

Blockchain-Based Event Detection And Trust Verification Using Natural Language Processing & Machine Learning

Amtul Shanaz¹, M.Varshitha², CH.Venkata Vardhini³

¹Assistant Professor, Department of CSE, Bhoj Reddy Engineering College for Women, India.

^{2,3}B.Tech Students, Department of CSE, Bhoj Reddy Engineering College for Women, India.

ABSTRACT

Online social media platforms are extensively used for sharing concise messages, often containing information about various events, including natural disasters. The automatic classification of these messages plays a crucial role in aiding emergency relief teams by providing insights into the number and nature of detected disasters. In the proposed work, Natural Language Processing Text API is employed to analyze text messages, converting them into training features. These features serve as input to different machine learning algorithms, evaluating their performance for classification. The study evaluates eight different algorithms, including Naïve Bayes, KNN, SVM, Decision Tree, Random Forest, XGBOOST, Logistic Regression, and Deep Learning. Notably, Deep Learning emerges as the most accurate algorithm, with each method assessed based on metrics like accuracy, precision, recall, and F-score.

Traditional social media platforms rely on centralized single servers to store user posts. However, this centralized approach poses a risk in case of server crashes or security breaches, leading to service disruptions. To address this vulnerability, the paper proposes the implementation of a Blockchain-based decentralized server. This decentralized architecture stores data across multiple nodes, ensuring continuous service availability even if one node experiences issues.

All user posts stored in the Blockchain are inherently

tamper-proof due to the technology's built-in support for data encryption and integrity. Each record is stored as a block/transaction, linked with a unique hash code. During the storage of new records, Blockchain verifies all previous hash codes. If the data remains unaltered, the hash code verification is successful; otherwise, it fails, indicating tampering. This inherent tamper-proof nature makes Blockchain a secure and reliable option for storing sensitive information.

Data storage and retrieval in Blockchain are facilitated through smart contracts, which contain functions to save and retrieve data. A specific contract is designed to store user posts, providing a robust and secure mechanism for managing social media content.

INTRODUCTION

In the contemporary digital age, the abundance of online information and events shared on social media platforms poses the challenge of distinguishing authentic and trustworthy content from misinformation. This project addresses the need for a robust event detection and trust verification system by leveraging the synergies of Blockchain, Natural Language Processing (NLP), and Machine Learning (ML) technologies. The goal is to enhance the reliability of event information circulating on social media, providing users with a mechanism to verify the trustworthiness of shared content.

The integration of blockchain technology with natural language processing (NLP) and machine learning (ML) presents a groundbreaking approach to event detection and trust verification. This convergence offers unparalleled opportunities to enhance transparency and reliability in various domains. By leveraging the decentralized and immutable nature of blockchain, coupled with NLP techniques for event extraction from textual data and ML algorithms for trust assessment, this innovative framework holds promise in revolutionizing industries such as finance, supply chain management, media, healthcare, and disaster response. This introduction sets the stage for exploring how blockchain, NLP, and ML synergize to enable robust event detection and trust verification mechanisms, fostering trust, accountability, and efficiency in an increasingly interconnected world.

PROPOSED SYSTEM

The proposed system introduces a novel approach to event detection and trust verification by integrating Blockchain technology with NLP and ML techniques. Blockchain, with its decentralized and tamper-proof nature, serves as the foundation for storing and securing event-related data. NLP is applied to analyze textual information, extracting key features for event detection. ML algorithms, including but not limited to Naïve Bayes, Decision Trees, and Neural Networks, are trained on labeled datasets to evaluate and classify events based on their trustworthiness.

The system employs smart contracts in the Blockchain network to facilitate trust verification processes. These contracts contain predefined functions for verifying and validating information stored in the Blockchain, ensuring that events are transparently recorded and accessible to users. The integration of these technologies aims to provide a reliable and automated solution for event detection

while enhancing trust verification mechanisms to curb the spread of misinformation.

LITERATURE SURVEY

Zeinab Shahbazi; Yung-Cheol Byun., Blockchain-Based Event Detection and Trust Verification Using Natural Language Processing and Machine Learning Information sharing is one of the huge topics in social media platform regarding the daily news related to events or disasters happens in nature or its human-made. The automatic urgent need identification and sharing posts and information delivery with a short response are essential tasks in this area. The key goal of this research is developing a solution for management of disasters and emergency response using social media platforms as a core component. This process focuses on text analysis techniques to improve the process of authorities in terms of emergency response and filter the information using the automatically gathered information to support the relief efforts. Specifically, we used state-of-art Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP) based on supervised and unsupervised learning using social media datasets to extract real-time content related to the emergency events to comfort the fast response in a critical situation. Similarly, the blockchain framework used in this process for trust verification of the detected events and eliminating the single authority on the system. The main reason of using the integrated system is to improve the system security and transparency to avoid sharing the wrong information related to an event in social media.

Jayakumar D; Haripriya G; Ramkumar M. O; Manjula S, Blockchain based Secure Event Management System using NLP and RNN Algorithm, When it comes to the daily news about incidents or disasters that occur in nature or are man-

made, exchange of information is among the most contentious issues on social media sites. The suggested system aims to enhance the security and trustworthiness of event information by leveraging the immutability and decentralization properties of blockchain technology, as well as the accuracy and efficiency of NLP and RNN algorithms in processing and analyzing natural language data. The NLP and RNN algorithms are then applied to the data to detect and verify the authenticity and relevance of the event information. The blockchain technology is used to store and distribute the validated event data in a secure and decentralized manner.

Zonyin Shae; Jeffrey Tsai, AI Blockchain Platform for Trusting News, An interdisciplinary effort is needed for solving the fake news crisis, because the solutions depend not only on AI, but also on social mechanisms. In this paper, we propose an AI blockchain platform to build a strong collaboration among AI blockchain researchers and news media to advance the research fighting against fake news. This platform will provide journalists with blockchain crowd-sourced and AI validated factual data on emerging news. This platform will gather blockchain traced data and AI tools that can provide pointers to the original data sources, news propagation path, AI analyzed experts to consult on a given topic. This will provide journalists with cheaper and reliable sources of information in the Internet social media age. So that factual-sourced reporting can outpace the spread of fake news on social media which will encourage factual news sources as a way to value and promote truth for society. The technical contributions of this paper are

(1) mechanism building the factual news database, (2) mechanism generating the news blockchain supply chain graph, and (3) AI blockchain based crowd sourcing fake news ranking mechanisms (4)

AI blockchain platform for trusting news ecosystem. (5) reviewing the state of fake news research from the technology and social aspects, and providing list of key research issues and technical challenges.

Li-Der Chou; Chia-Wei Tseng; Fan-Hsun Tseng; Chien-Chang Liu, Blockchain-Based Traffic Event Validation and Trust Verification for VANETs, Sharing traffic information on the vehicular network can help in the implementation of intelligent traffic management, such as car accident warnings, road construction notices, and driver route changes to reduce traffic congestion earlier. In the future, in the case of autonomous driving, traffic information will be exchanged more frequently and more immediately. Once the exposed traffic incident is incorrect, the driving route will be misleading, and the driving response may be in danger. The blockchain ensures the correctness of data and tampers resistance in the consensus mechanism, which can solve such similar problems. This paper proposes a proof-of-event consensus concept applicable to vehicular networks rather than proof-of-work or proof-of-authority approaches. The traffic data are collected through the roadside units, and the passing vehicles will verify the correctness when receiving the event notification. In addition, a two-phase transaction on blockchain is introduced to send warning messages in appropriate regions and time periods. The simulation results show that the proposed mechanism can effectively feedback the correctness of traffic events and provide traceable events with trust verification.

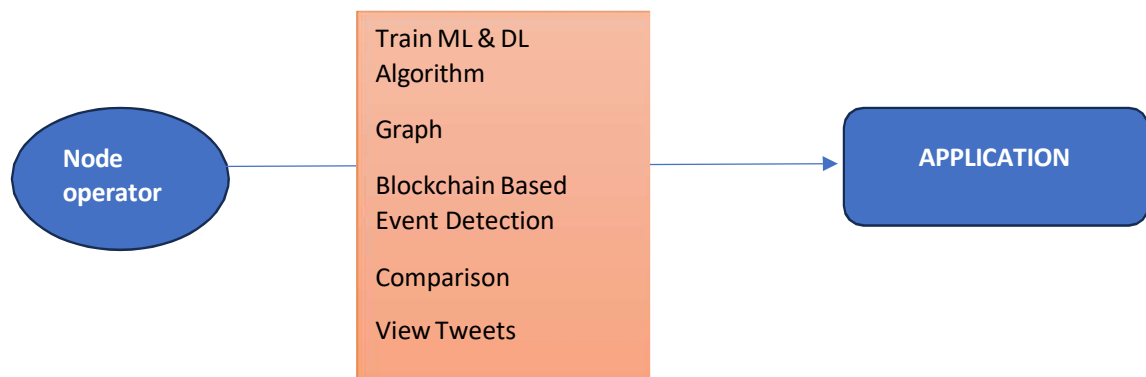
Zeinab Shahbazi; Yung-Cheol Byun, Fake Media Detection Based on Natural Language Processing and Blockchain Approaches, Social media network is one of the important parts of human life based on the recent technologies and developments in terms of computer science area. This environment has

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. To overcome this problem, we have proposed an integrated system for various aspects of

blockchain and natural language processing (NLP) to apply machine learning techniques to detect fake news and better predict 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.

SYSTEM DESIGN

SYSTEM ARCHITECTURE



DESIGN

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by

having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in

providing input.

- Methods for preparing input validations and steps to follow when error occur.

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. Select methods for presenting information. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

IMPLEMENTATION

NODE OPERATOR

In this module, the Node operator has to login by using valid user name and password. After login successful he can do some operations such as Train & Test Agriculture Crop Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Agricultural Text Classification Type, View event detection Text Classification Type Ratio, Download Predicted Data Sets, View Event detection Text Classification Type Ratio Results, View All Remote Users. **View and Authorize Users**

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

RESULTS/DISCUSSION

SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application

.it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

INTEGRATION TESTING

Integration tests are designed to test integrated

FUNCTIONAL TEST

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input identified classes of valid input must be accepted. Invalid Input identified classes of invalid input must be rejected. Functions identified functions must be exercised. Output identified classes of application outputs must be exercised. Systems/Procedures : interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before

BLACK BOX TESTING

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a

software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

functional testing is complete, additional tests are identified and the effective value of current tests is determined.

SYSTEM TEST

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

WHITE BOX TESTING

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box you cannot “see” into it. The test provides inputs and responds to outputs without considering how the

software works.

UNIT TESTING

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

TEST STRATEGY AND APPROACH

Field testing will be performed manually and functional tests will be written in detail.

TEST OBJECTIVES

- All field entries must work properly.

- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

FEATURES TO BE TESTED

- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

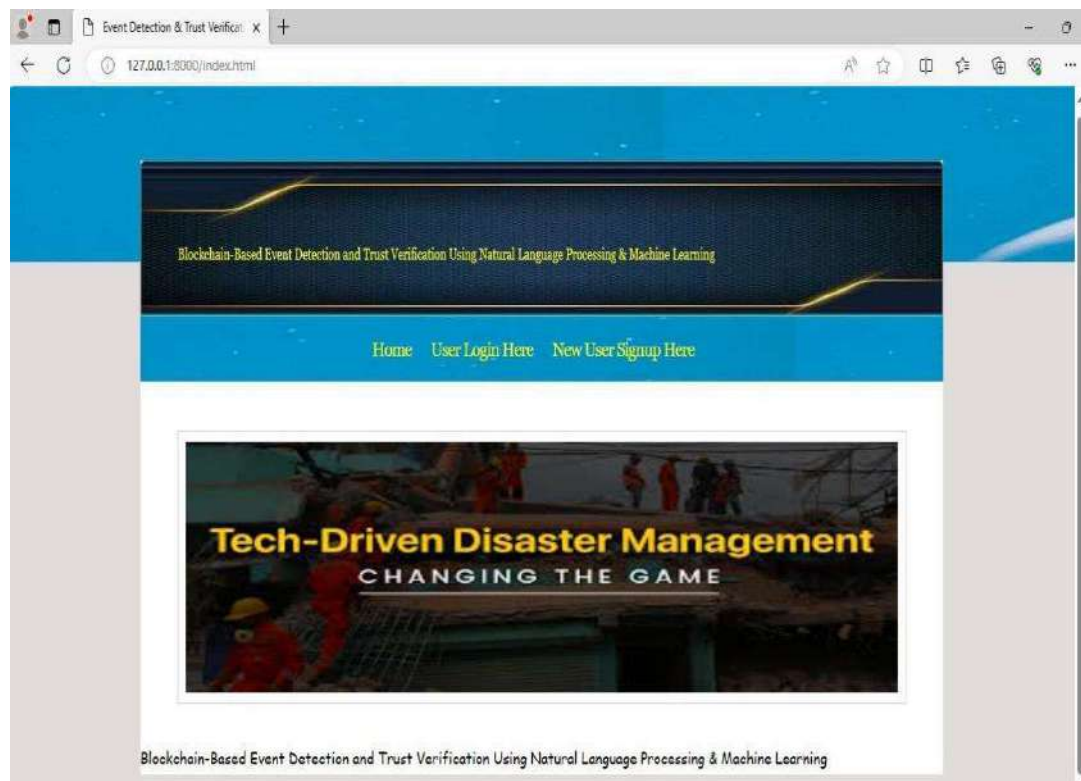
INTEGRATION TESTING

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

RESULT

SCREENSHOTS

FIG 1:



In above screen click on 'New User Signup Here' link to get below page

FIG 2:


127.0.0.1:8000/Register.html

Home User Login Here New User Signup Here

Tech-Driven Disaster Management
CHANGING THE GAME

New User Signup Screen

Username:

Password:

Contact No:

Email ID:

Address:

In above screen user is entering signup details and then press button to get below page

FIG 3:


127.0.0.1:8000/registration

Home User Login Here New User Signup Here

Tech-Driven Disaster Management
CHANGING THE GAME

New User Signup Screen

Signup process complete and record saved in Blockchain

Username:

Password:

Contact No:

Email ID:

Address:

In above screen signup task completed and similarly you can add as many users as you want. Now click on 'User Login Here' link to get below page

FIG 4:


In above screen user is login and after login will get below page

FIG 5:


In above screen click on 'Train ML & DL Algorithms' link to get below page

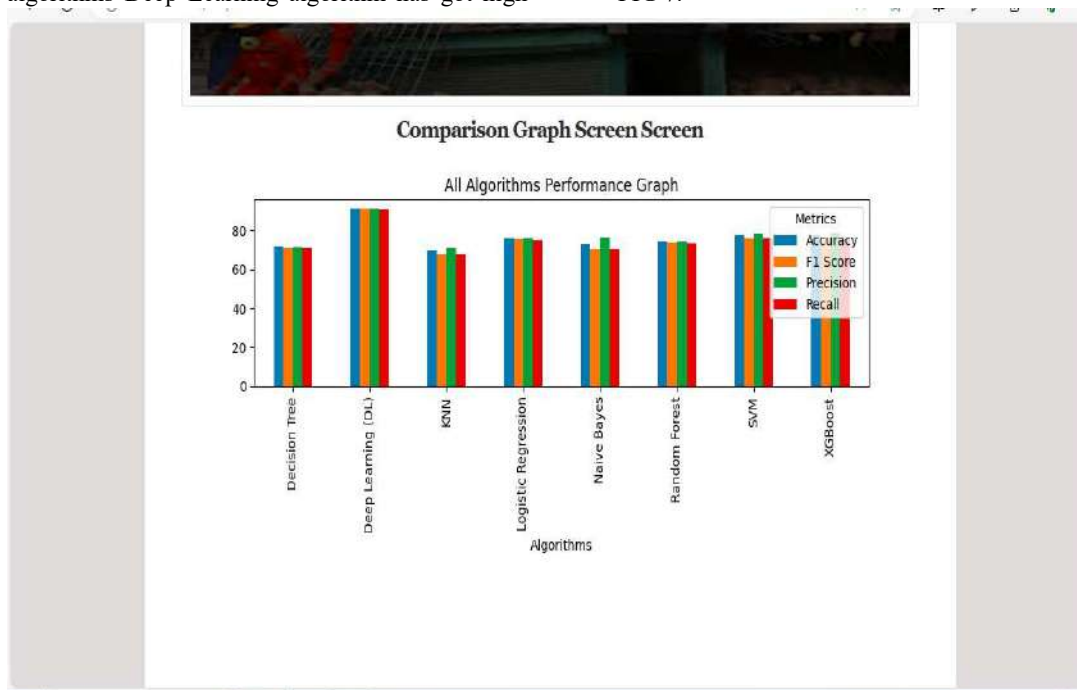
FIG 6:



In above screen all algorithms training completed and can see performance of each algorithm and in all algorithms Deep Learning algorithm has got high

accuracy and now click on ‘Comparison Graph’ link to get below page

FIG 7:



In above graph x-axis represents algorithm names and y-axis represents accuracy, precision and other metrics in different colour bars and in all algorithms

Deep Learning got high performance. Now click on ‘Blockchain Based event Detection’ link to get below page

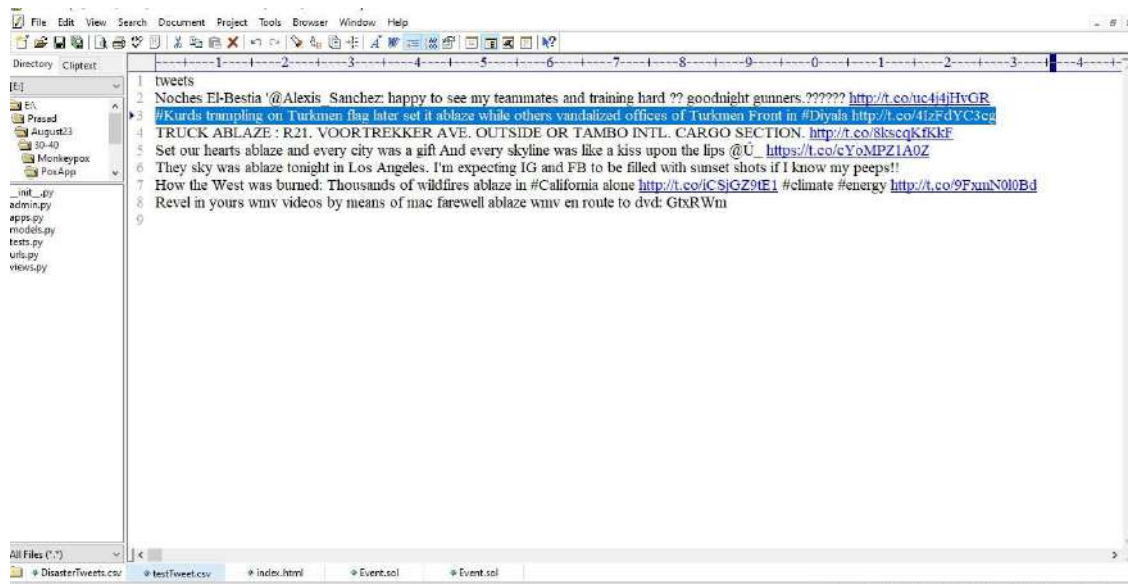
FIG 8:



In above screen user can enter some post and this post will get saved in Blockchain and ML algorithms will predict weather tweet is 'Normal or Disaster Events'. Emergency team will read all disaster

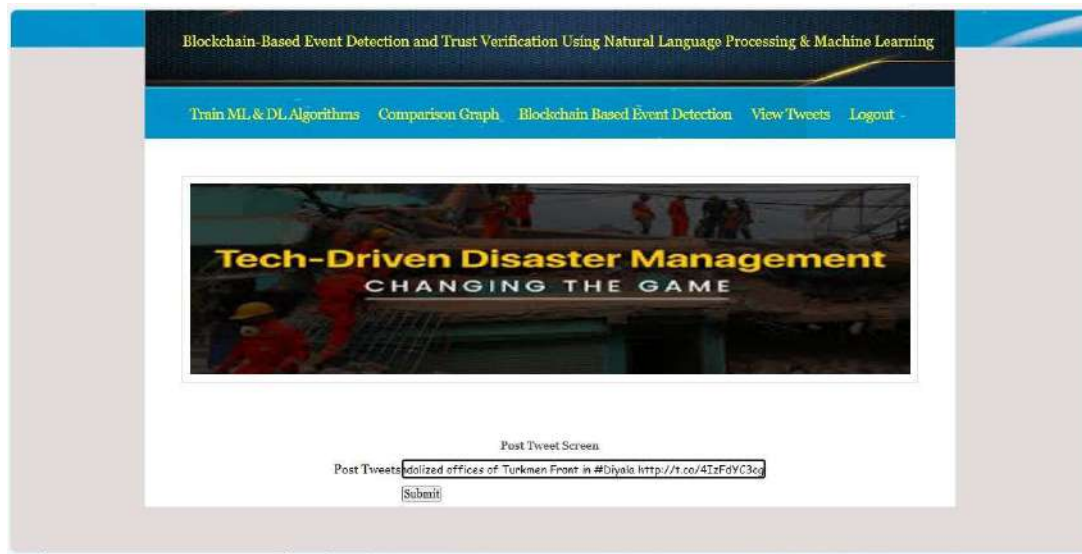
tweets and arrange their teams. If you don't know post details then you can copy tweet from 'test tweets.csv' file and paste in above field.

FIG 9



In above screen copying some tweets and paste in below screen

FIG 10:



In above screen pasting copied tweet and then click on ‘Submit’ button to get below output

FIG 11:



In above screen in red colour text can see post classification result and this result will get saved in Blockchain. Similarly you can test other tweets and below are the other example

FIG 12:



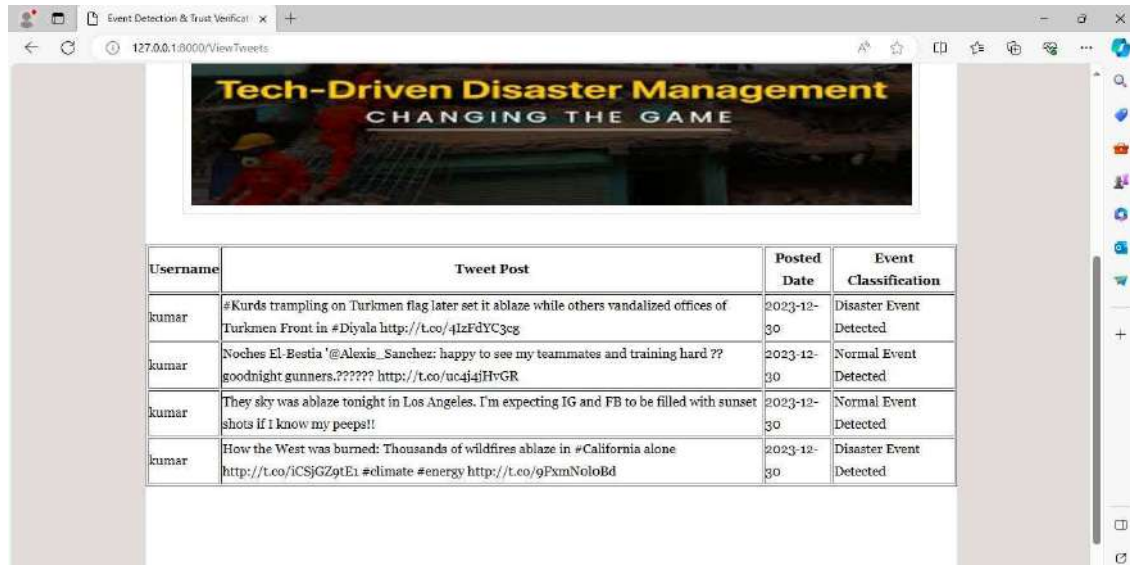
In above screen entered some other tweet and below is the output

FIG 13:



In above screen tweet classified as 'Normal Event' and now click on 'View Tweets' to get all tweets from Blockchain like below screen

FIG 14:



Username	Tweet Post	Posted Date	Event Classification
kumar	#Kurds trampling on Turkmen flag later set it ablaze while others vandalized offices of Turkmen Front in #Diyala http://t.co/4lzFdYC3eg	2023-12-30	Disaster Event Detected
kumar	Noches El Bestia '@Alexis_Sanchez: happy to see my teammates and training hard ?? goodnight gunners????? http://t.co/uc4j4jHvGR	2023-12-30	Normal Event Detected
kumar	They sky was ablaze tonight in Los Angeles. I'm expecting IG and FB to be filled with sunset shots if I know my peeps!!	2023-12-30	Normal Event Detected
kumar	How the West was burned: Thousands of wildfires ablaze in #California alone http://t.co/iCSjGZgtE1 #climate #energy http://t.co/9FxmNoloBd	2023-12-30	Disaster Event Detected

In above screen all users can see 'tweets' uploaded by different users and can see tweet message, date and predicted event type. All the above tweets are fetching from decentralized Blockchain servers. Similarly you can add any number of tweets which will saved in Blockchain and ML will classify tweets event type.

CONCLUSION

In conclusion, the Blockchain-Based Event Detection and Trust Verification project represents a groundbreaking initiative to address the challenges associated with the reliability of event information on social media. By combining Blockchain's decentralized and tamper-proof architecture with the analytical capabilities of NLP and ML, the proposed system offers an automated and secure solution for event detection and trust verification. The implementation of smart contracts further streamlines the validation process, providing users with a trustworthy and transparent mechanism to verify the authenticity of shared events. This project contributes to the development of more reliable information ecosystems, fostering a safer and more

informed online community.

FUTURE SCOPE

The future scope for blockchain-based event detection and trust verification using natural language processing (NLP) and machine learning (ML) is poised for remarkable advancements. As NLP and ML algorithms continue to evolve, they will play a pivotal role in enhancing the reliability, security, and efficiency of blockchain networks. One area of exploration lies in refining trust mechanisms within blockchain systems, leveraging NLP and ML to analyze and verify the authenticity of information and transactions. Additionally, advancements in event detection techniques, empowered by NLP algorithms capable of understanding the semantic meaning of text within blockchain transactions, will enable real-time monitoring and response to relevant events. Integration with emerging technologies such as IoT, AI, and edge computing will further bolster the capabilities of blockchain-based systems, enabling comprehensive monitoring and verification across diverse domains. Moreover,

addressing challenges related to scalability, privacy, and regulatory compliance will be crucial for unlocking the full potential of blockchain-based solutions in various industries, including finance, healthcare, supply chain management, and legal services. Overall, continued research and development in this field hold the promise of transformative innovations that will reshape the landscape of decentralized systems and foster trust and efficiency in an increasingly interconnected world.

REFERENCE

1. P. Williams, "Crisis management" in *Contemporary Strategy*, Evanston, IL, USA:Routledge, pp. 152-171, 2021.
2. L. Ardito, M. Coccia and A. M. Petruzzelli, "Technological exaptation and crisis management: Evidence from COVID-19 outbreaks", *RD Manage.*, vol. 51, no. 4, pp. 381-392, Sep. 2021.
3. J. Abbas, D. Wang, Z. Su and A. Ziapour, "The role of social media in the advent of COVID- 19 pandemic: Crisis management mental health challenges and implications", *Risk Manag. Healthcare Policy*, vol. 14, pp. 1917, May 2021.
4. S. Wang, Z. Yang and Y. Chang, "Bringing order to episodes: Mining timeline in social media", *Neurocomputing*, vol. 450, pp. 80-90, Aug. 2021.
5. S. G. Arapostathis, "A methodology for automatic acquisition of flood-event management information from social media: The flood in Messinia South Greece 2016", *Inf. Syst. Frontiers*, vol. 23, pp. 1127-1144, Jan. 2021.
6. Kruspe, J. Kersten and F. Klan, "Detection of informative tweets in crisis events", *Natural Hazards Earth Syst. Sci.*, 2021, [online] Available: <https://nhess.copernicus.org/articles/21/1825/2021/>.
7. M. Fedoryszak, B. Frederick, V. Rajaram and C. Zhong, "Real-time event detection on social data streams", *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, pp. 2774-2782, Jul. 2019.
8. F. Jamil, L. Hang, K. Kim and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital", *Electronics*, vol. 8, pp. 505, Apr. 2019.
9. F. Jamil, S. Ahmad, N. Iqbal and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals", *Sensors*, vol. 20, no. 8, pp. 2195, Apr. 2020.
10. B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system", *Comput. Netw.*, vol. 200, Dec. 2021.