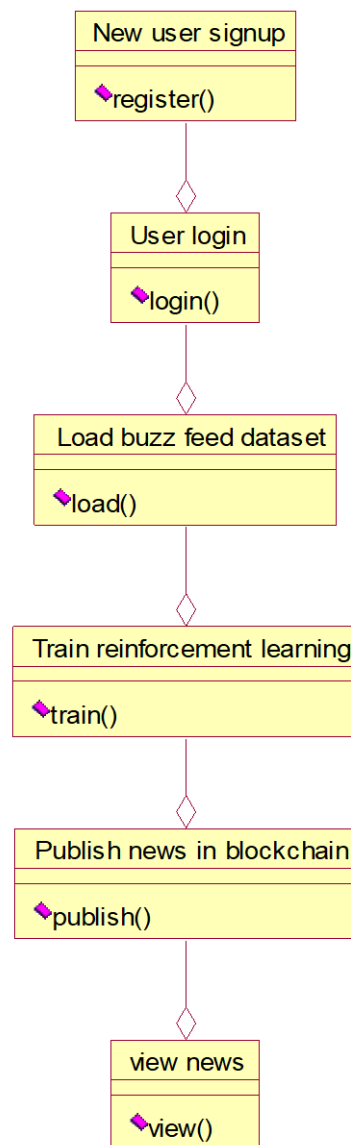


**Fig.3.2.1 Usecase diagram**

### **3.2.2 Class diagram:**

To refine the use case diagram, the class diagram is utilized, which serves as a blueprint for a comprehensive system design. The class diagram aids in categorizing the participants in the use case diagram into relevant classes. The classes can be interconnected by "is-a" or "has-a"

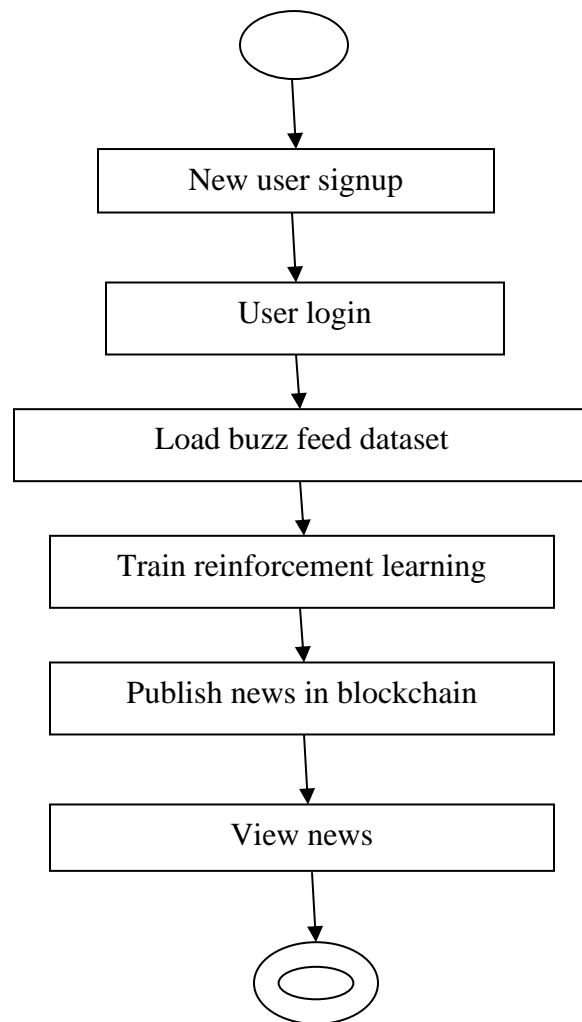
relationships. Each group in the diagram's structure may possess several attributes, which serve as the "methods" the class provides. Furthermore, each class may have distinct "attributes" that distinguish it from other classes.



**Fig.3.2.2 Class diagram**

### 3.2.3 Activity diagram:

In the activity diagram, the system's process flows are depicted. An activity diagram has the same components as a state diagram, including activities, actions transitions, initial and final states, and guard conditions.

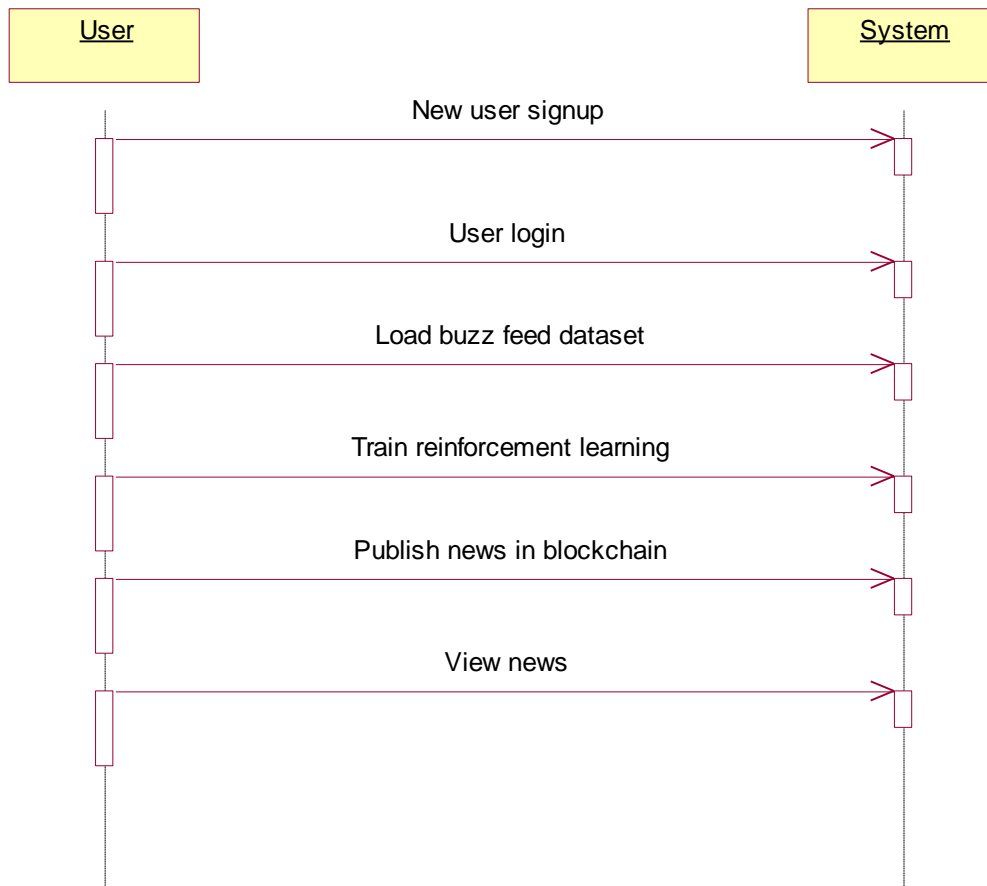


**Fig.3.2.3 Activity diagram**



### 3.2.4 Sequence diagram:

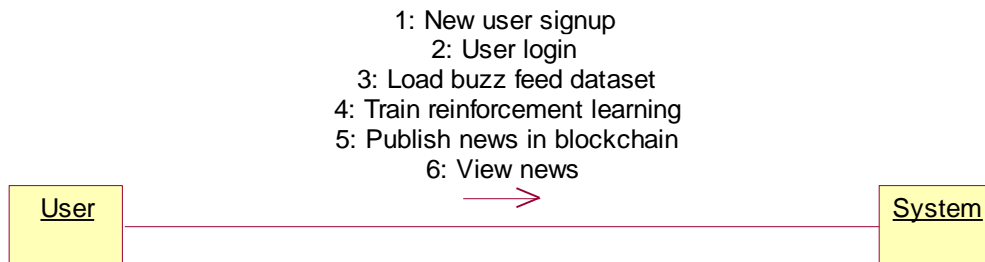
A sequence diagram shows how various system items interact with one another. The fact that a sequence diagram is time-ordered is crucial. This indicates that the precise order of the objects' interactions is displayed step by step. The sequence diagram shows how various things communicate.



**Fig.3.2.4 Sequence diagram**

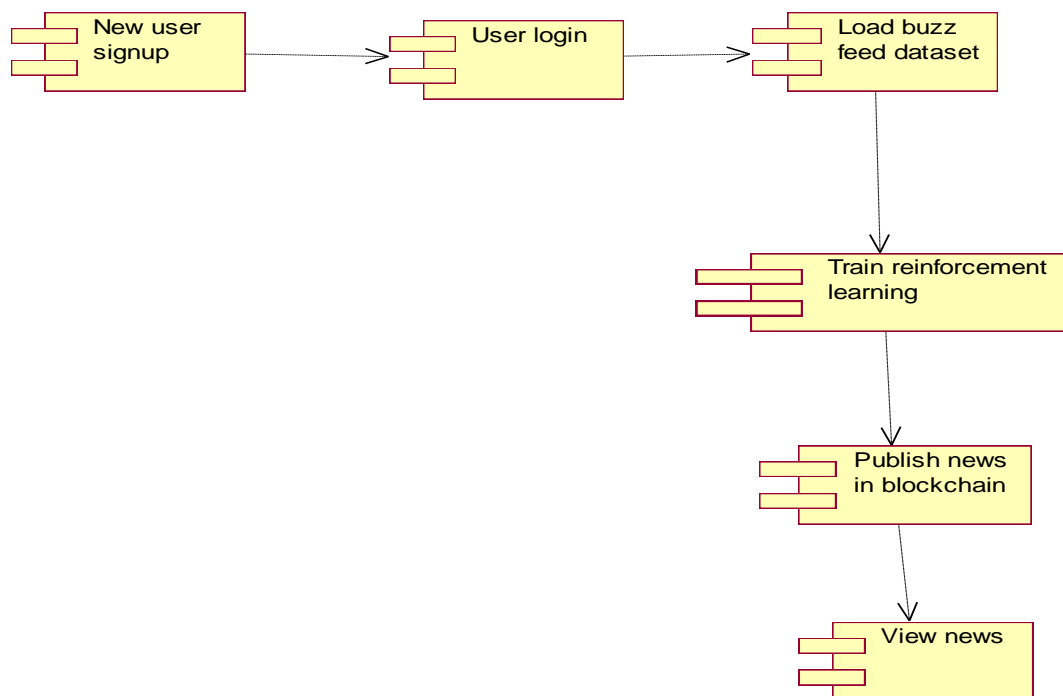
### 3.2.5 Collaboration diagram:

The interactions between several items are gathered in a cooperation diagram. The interactions are listed as numbered interactions to make it easier to follow their order. The collaboration diagram makes it easier to see every potential interaction between each object and other things.



### 3.2.6 Component Diagram:

The system's high-level components are depicted in the component diagram. At a high level, the system's components and their relationships are shown in this diagram. A part chart portrays the parts winnowed after the framework has gone through the turn of events or development stage.



**Fig.3.2.6 Component diagram**

**3.2.7 Deployment diagram:** The application's runtime configuration is depicted in the deployment diagram. When a system is constructed and prepared for deployment



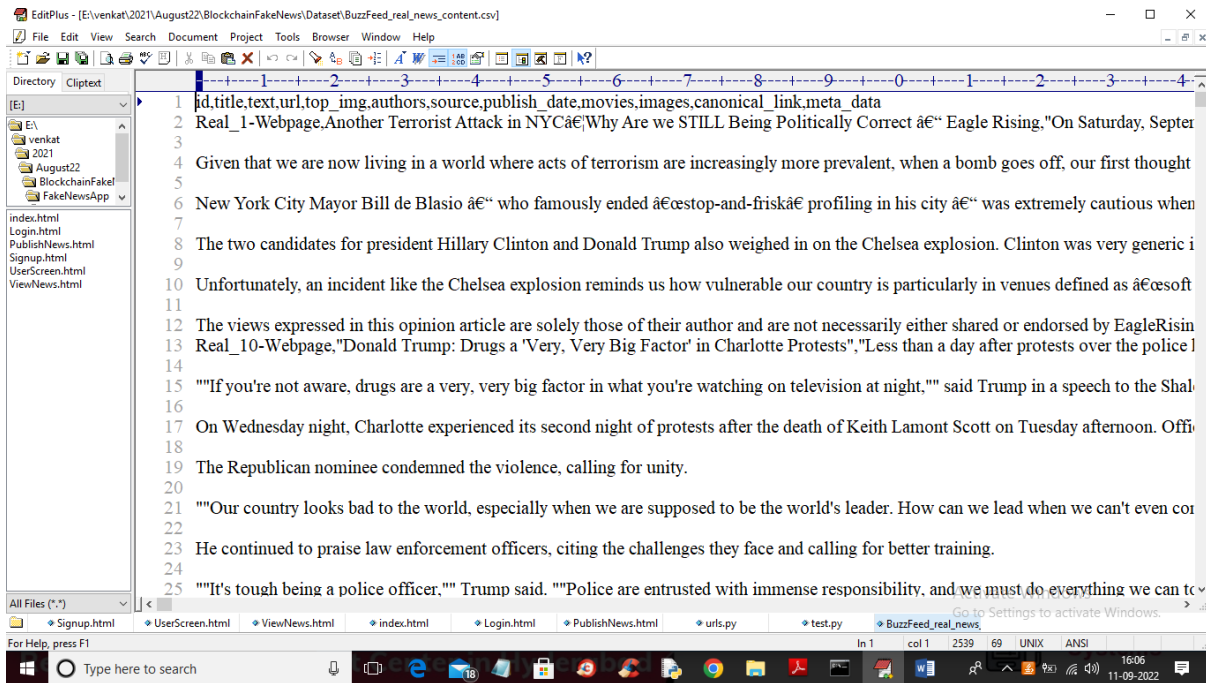
**Fig.3.2.7 Deployment diagram**

## **CHAPTER 4**

### **IMPLEMENTATION**

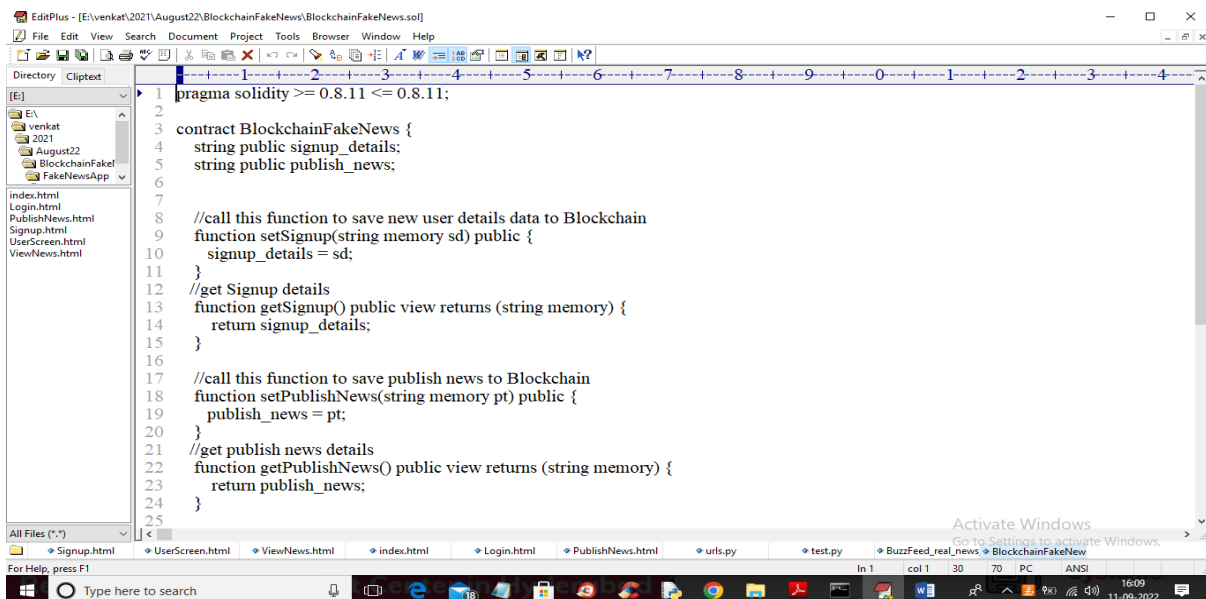
#### **4.1 Implementation**

Now-a-days all users are using social media to access news content but sometime some malicious users will alter genuine news and then spread fake news which may degrade social media fame and to avoid such fake news many existing algorithms were introduced but all those algorithms are based on traditional machine learning algorithms such as SVM or Random Forest. This algorithms lack of security and authorization. In propose paper author is using Reinforcement Deep Learning algorithm to detect fake news and then applying Blockchain technology to provide security to NEWS data. Reinforcement algorithm will match similarity between old news and current news and if news contains more similarity then it will detect as Fake news and penalized the user and if news is REAL then algorithm will reward user and then store NEWS in Blockchain. Blockchain store each news as block/transaction and associate each block with unique hashcode and then store this block in multiple nodes as Decentralized storage and if one node is down then Blockchain will access News from other working nodes. Blockchain verify all hashcode before storing new block and if all blocks verification successful then only new block will store and this mechanism is called as proof of work or proof of authority. To detect fake news in propose paper applying NLTK (natural language tool kit) technique to remove STOP WORDS, special symbols, data normalization, converting words into numeric vector (numeric vector will assign average count of each word), STEMMING and lemmatization. Vector will be input to Reinforcement algorithm to train FAKE news model and this trained model will be applied on all TEST news to predict weather news is fake or real. Reinforcement will take each INPUT as state and then apply model to predict ACTION and if action is Fake then algorithm will penalized user and if action is real then user or news publisher will get reward. To implement this project author has used BUZZ NEWS and many more dataset but we are using BUZZ news dataset only and below is the dataset screen shots



**Fig.4.1.1 Dataset Values**

In above screen first row contains dataset column names and remaining rows contains dataset values and by using above dataset we will train Reinforcement algorithm. To store or access data from Blockchain we need to develop SMART CONTRACT which will contains functions to STORE and READ data and below is the SMART CONTRACT for Fake News application.



**Fig.4.1.2 Smart Contract Function**

In above screen we have define smart contract functions to store USER & NEWS details and we need to deploy this contract in Blockchain server and for deployment we need to follow below steps

- 1) First go inside 'hello-eth/node\_modules/.bin' folder and then double click on 'runBlockchain.bat' file to get below screen

```

C:\Windows\system32\cmd.exe
C:\acc\manoj\November21\hello-eth\node_modules\.bin>truffle develop
Truffle Develop started at http://127.0.0.1:9545/

Accounts:
(0) 0xc7b56c1b125271e1deedffa10a84a83cc620313f
(1) 0xbe597cdec3c2f1a2b51d7d79e06f20e46dd9dea3e
(2) 0xc432c93aa581c68ed3f05fa0b212f3f41e1ec712
(3) 0xa29fb6a3000361e87408f7a61f1ee30b25d11d
(4) 0x2432dbdc222f2fca4c54733423d1af5d5d864a7f8
(5) 0x87179afb9c0a0904764053551a70081ab0f70ef8
(6) 0x726facb8dea3534b06e72d2df7e063cf497ed9b3
(7) 0x55f4b977e6c8a1cccbeeb10ebdb2a67f7ba2d3
(8) 0x5f9eb3646fdc53c304783f38f46800431603e425
(9) 0xb94279d4329857270b8b8ceec22ac90e07ac89

Private Keys:
(0) bd0f17ca0eb13a6788828dd1d59f520caef17029835d405f9e21d350b60fcd5e
(1) 1aefe2209d068ef6c98b15e8a590eb49fd973d09e4079d439e8384b11ea6381
(2) 3721b80873a2d7e1907a4006f720fd5852a639feeb69cb1d5d52f7204daf01f5
(3) bba03a797a8b8dbba41f209b3d813e3a1346bd4015edb55a7c56e36b05aa7966f
(4) 77fe4d767986f96c3ec170db1dba5da803d91b3f27f550e4e0c11ee2ca58cc2c
(5) 5783fbbd3d88812ef707fb7c1f87bfb3d660dd53639ca4748b422c2eb5f490d2
(6) b337a06d579c2a284d625ac11eac730a81854cb5febcbac382d90a2d8202543
(7) 5cf4d9e9bb5f30c4a69f340665f84a713e9b3f2f401ff0c10b7abe18c4221afe
(8) 934bb791489ad5bf5452251000bea59e237456410bc1ab057999245a603ed527
(9) 3b3852138739d1c84d1ee9349e4bf3fdb9f61f5059f2dd0eeba0da31e1da4c05

Mnemonic: repeat kitten art call plastic talent gather cannon cabbage stove find convince
Important : This mnemonic was created for you by Truffle. It is not secure.
Ensure you do not use it on production blockchains, or else you risk losing funds.

truffle(develop)> truffle migrate

Compiling your contracts...
-----
> Compiling .\contracts\BlockchainFakeNews.sol
> Compiling .\contracts\Migrations.sol
> Compilation warnings encountered:

Warning: SPDX license identifier not provided in source file. Before publishing, consider adding a comment containing "SPDX-License-Identifier: UNLICENSED" to each source file. Use "SPDX-License-Identifier: UNLICENSED" for non-open-source code. Please see https://spdx.org for more information.
--> project:/contracts/BlockchainFakeNews.sol
  
```

**Fig.4.1.3 Generation of Private key and account**

In above screen Blockchain generated Private keys and default account address and now type command as 'truffle migrate' and then press enter key to deploy contract and get below output

```
Select C:\Windows\system32\cmd.exe
> gas price: 2 gwei
> value sent: 0 ETH
> total cost: 0.000497708 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost: 0.000497708 ETH

2_deploy_contracts.js
=====
Deploying 'BlockchainFakeNews'
-----
> transaction hash: 0xec90e5e10718561507ed2eac61eef0fed87830ed20bf9e6ce9ba43658eee3133
> Blocks: 0 Seconds: 0
> contract address: 0x1DD4fb45C1cdC8C3f32cbaA60464c8107D4D4058
> block number: 3
> block timestamp: 1662879391
> account: 0xc7856c18125271E1dEeFFA10a84a83cC628313f
> balance: 92.989513012
> gas used: 452127 (0x6e61f)
> gas price: 2 gwei
> value sent: 0 ETH
> total cost: 0.000904254 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost: 0.000904254 ETH

Summary
=====
> Total deployments: 2
> Final cost: 0.001401962 ETH

- Blocks: 0 Seconds: 0
- Saving migration to chain.
- Blocks: 0 Seconds: 0
```

**Fig.4.1.4 Blockchain Deployment**

In above screen in white colour text we can see Blockchain Fake News contract deployed and we got contract address also and this address we need to specify this address in python program to access above contract info and read data from Blockchain.

```
views.py - E:\venkat\2021\August22\BlockchainFakeNews\FakeNewsApp\views.py (3.7.0)
File Edit Format Run Options Window Help

global details
details = ""
print(contract_type+"=====")
blockchain_address = 'http://127.0.0.1:9545' #Blockchain connection IP
web3 = Web3(HTTPProvider(blockchain_address))
web3.eth.defaultAccount = web3.eth.accounts[0]
compiled_contract_path = 'BlockchainFakeNews.json' #Blockchain fakeneews contract code
deployed_contract_address = '0x1DD4fb45C1cdC8C3f32cbaA60464c8107D4D4058' #hash address to access OSN contract
with open(compiled_contract_path) as file:
    contract_json = json.load(file) # load contract info as JSON
    contract_abi = contract_json['abi'] # fetch contract's abi - necessary to call its functions
file.close()
contract = web3.eth.contract(address=deployed_contract_address, abi=contract_abi) #now calling contract to access data
if contract_type == 'signup':
    details = contract.functions.getSignup().call()
if contract_type == 'news':
    details = contract.functions.getPublishNews().call()
print(details)

def saveDataBlockChain(currentData, contract_type):
    global details
    global contract
    details = ""
    blockchain_address = 'http://127.0.0.1:9545'
    web3 = Web3(HTTPProvider(blockchain_address))
    web3.eth.defaultAccount = web3.eth.accounts[0]
    compiled_contract_path = 'BlockchainFakeNews.json' #Blockchain fake news contract file
    deployed_contract_address = '0x1DD4fb45C1cdC8C3f32cbaA60464c8107D4D4058' #contract address
    with open(compiled_contract_path) as file:
        contract_json = json.load(file) # load contract info as JSON
        contract_abi = contract_json['abi'] # fetch contract's abi - necessary to call its functions
    file.close()
    contract = web3.eth.contract(address=deployed_contract_address, abi=contract_abi)
    readDetails(contract_type)
    if contract_type == 'signup':
        details=currentData
        msg = contract.functions.setSignup(details).transact()
        tx_receipt = web3.eth.waitForTransactionReceipt(msg)
    if contract_type == 'news':
        details=currentData
        msg = contract.functions.setPublishNews(details).transact()
    tx_receipt = web3.eth.waitForTransactionReceipt(msg)
```

**Fig.4.1.5 Blockchain Function**

In above screen read red colour comments to know about how to call Blockchain function to store and read data using Python program

## **4.2 Software Environment**

Development standards control defining the programming asset precondition and needs that need to be installed on a PC to provide perfect application performance. These needs or demands should be provided separately prior to the product is offered since they are typically not included in the product setup package.

**Platform:** In computing, a platform is a term for a software or hardware framework that enables software to run. A computer's architecture, OS, or codes and their runtime libraries are all typical platforms. When defining system requirements (software), the operating system is one of the first requirements mentioned. Although some backward compatibility is frequently maintained, software may not be compatible with different versions of the same OS. The majority of software designed for MS Windows XP, for instance, cannot be used with MS Windows 98, although this does not always accepted. Likewise, Linux distributions running Kernel v2.2 or v2.4 generally cannot run or compile software developed with the most recent features of Linux Kernel v2.6.

**APIs and drivers:** Software that makes a lot of use of special hardware, like high-end display adapters, needs a special API or driver for those devices, which are more recent. DirectX, a set of APIs for handling multimedia, particularly game programming, tasks on MS platforms, is a good example.

**Web browser:** Most software as well as web-based apps that extensively count on Internet technology access the system's default browser. Microsoft Web Pilgrim is a continuous decision of programming running on Microsoft Windows, which utilizes ActiveX controls, notwithstanding their weaknesses.



1)The latest version of Visual Studio Community; 2) Nodejs (version 12.3.1); and 3) Python IDEL (version 3.7).Python is a high-level, interpreted programming language with dynamic semantics that is object-oriented. It is quite appealing for Speedy Software Growth and for usage as a prearranging or stick language to connect already present elements together because to its unquestionably level underlying information structures, dynamic writing, and dynamic limiting. Python's simple syntax places a strong emphasis on readability, which minimises management costs of programmes. Code reuse and programme modularity are encouraged by Python's allowance of modules and packages. For every single significant stage, the Python translator and the extensive standard library are freely available in sources or double structure and can be distributed without restriction. Python often has developers falling over their steps because of its improved productivity. Due to there is not one compilation step, the edit, test, and debug cycle is very quick. Python programmes repair is clear: A defect or poor input is unlikely to result in a segmentation malfunction. When the third party makes a mistake, it raises a special case, all things examined. When the programme fails to identify the error, the interpreter outputs a stack trace. A source level debugger makes it achievable to set breakpoints, walk throughout the code one line at a time, check local and global variables, evaluate arbitrary expressions, and perform other functions. Python is used to write the debugger, demonstrating Python's intelligent capabilities. On an additional , the easiest approach to debug a programme is typically by adding a few print statements to the source code: This simple method's rapid cycle of editing, testing, and debugging makes it incredibly efficient. It is procedural-oriented and object-oriented is both supported. We do not need to define the type of a variable as Python is a dynamically typed language. For instance, any sort of x, such as a String or an int, can be used in the statement `x = 10`.Python has several characteristics.There are a tonne of features in Python, a few of them are listed below:

Openly accessible and cost-free

Python language and its code is publicly available on the official site, and you may download it and use it.

1. Python is a high-level programming language that is easy to learn and use. It is a pretty straightforward language to learn when compared to other programming languages such as C, C#, JS, and furthermore. It is also user-friendly for developers.
2. Readability: As you will see, learning Python is not difficult. Python's syntax is extremely straightforward, as was previously established. Instead of semicolons or brackets, the indentations define the code block.
3. Object-Oriented Programming (OO programming) is one of Python's most important features. Python upholds object-oriented language and ideas of classes, object exemplification, and so forth.
4. Support for GUI Programming A module such as PyQt5, PyQt4, wxPython, or Tk in Python can be used to create graphical user interfaces. The most widely used Python framework for building graphical applications is PyQt5.
5. Python is a programming language that operates at a high-level. This means that when we write programs in Python, we don't need to concern ourselves with the underlying system architecture, and we don't have to manually manage memory.
6. Simple for debugging , Once you understand how to interpret Python's error traces, you will be prepared to swiftly recognise and fix majority of the problems in your code. You can tell what the code is supposed to perform just by observing it.
7. The Python programming language is also a portable language. For instance, if we have Python code for Windows and want to run it on Linux, Unix, and Mac, we don't have to change it; we can run it on any platform.
8. Python functions as an integrated language since it is easy to combine it with other programming languages .
9. Language Interpretation:

Because Python code is executed line by line at a time, it is an interpreted language. like Java, C, and other programming languages. Python code doesn't need to be compiled, which makes it easier to debug our code. Bytecode is the immediate representation of Python's source code.

10. It offers a big standardised library that consists of an extensive amount of modules and functions, minimising the time and effort of developing custom code for all of them. Regular expressions, unit-testing, web browsers, and a number of other libraries are included in Python.
11. Dynamically Typed Language Python is a language with dynamic typing. That implies the sort (for instance int, twofold, long, and so on.) because of this feature, we do not need to specify the type of variable because the value of a variable is determined at run time rather than in advance.
12. Web Dev along the new project py script, you can use the straightforward HTML tags py-script>, py-env>, and so on to run and write Python code. You can use this to do javascript-like frontend development in Python. Because of its frameworks like Django and Flask, Python's backend is a strong suit. It is frequently utilized for this type of work.
13. Memory allocation that is dynamic The data type of a variable need not be declared in Python. At time of execution, when a variable is provided with a value, the memory is logically assigned to it. Developers only need to put y=18 if the integer value 15 is assigned to y rather than writing int y = 18.

#### LIBRARIES/PACKGES :-

TensorFlow is a free and open-source software library for differentiable programming and dataflow in a variety of applications. It is also utilized as a library for symbolic computation in applications using neural networks and other types of machine learning. It is employed by Google both for analysis and creation. TensorFlow was produced by the Google Brain team for internal usage. It was released on November 9th, 2015, under the Apache 2.0 open-source licence.

Numpy-Numpy is a general-purpose array processing package that provides a multidimensional array object and tools for working with these arrays. It is a fundamental package for scientific computing in Python. Numpy offers several essential features, such as C/C++ and Fortran code integration tools, sophisticated broadcasting functions, linear algebra and Fourier transform capabilities, and random number generators. Numpy can also serve as an efficient multi-dimensional container for generic data. The package supports consistent data types, allowing for efficient integration with various datasets. Pandas- Pandas is a high-performance data manipulation and analysis tool made possible by its powerful data structures. It is an open-source Python library. Python was significantly utilized for information munging and planning. It contributed very little to the analysis of the data.

Pandas found a solution to this challenge. It may be used to carry out the five typical statistical phases of load, set up, modify, model, and analyse irrespective of the origin of the information. Numerous academic and commercial domains employ Python with Pandas, including finance, economics, statistics, analytics, and others.

Matplotlib-Matplotlib is a Python 2D plotting library that can generate high-quality visualizations in various output formats and interactive environments across platforms. It can be integrated with four graphical user interface toolkits, Python scripts, the Python and IPython shells, and web application servers. Matplotlib strives to make complex tasks possible and simple tasks easy. With just a few lines of code, you can create plots, histograms, power spectra, bar graphs, error charts, scatter plots, and more. Refer to the example plots and thumbnail display for illustrations. When used with IPython, the pyplot module provides a user interface similar to that of MATLAB for straightforward plotting. The power user can control line styles, font properties, axes properties, and other properties using an object-oriented interface or a set of MATLAB-like functions..

Scikit – learn - It gives a scope of directed and unaided learning calculations by means of a reliable connection point in Python. With a liberal clarified BSD licence that encourages both research and commercial usage, included with many Linux versions.

## CHAPTER 5

### TESTING

#### 5.1 Testing

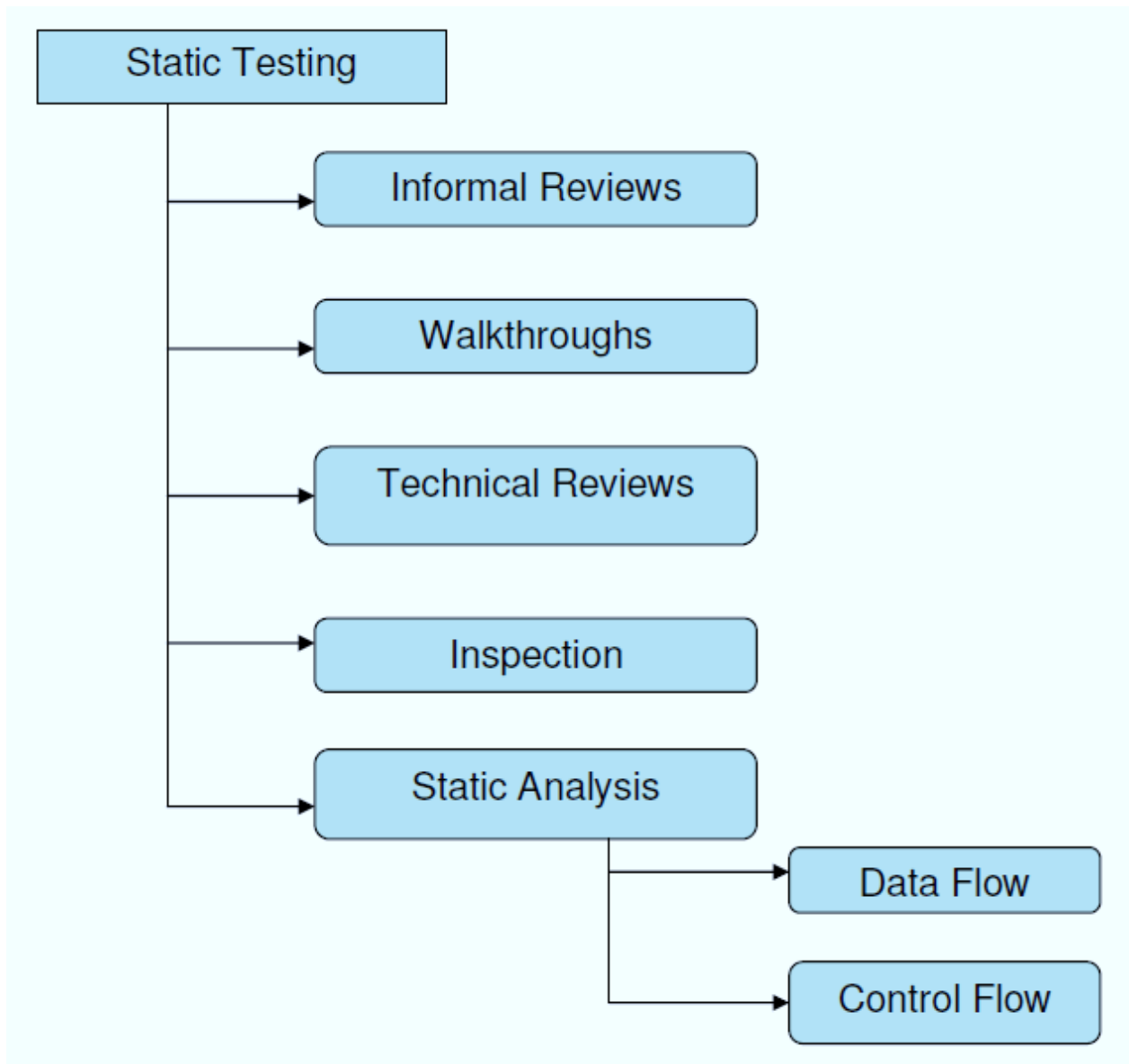
Framework testing, also known as frameworklevel testing or integrated testing, is the cycle in which the Quality Assurance (QA) team evaluates how different application functions work in execution, integration, or implementation. System testing ensures that applications perform their intended functions. This step is a kind of black box testing based on the validity of the application. For example, system testing can ensure that all aspects of user input throughout the application generate the desired product..

System testing phases: a tutorial video for this test level. System testing looks at each part of an application to make sure they work together as a whole. After performing functional or user-story testing on each module and integration testing on each component, a QA team typically performs system testing. Before going into production, where users consume the software, a software build receives a final check through acceptance testing if it achieves the desired results in system testing. An app-dev team keeps track of all defects and decides how many and what kinds of defects are acceptable.

Methodologies for Software Testing: The best way to make it work in software engineering is to optimize how testing is done. A product testing methodology characterizes what, when, and how to do whatever is important to make a finished result of superior grade. Typically, this major goal is achieved by employing the following software testing strategies and their combinations:

Static Evaluation: Static testing is the early-stage testing strategy: It is done without running the developing product at all. This kind of desk-checking is basically necessary to find bugs and problems in the code itself. A check like this is crucial at the pre-deployment stage because it helps

prevent issues caused by software structure deficiencies and code errors.

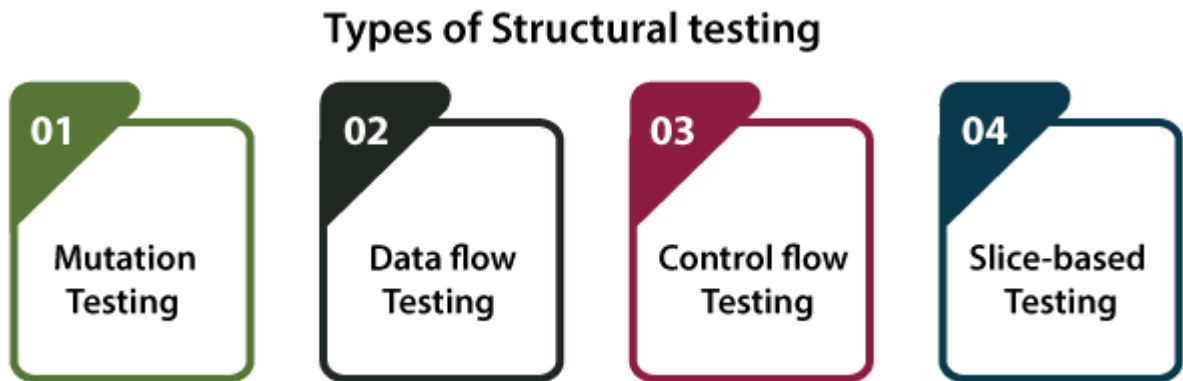


**Fig.5.1.1 Static Testing**

Structural Testing:

Effective testing is impossible without running the software. During the initial design of the software development process, model testing, also known as white box testing, is necessary to find and fix bugs and bugs. At this stage, the unit of measurement is completed according to the product model by using repeated measurements. Usually, it is the robotization cycle that runs in the robotization test system to speed up the interface before this stage. Data analysis gives developers

and quality assurance engineers access to the software's structure and data flow, enabling them to monitor changes in behavior through interaction. compare test results with previous changes (test changes).



**Fig.5.1.2 Structural Testing**

Behavioral Testing:

The software's responses to various activities are the focus of the final testing stage, not the mechanisms that cause them. All in all, social testing, otherwise called black-box testing, assumes running various tests, for the most part manual, to see the item according to the client's perspective. To run usability tests, for instance, and respond to bugs in the same way that regular users of the product would, QA engineers typically have some specific information about a business or other purposes of the software (known as "the black box"). If repetitive tasks are required, behavioral testing may also include automation (regression tests) to eliminate human error. For instance, the automation of this test is preferable because you might need to fill out 100 registration forms on the website to see how the product handles such a task. To run usability tests, for instance, and respond to bugs in the same way that regular users of the product would, QA engineers typically have some specific information about a business or other purposes of the software (known as "the black box"). If repetitive tasks are required, behavioral testing may also include automation (regression tests) to eliminate human error.

## Black Box Testing

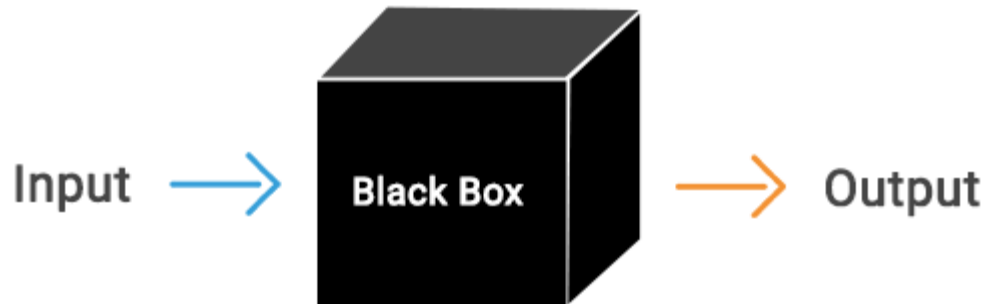


Fig.5.1.3 Black-box Testing

### 5.2 Test Cases

S.NO	INPUT	If available	If not available
1	User signup	User get registered into the application	There is no process
2	User signin	User get login into the application	There is no process
3	Load buzz feed dataset	Dataset loaded	There is no process
4	Train Reinforcement learning	Algorithm trained	There is no process



5	Publish news in blockchain	classify weather news is Fake or Real	There is no process
6	View news	View list of news	There is no process

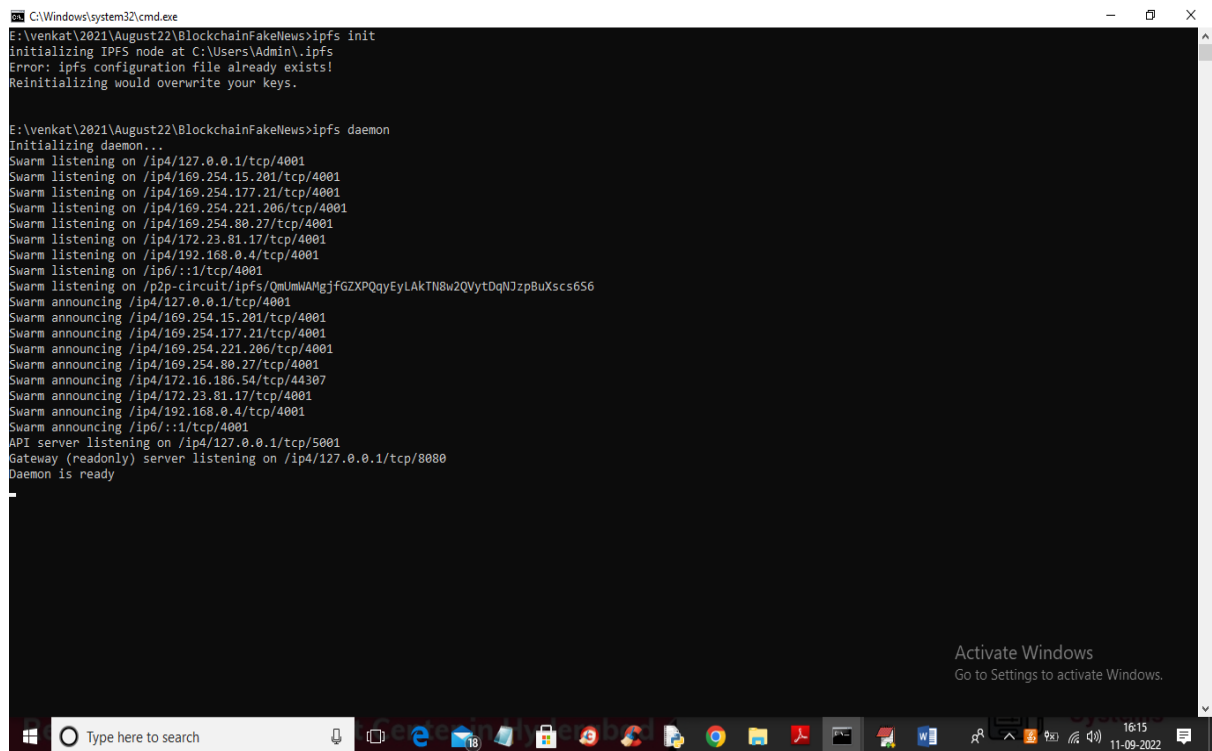
Table 5.2.1 Test-Cases

# CHAPTER 6

## RESULTS AND OUTPUTS

### 6.1 Output

Now after deployment double click on ‘Start\_IPFS.bat’ file to start IPFS server to store image of application and to get below screen



```
C:\Windows\system32\cmd.exe
E:\venkat\2021\August22\BlockchainFakeNews>ipfs init
Initializing IPFS node at C:\Users\Admin\.ipfs
Error: ipfs configuration file already exists!
Reinitializing would overwrite your keys.

E:\venkat\2021\August22\BlockchainFakeNews>ipfs daemon
Initializing daemon...
Swarm listening on /ip4/127.0.0.1/tcp/4001
Swarm listening on /ip4/169.254.15.201/tcp/4001
Swarm listening on /ip4/169.254.177.21/tcp/4001
Swarm listening on /ip4/169.254.221.206/tcp/4001
Swarm listening on /ip4/169.254.80.27/tcp/4001
Swarm listening on /ip4/172.23.81.17/tcp/4001
Swarm listening on /ip4/192.168.0.4/tcp/4001
Swarm listening on /ip6::1/tcp/4001
Swarm listening on /p2p-circuit/ipfs/QmUmmAMgjF6ZXPQyEyLakTNBw2QVytDqNjzpBuXscs6S6
Swarm announcing /ip4/127.0.0.1/tcp/4001
Swarm announcing /ip4/169.254.15.201/tcp/4001
Swarm announcing /ip4/169.254.177.21/tcp/4001
Swarm announcing /ip4/169.254.221.206/tcp/4001
Swarm announcing /ip4/169.254.80.27/tcp/4001
Swarm announcing /ip4/172.16.186.54/tcp/44307
Swarm announcing /ip4/172.23.81.17/tcp/4001
Swarm announcing /ip4/192.168.0.4/tcp/4001
Swarm announcing /ip6::1/tcp/4001
API server listening on /ip4/127.0.0.1/tcp/5001
Gateway (readonly) server listening on /ip4/127.0.0.1/tcp/8080
Daemon is ready
```

**Fig.6.1.1 IPFS Server**

In above screen IPFS server started and now double click on ‘runServer.bat’ file to start python server and get below output

```
C:\Windows\system32\cmd.exe
nvm of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint8 = np.dtype(("Quint8", np.int8, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\dtypes.py:517: FutureWarning: Passing (type, 1) or '1type' as a syno
nvm of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint8 = np.dtype(("Quint8", np.uint8, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\dtypes.py:518: FutureWarning: Passing (type, 1) or '1type' as a syno
nvm of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint16 = np.dtype(("Quint16", np.int16, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\dtypes.py:519: FutureWarning: Passing (type, 1) or '1type' as a syno
nvm of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint16 = np.dtype(("Quint16", np.uint16, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\dtypes.py:520: FutureWarning: Passing (type, 1) or '1type' as a syno
nvm of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint32 = np.dtype(("Quint32", np.int32, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorflow\python\framework\dtypes.py:525: FutureWarning: Passing (type, 1) or '1type' as a syno
nvm of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np_resource = np.dtype(("resource", np.ubyte, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:541: FutureWarning: Passing (type, 1) or '1type' as
a synonym of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint8 = np.dtype(("Quint8", np.int8, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:542: FutureWarning: Passing (type, 1) or '1type' as
a synonym of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint8 = np.dtype(("Quint8", np.uint8, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:543: FutureWarning: Passing (type, 1) or '1type' as
a synonym of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint16 = np.dtype(("Quint16", np.int16, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:544: FutureWarning: Passing (type, 1) or '1type' as
a synonym of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint16 = np.dtype(("Quint16", np.uint16, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:545: FutureWarning: Passing (type, 1) or '1type' as
a synonym of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np Quint32 = np.dtype(("Quint32", np.int32, 1))
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:550: FutureWarning: Passing (type, 1) or '1type' as
a synonym of type is deprecated; in a future version of numpy, it will be understood as (type, (1,)) / '(1,)type'.
np_resource = np.dtype(("resource", np.ubyte, 1))
System check identified no issues (0 silenced).
You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
September 11, 2022 - 16:17:09
Django version 2.1.7, using settings 'FakeNews.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.

Activate Windows
Go to Settings to activate Windows.
```

Fig.6.1.2 IPFS Server Started

In above screen python server started and now open browser and enter URL as ‘http://127.0.0.1:8000/index.html’ and press enter key to get below home page.

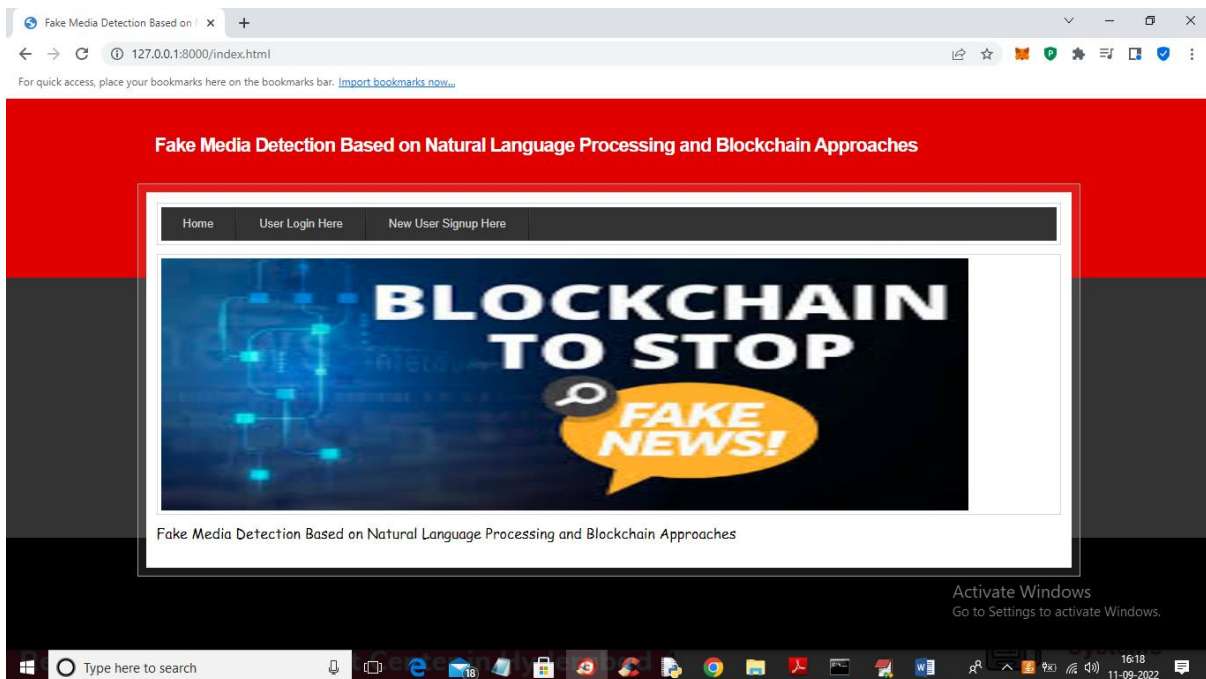


Fig.6.1.3 User Interface

In above screen click on ‘New User Signup Here’ link to get below signup screen

Home User Login Here New User Signup Here

**BLOCKCHAIN TO STOP FAKE NEWS!**

**User Signup Screen**

Username

Password

Contact No

Gender

Email ID

Address

Activate Windows  
Go to Settings to activate Windows.

**Fig.6.1.4 New User Sign-up**

In above screen user is entering signup details and then click on ‘Submit’ button to get below output

**User Signup Screen**

Signup process completed and record saved in Blockchain

Username

Password

Contact No

Gender

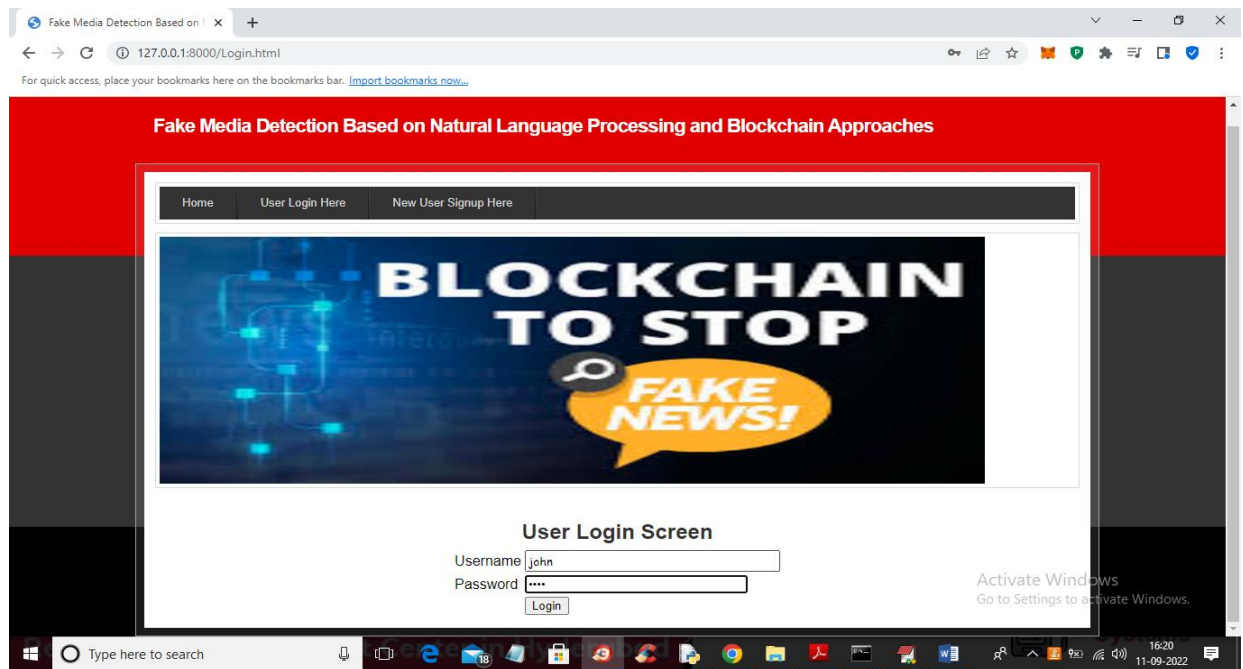
Email ID

Address

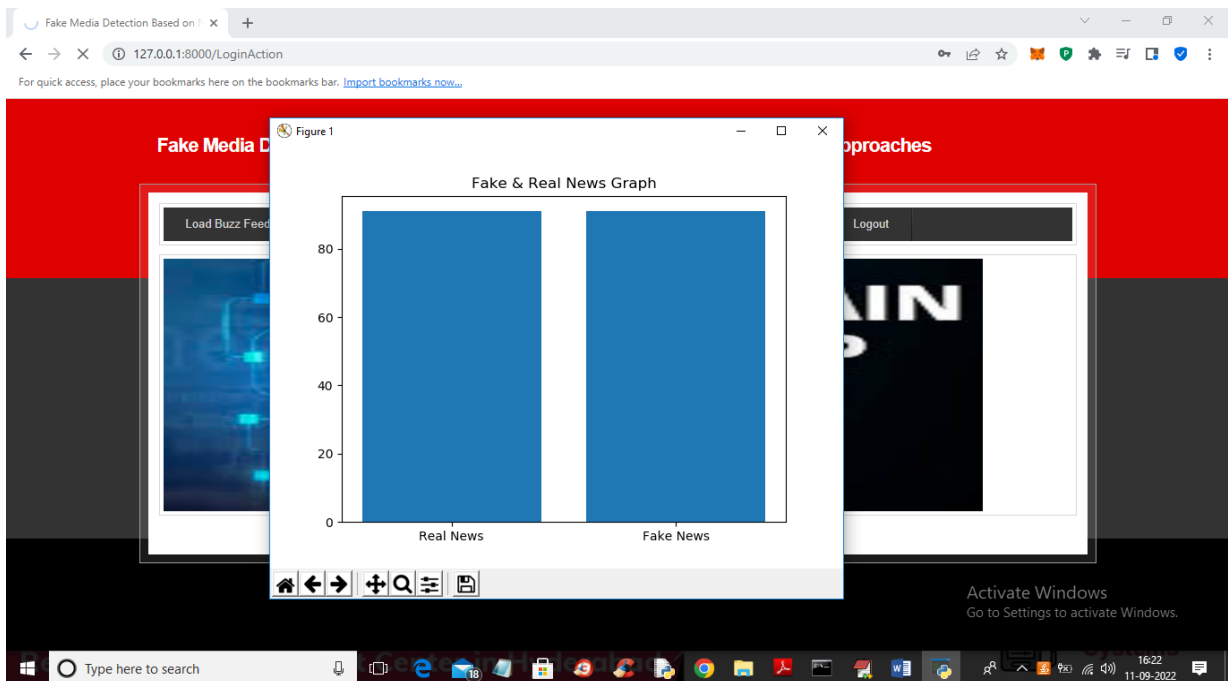
Activate Windows  
Go to Settings to activate Windows.

**Fig.6.1.5 Signup Process Completed**

In above screen in red colour text we can see user details saved in Blockchain and now click on ‘User Login Here’ to get below login screen.



**Fig.6.1.6 User Login Screen**



**Fig.6.1.7 Load Buzz Feed Dataset**

In above screen dataset loaded and we can see number of Fake and Real NEWS graph and in above graph x-axis represents NEWS TYPE and y-axis contains count of that news type and now close above graph to get below output

ID	Title	News Text	URL
Fake_1-Webpage	Proof The Mainstream Media Is Manipulating The Election By Taking Bill Clinton Out Of Context	I woke up this morning to find a variation of this headline splashed all over my news feed. Bill Clinton: âNaturalâ For Foundation Donors to Seek Favors Hereâ Google: Naturally, my reaction was âOh, s**t, what did Bill Clinton do to damage his wifeâ campaign now?â Of course, the headline sounds really, really awful. It plays right into the idea that the Clinton Foundation is all about pay to play, just like Donald Trump has been saying all along. Unfortunately, it takes reading beyond the headlines, which is something most people donâ do, to find out the real story â and the real story is that there is no pay to play. âIt was natural for people whoâve been our political allies and personal friends to call and ask for things. And I trusted the State Department wouldnâ do anything they shouldnâ do.â Clinton told NPR in an interview that aired Monday morning. Source: CNN In other words, people can ask for favors, but that certainly doesnâ mean theyâll get them. Leaked emails have shown that some Clinton Foundation donors have gotten meetings with Clinton and that others were turned down. There is zero evidence of pay to play. In other words, people might have asked for favors, but thereâs no evidence they got them. Now, letâs talk about the foundation the media doesnâ like to mention, the Trump Foundation. Trump hasnâ given to his own foundation since 2008. He does collect money from others, though, and gives it in his name. He also takes from the charity and allegedly buys things like oil paintings and football helmets, all for himself, but out of charity money. New York Attorney General Eric Schneiderman said in a September 13 CNN interview that his office is investigating Trumpâs charitable foundation over concerns that it âengaged in some inappropriateâ as related to New York charity laws. The	http://www.addictinginfo.org/2016/09/19/proof-of-the-mainstream-manipulating-the-election-by-taking-bill-clinton-out-of-context/

Fig.6.1.8 Data-Set

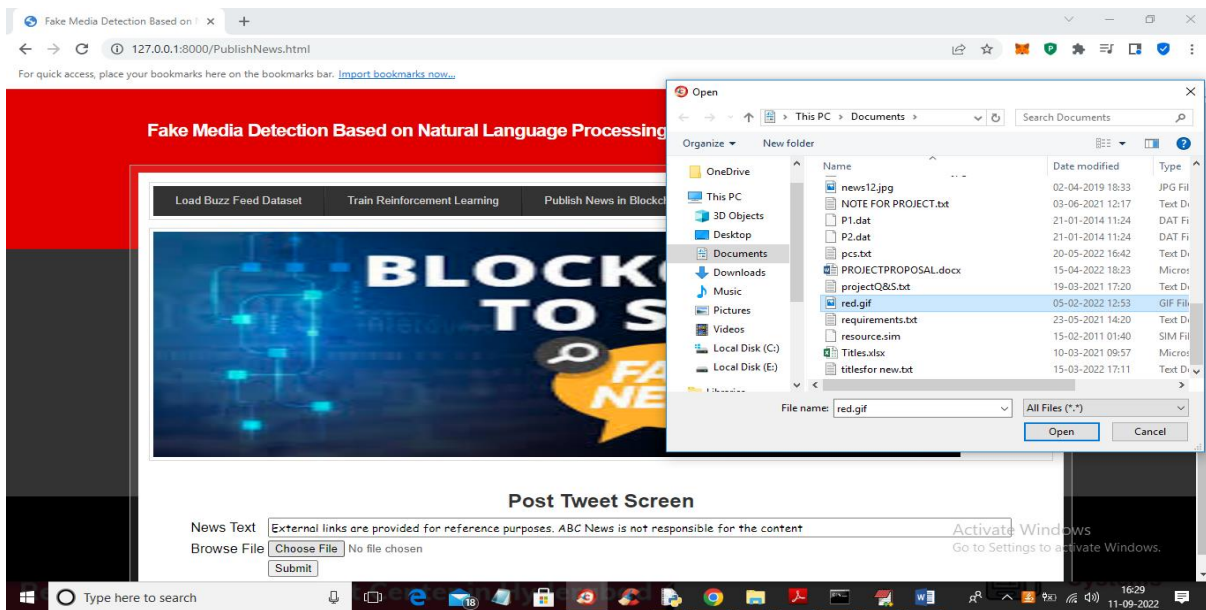
In above screen we can see News loaded from dataset and now click on ‘Train Reinforcement Learning’ link to train Reinforcement algorithm and get below output

Algorithm Name	RMSE	MAE	Reward	Penalty
Random Forest	0.4793013	0.22972974	0	0
Propose Reinforcement Learning	0.1643989873053573	0.02702702702702703	0.40540540540540543	0.5945945945945946



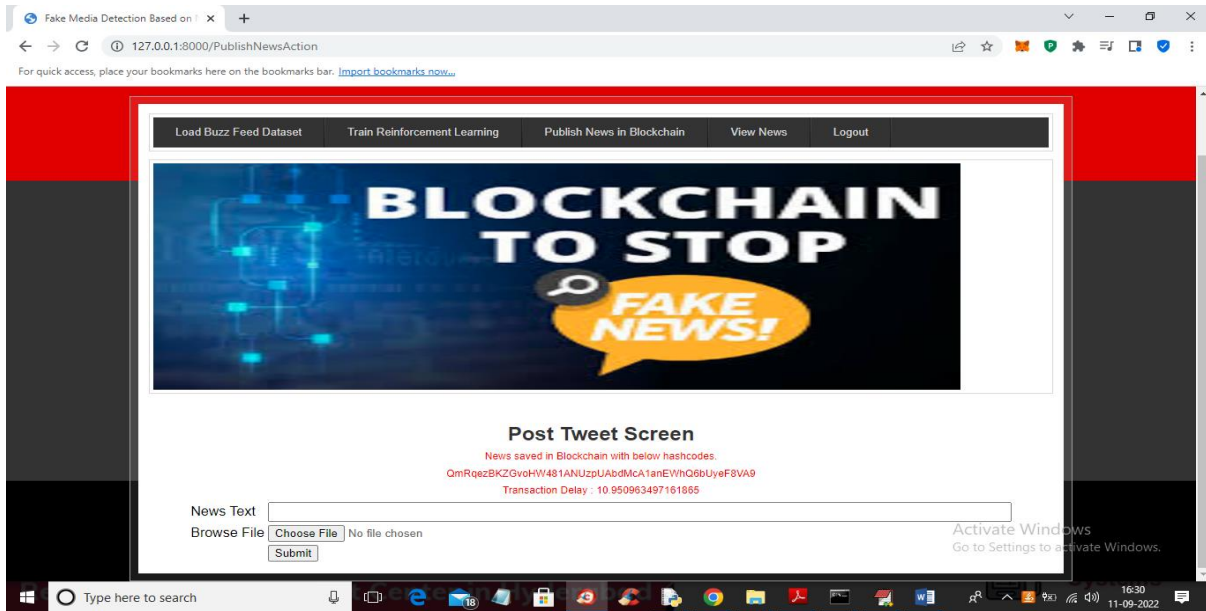
**Fig.6.1.9 Trained Dataset With Algorithm**

In above screen we have trained dataset with existing Random Forest and propose Reinforcement algorithm and then we got RMSE, MAE, reward and penalty for both algorithms. Existing Random forest do not have support for REWARD and Penalty and we can see Propose reinforcement got less RMSE and MAE compare to existing algorithm. The lower the RMSE and MAE the better is the algorithm. Now algorithm model is trained and ready and now click on 'Publish News in Blockchain' link to publish news and then Reinforcement will classify weather news is Fake or Real.



**Fig.6.1.10 Post News Screen**

In above screen I entered some NEWS and then uploading picture and then click on 'Open' and 'Submit' button to detect news as Fake or Real and then store in Blockchain and will get below output



**Fig.6.1.11 Post News Screen With File**

In above screen we can see News is stored in Blockchain and we got hashcode of news storage and Transaction storage DELAY and now click on ‘View News’ link to view LIST of all news published by all users

News Publisher	News Text	News Hashcode	News Image	News Date Time	Detection Result
aaa	Less than a day after protests over the police killing of an African	QmXkZy7yVuFLvR9xh2yRoY1YrmydVvg5vAUJN9cMbTJSyF	1.1 What is computer vision? As humans, we perceive the three-dimensional structure of the world around us with great ease. Think of how you find the face of a friend in a crowd or how you can recognize a friend's face in a photo. You do this by using the visual patterns of light and shadow that the face sends to your eyes and brain. But what if you could see the world through the eyes of a machine? In this paper, we will explore the challenges of machine vision and how we can overcome them. We will discuss the importance of feature extraction and how it can be used to identify objects in a scene. We will also discuss the importance of deep learning and how it can be used to improve machine vision performance. Finally, we will discuss the importance of data and how it can be used to train machine vision models.	2022-09-11 14:17:24	Fake
aaa	Story highlights Bush will deliver his first lecture on Thursday He is a staunch advocate for chart	QmbA9FsiJ2q8toyGNr4SnsZTSLja6rV83631UvCu5RIPWF	These 'Secrets' are too good to keep under your hat The world is full of secrets. Some are hidden in plain sight, while others are kept in the shadows. In this paper, we will explore the importance of secrets and how they can be used to protect information. We will discuss the challenges of keeping secrets and how we can overcome them. We will also discuss the importance of deep learning and how it can be used to improve secret detection performance. Finally, we will discuss the importance of data and how it can be used to train secret detection models.	2022-09-11 14:18:42	Real
john	External links are provided for reference purposes. ABC News is not responsible	QmRqezBKZGvoHW481ANUzpUAbdMca1anEWhQ6bUyeF8VA9		2022-09-11 16:29:09	Real

**Fig.6.1.12 Detection Result**



In above screen we can see names of USERS who publish news and then we can see detection output as FAKE or REAL. Similarly you can upload and test other news.

Note: if u don't have any TEST news data then you can copy some lines from 'Test\_News.csv file'

## **6.2 Analysis**

Blockchain technology can be used to verify the authenticity and integrity of information by creating an immutable record of transactions. However, it alone may not be enough to detect fake news. Natural Language Processing (NLP), on the other hand, is a branch of artificial intelligence that deals with the processing and analysis of natural language data. NLP techniques can be used to analyze the content of news articles and determine their authenticity. Using only blockchain for fake news detection would involve creating a blockchain-based system where news articles are stored and verified through cryptographic algorithms. While this would provide a reliable record of the publication of a news article, it would not necessarily determine the authenticity of its content. On the other hand, using blockchain with NLP would involve combining the two technologies to verify both the publication of news articles and the accuracy of their content. NLP algorithms could be used to analyze the language and sentiment of news articles to determine their authenticity, while blockchain could provide a secure and immutable record of the verification process. In summary, while blockchain can provide a secure and reliable way to verify the publication of news articles, using NLP in combination with blockchain can help to determine the authenticity of their content.

## **CHAPTER7**

### **CONCLUSION**

Fake news sharing is one of the popular research problems in recent technology based on lack of security and trust in terms of the truth of shared news in Social media. In this article, we have presented the combination of blockchain and machine learning techniques to provide solutions and design a trust-based architecture toward shared news online. We have applied the reinforcement learning technique, a learningbased algorithm, to make a strong decision-making architecture and combine it with blockchain framework, smart contract, and customized consensus algorithm, which is well fit for the Proof-of-Authority protocol. Social media plays a key role in this process. The shared information platform contains fake news, and its a beneficial challenge to enhance and investigate the Proof-of-Authority protocol and user validation. Fake news spread is one of the most well-known concentrate on points in present day innovation, inferable from an absence of safety and trust in the veracity of data distributed via virtual entertainment. Here, we offered arrangements and fostered a trust-based engineering for online news sharing utilizing a blend of blockchain and ML techniques. We joined a blockchain structure, shrewd agreements, and a custom agreement calculation that is great for the Evidence of-Authority convention with the support learning approach, a learning-based calculation, to make a powerful dynamic design. In this cycle, virtual entertainment is pivotal. The Evidence of-Authority convention and client approval face a critical test given that the common data stage contains fake news.

## CHAPTER 6

### REFERENCES

- [1] V. P. Miletskiy, D. N. Cherezov, and E. V. Strogetskaia, “Transformations of professional political communications in the digital society (by the example of the fake news communication strategy),” in *Proc. Commun. Strategies Digit. Soc. Workshop (ComSDS)*, 2019, pp. 121–124.
- [2] N. R. de Oliveira, D. S. V. Medeiros, and D. M. F. Mattos, “A sensitive stylistic approach to identify fake news on social networking,” *IEEE Signal Process. Lett.*, vol. 27, pp. 1250–1254, 2020.
- [3] G. Liu, Y. Wang, and M. Orgun, “Optimal social trust path selection in complex social networks,” in *Proc. AAAI Conf. Artif. Intell.*, vol. 24, 2010, pp. 1391–1398.
- [4] M. N. Nikiforos, S. Vergis, A. Styliou, N. Augoustis, K. L. Kermanidis, and M. Maragoudakis, “Fake news detection regarding the Hong Kong events from tweets,” in *Proc. Int. Conf. Artif. Intell. Appl. Innov. Greece: Springer*, 2020, pp. 177–186.
- [5] A. R. Merryton and G. Augusta, “A survey on recent advances in machine learning techniques for fake news detection,” *Test Eng. Manag.*, vol. 83, pp. 11572–11582, 2020.
- [6] X. Dong, U. Victor, S. Chowdhury, and L. Qian, “Deep two-path semisupervised learning for fake news detection,” 2019, arXiv:1906.05659. [Online]. Available: <http://arxiv.org/abs/1906.05659>
- [7] S. Kumar, R. Asthana, S. Upadhyay, N. Upreti, and M. Akbar, “Fake news detection using deep learning models: A novel approach,” *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, p. e3767, Feb. 2020.
- [8] P. Bahad, P. Saxena, and R. Kamal, “Fake news detection using bidirectional LSTM-recurrent neural network,” *Procedia Comput. Sci.*, vol. 165, pp. 74–82, Jan. 2019.
- [9] G. Sansonetti, F. Gasparetti, G. D’Aniello, and A. Micarelli, “Unreliable users detection in social media: Deep learning techniques for automatic detection,” *IEEE Access*, vol. 8, pp. 213154–213167, 2020.

- [10] M. Mahyoob, J. Algaraady, and M. Alrahaili, “Linguistic-based detection of fake news in social media,” *Int. J. English Linguistics*, vol. 11, no. 1, p. 99, Nov. 2020.
- [11] A. Koirala, “COVID-19 fake news classification using deep learning,” *Tech. Rep.*, 2020. [Online]. Available: <https://www.cs.ait.ac.th/xmlui/handle/123456789/981>
- [12] H. Gill and H. Rojas, “Chatting in a mobile chamber: Effects of instant messenger use on tolerance toward political misinformation among south Koreans,” *Asian J. Commun.*, vol. 30, no. 6, pp. 470–493, Nov. 2020.
- [13] J. L. Alves, L. Weitzel, P. Quaresma, C. E. Cardoso, and L. Cunha, “Brazilian presidential elections in the era of misinformation: A machine learning approach to analyse fake news,” in *Proc. Iberoamerican Congr. Pattern Recognit. Havana, Cuba: Springer*, 2019, pp. 72–84.
- [14] N. R. de Oliveira, P. S. Pisa, M. A. Lopez, D. S. V. de Medeiros, and D. M. F. Mattos, “Identifying fake news on social networks based on natural language processing: Trends and challenges,” *Information*, vol. 12, no. 1, p. 38, Jan. 2021.
- [15] D. Mouratidis, M. N. Nikiforos, and K. L. Kermanidis, “Deep learning for fake news detection in a pairwise textual input schema,” *Computation*, vol. 9, no. 2, p. 20, Feb. 2021
- [16] Shovon Paul; Jubair Islam Joy; Shaila Sarker,”Fake News detection using blockchain” 2019 7th International Conference on Smart Computing & Communications (ICSCC).
- [17] Eishvak Sengupta, Renuka Nagpal, Deepti Mehrotra & Gautam Srivastava ProBlock: a novel approach for fake news detection 4 August 2021
- [18] Akash Dnyandeo Waghmare; Girish Kumar Patnaik; Social Media Fake News Detection using mNB in Blockchain;2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS); 07-09 April 2022
- [19] Zeinab Shahbazi; Yung-Cheol Byun; Fake Media Detection Based on Natural Language Processing and Blockchain Approaches; IEEE Access ; 14 September 2021.
- [20] Zonyin Shae; Jeffrey Tsai; AI Blockchain Platform for Trusting News; 2019 IEEE 39<sup>th</sup> International Conference on Distributed Computing Systems (ICDCS); 07-10 July 2019.

## ANNEXURE

### LIST OF PUBLISHED PAPER

Review Paper for the said project has been Presented in International Emerging Trend in Computational Intelligence And Application 2023

Paper Title: Review On Fake News detection.

Abstract: —The online social networks facilitate to share information among the users based on their interests. The specific information being shared by a user may be legitimate or fake. Often, misinformation propagated by users and groups can create chaos and riots in the worst circumstances. Nowadays, a third party like ALT news and Cobrapost check the authenticity of the information, but it takes too much time to validate it. Therefore, there is a need to establish a new robust system to check the information authenticity within the network. In this paper we have done literature survey of the recent paper on fake news detection and various model discussed in those paper and their limitation. Going through the different model proposed by different authors using various technology such as Artificial intelligence , machine learning, blockchain, polygraph, natural language processing etc . the main problem with the current model available are as follows Traceability, credibility, new user authentication, Trust model, Ledger design, credible peer , authenticity .

Authors: Jai Sanger, Renu Mishra, Taslim Raza Ahmad, Veetu Kaushik



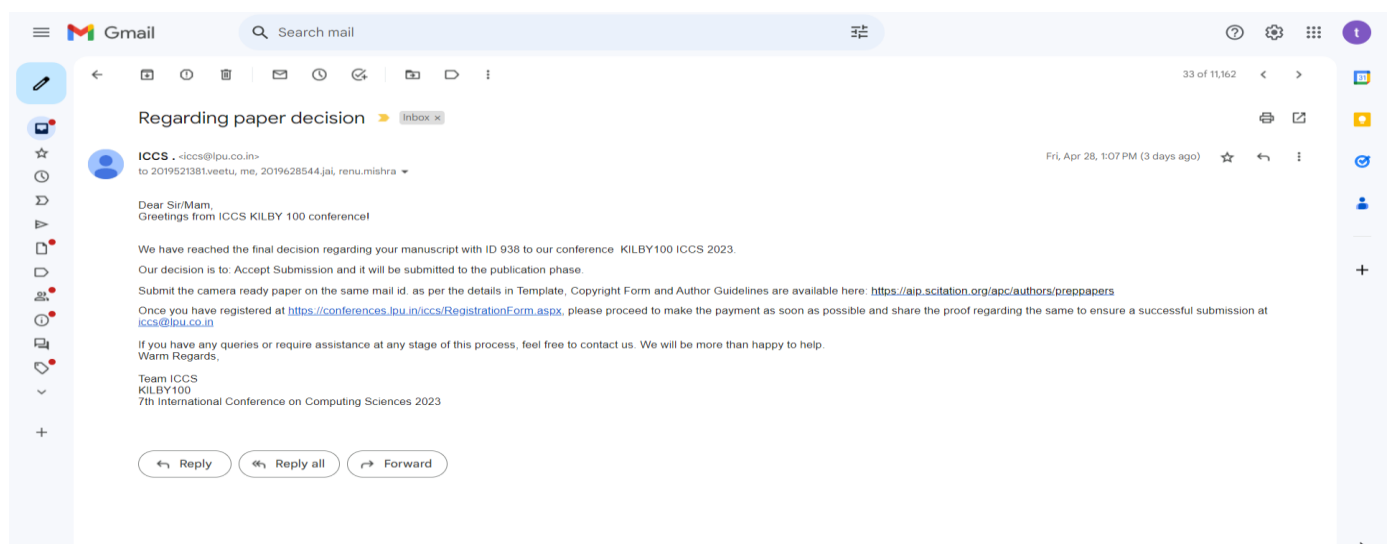
Research Paper for the said project has been Presented on 5<sup>th</sup> May 2023 in KILBY100 7<sup>th</sup> International Conference on Computing Sciences 2023

Paper Title: Fake News Detection Using Blockchain

Abstract: Social media networks have emerged as an essential component of human existence as a result of recent technological advancements in computing era. This climate has turned into a notable stage for trading data and news on various topics, as well as day to day reports, and it is the essential time frame for information assortment and transmission. This climate enjoys many benefits, however it likewise contains a ton of fake news and data that confounds clients and perusers about the data they require. The absence of real-time social media news and reliable information is a major concern for the system. We suggested a machine learning-based integrated solution that would better anticipate bogus user accounts and postings and identify false news for multiple blockchain components using natural language processing (NLP). The proposed methodology utilizes the Support Learning procedure and decentralized blockchain architecture, which gives an outline of computerized content power verification to improve the stage's security. The target of this framework is to offer a solid strategy for foreseeing and distinguishing fake news via social media stages.

Authors: Jai Sanger, Renu Mishra, Taslim Raza Ahmad, Veetu Kaushik

Github Link: <https://github.com/Taslim932/FakeNewsDetection>





**Money Paid Successfully**

**₹ 10500** 

**Rupees Ten Thousands Five Hundred only**

To

**LPU Other Fees**

Paid From

**91XXXX3101**

