



Vel Tech
Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology
(Deemed to be University Estd. u/s 3 of UGC Act, 1956)

Department of Information Technology
Major Project Review 0

**FORGERY DATA DETECTION FOR NATIONAL
SECURITY USING BLOCKCHAIN**

SUPERVISED BY

Mrs. JAYANTHI. K
M.Tech
Assistant Professor

PRESENTED BY

Yugandhar Surya (VTU 12278)

FORGERY DATA DETECTION FOR NATIONAL SECURITY USING BLOCKCHAIN

ABSTRACT

One of the most important outlets for exchanging information between social groups is social networking. Not only real news, but also rumours and fake news, are widely disseminated via social media. Users benefit from online platforms since they can simply get news. However, this provides a chance for cyber thieves to distribute bogus news via these channels. Readers read the news and begin to believe it before verifying it. Detecting false news is a significant difficulty since it is not a simple process. To address this issue, blockchain is being utilised to control the spread of misinformation. The suggested system records and analyses disseminated material, limiting the amount of fake news and user manipulation. The system also includes a real-time alert panel that uses user votes to determine the truth of the news.

Once the threshold value is achieved, the news status is continually monitored and adjusted. The false word data collection may be used to identify misleading phrases and stop fake news from spreading. To reduce the consequences of rumours and their uncontrolled spread, all news that reaches the public eye must first be cross-verified by intellects. With the use of block-chain, the proposed initiatives might give governmental entities the capacity to check material and decide whether or not it is authentic enough to be spread among everybody. Because, unlike traditional methods, blockchain tends to share copies of the same data to every individual with hash codes in the system, the certainty that the data cannot be hijacked or corrupted is strong. Along with various characteristics that protect data from cyber-attacks, blockchain technology has the potential to grow service in all areas while maintaining total transparency and intelligence.

Guided by

Mrs. JAYANTHI. K

M.Tech

Assistant Professor

Presented by

Yugandhar Surya (VTU 12278)

INTRODUCTION

Blockchain is basically an storage or electronic ledger which safegaurds the digital data, information, content or currencies with locks in terms of hashes that changes each time if any change in information takes place anywhere in the chain. Change in the hash code keeps all the participants updated with new updates. In near future, Blockchain technology is likely to bring advancements in all sector including banks and online transactions, automobile, automotive, food supplies etc. Smart contract plays very crucial role in the field of blockchain. Smart contracts are similar as contracts but in e-format. Every participants of each chain are connected with each other through smart contracts. Blockchain re-evaluated the requirement of third-parties in trading or transactions and eliminated them which resulted in making the whole process de-centralized and secure.

Forgery in any kind of data or information becomes quite simple, nowadays technology like GANs is being used to generate deep fakes and fake images. The bitter truth is to be captured here is, these thing is being used in creating child sexual abuse material, bullying, financial fraud, revenge porn, fake news, etc.

The main reason behind these forgery data is the invisibility of the creator, mutable data, and insecurity on web2.0. At a saturated level machine or deep learning fails to identify the deep fakes and also to achieve high accuracy, these algorithms need data in bulk to train with, and to store big data high computational database is needed which will cost higher. Using blockchain the data will be transparent, secured, immutable and so the authenticity of data increases.

LITERATURE SURVEY

[1] L. Zhang et al.(2021).”Peer-to-Peer Networking and Applications” To take action against news and online curated content on the internet which could be inimical to the sovereignty of any nation, the proposed solution being implemented by smart contracts may have the capacity to identify and flag such content on websites and social media. According to L. Zhang et al.(2021)[1] Fake news, press freedom disputes, advertising fraud, difficulty in digital rights management, flaws in content creation methods, and rumour spreading exacerbated by social media are all challenges that content producers and social media must deal with. All of the difficulties stated above are mostly caused by centralized servers or, to put it another way, management and all of the conceivable decisions made by a single person, allowing anybody to modify data as they choose. Blockchain technology, characterized by decentralization, security, and tamper-proof, offers a brand-new perspective on the above problems.

[2] P. Fraga-Lamas and T. M. Fern´andez-Caram´es (2020) ”Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality”, fake news raises worries about the Internet and social media’s role in modern democratic countries, which might result in large economic losses or national security problems. This study attempts to investigate the potential of distributed ledger technologies (DLTs) to prevent digital deception by defining the most relevant applications and identifying the main problems they face. Blockchain and other distributed ledger technologies (DLTs) guarantee the provenance and traceability of data by providing a transparent, immutable, and verifiable record.

[3] S.Cho and C.Jeong (2019) ”A blockchain for media: Survey”, In their study they have stated that We can assure that any type of content is fully secured using blockchain. In their paper, they looked at how to characterise blockchain in digital subjects like media and interactive media as media blockchain. They also stated that a network is made up of devices that are lightweight, such as low storage space and computing performance, and that these issues degrade network security performance. It can be used for tracing and managing right information on content delivery platforms.

[4] S. E. Haddouti, et.al, 2019, ”Analysis of Identity Management Systems Using Blockchain Technology,”. They have investigated and gives us analysis of the most popular Identity Management Systems using Blockchain: uPort, Sovrin, and ShoCard. It then evaluates them under a set of features of digital identity that characterizes the successful of an Identity Management solution. The comparison analysis findings are provided in a clear and straightforward manner, allowing readers to quickly determine which systems meet which standards, allowing them to choose the best system for a given scenario.

[5] Shilpashree B N, et al.(2021),“Counterfeit Detection of Documents using Blockchain” it’s shown that InterPlanetary File System [IPFS] protocol and also a peer-to-peer-network for storing and sharing data in a distributed file system and can make a system that will be more secure and efficient for digital certificate validation.They advocated using blockchain technology to solve the problem of document counterfeiting.The blockchain technology offers the user’s documents with the authentication, authorisation, privacy, secrecy, and ownership that are required attributes of digital documents.

EXISTING SYSTEM

Existing system runs with the help of Machine learning and natural language processing and it tries to aggregate the news and later determine whether the news is real or fake using Support Vector Machine. It has higher data set. The ML based system has centralised access to the data, and it can be easily manipulated by anyone. Because of the multi-dimensional nature of fake news, the recognizing the category of news is not so easy. The proposed strategy is completely made out of Artificial Intelligence which is basic.

PROPOSED SYSTEM

The proposed system tracks and analyzes the news that is shared, thus restricting where it is fake or user manipulated. The system also proposes a real-time alert panel that aims to find out the reality of the news by taking user's votes. The news status is constantly tracked and then eventually modified once the threshold value is reached. The fake word data set can be used to spot misleading terms and prevent the fake news.

Pros:

- Decentralized structure and Trust
- Immutability
- Transparency

FEASIBILITY STUDY

A feasibility study is a test of a system proposal according to its work ability for impact organization, to meet user needs and effective use of resources. The objective of a feasibility study is not to solve only the problem, but to acquire and sense of its scope. During the study, the problem definition is crystallized and the aspects of the problem to be included in the system are determined. After the initial investigation of the system that helped to have in-depth study of the existing system, understanding its strength and weaknesses and the requirements for the new proposed system.

Economic Feasibility:

Economic feasibility deals about the economic impact faced by the industry to implement a brand new system. The proposed system provides an efficient outcome. The whole setup is processed with ethereum based transactions. Cost per usage is least and it provides an safe digital transaction.

Technical Feasibility:

Technical Feasibility centers on the existing computer system. It can support the proposed system in addition proposed system IPFS database used for easily accessibility of data, ReactJs is used for SPA(Single Page Application) and it is a user friendly application.

Social Feasibility:

The aspect of social feasibility is to test the amount of acceptance of the system by the user. The project has software installations that are easily accessible and operational to common user. It is an asset to eradicate spread of fake data along web. It is user-friendly after a briefing on the system connections.

Market Feasibility:

The application would be free of cost for users. Prediction and estimation of the budget will be based on size, server, and project maintenance costs. A statistical analysis of the no. of consumers and participating retailers would decide the market scope of the application.

SYSTEM DESIGN

Architecture diagram:

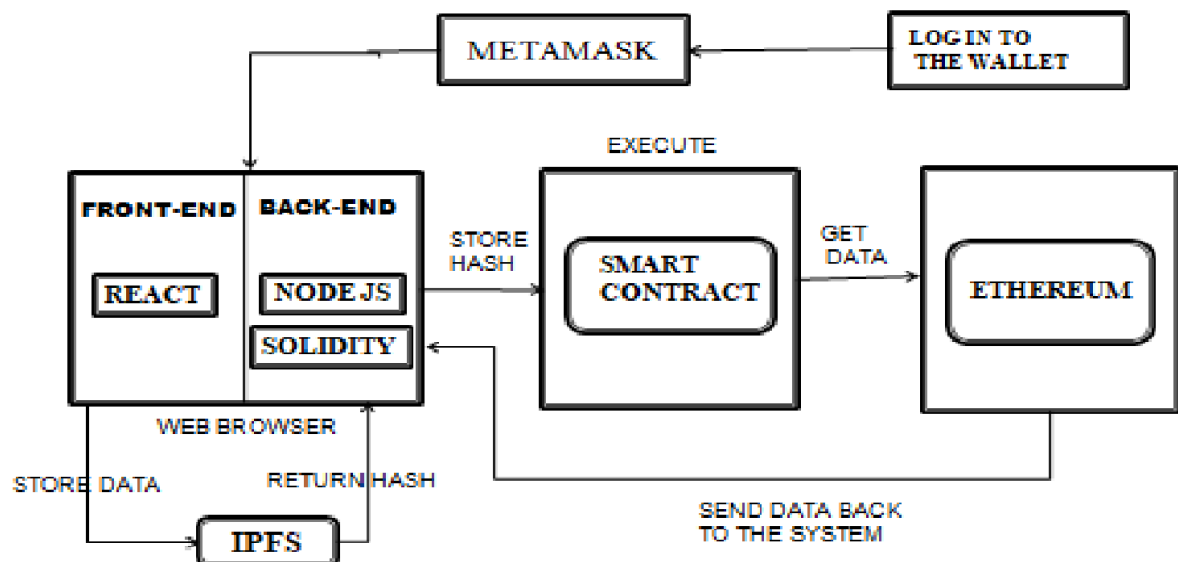


Fig 1: Architecture diagram

Given architectural diagram is pictorial representation of step-by-step procedure that we followed to receive desired output. The proposed system has a transactional architecture. It works on the block chain framework. The system uses ganache that provides counterfeit currency to be used in local host and metamask for smart contract based transaction. Ethereum is used for the transactional functioning. The front end is procured using ReactJs and the back-end is managed by solidity. Metamask is the web extension that helps in logging to the crypto wallet and it is used for getting the data and sending it back to the system.

CONCLUSION

A new system is proposed to detect and avoid further spreading of fake news and validate the information from origin. The proposed systems make use of block-chain technology for verifying the source and content of the news. Using block chain makes it secure, transparent, smart and efficient as it identifies the user's malicious intent (if any) and hence prevents it from spreading fake news. It also restricts any further change in the content ones uploaded and reduces the chance to escape after creating a havoc. RTAP (Real Time Alert Panel) keeps track of the live news and constantly updates news status. Block chain based forgery data detection preserves the interest and sterility of the readers.

REFERENCES

1. Liqun Liu, Weihang Zhang, Cunqi Han, 2021, "A survey for the application of blockchain technology in the media", Peer-to-Peer Networking and Applications, Issue 5, May 2021
2. P. Fraga-Lamas and T. M. Fernández-Caramés, 2020, "Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality," in IT Professional, vol. 22, no. 2, pg no. 53-59, Issue March-April 2020.
3. S. Cho and C. Jeong, 2019, "A blockchain for media: Survey", 2019 International Conference on Electronics, Information, and Communication (ICEIC), Issue Jan 2019, pg no. 1-2.
4. S. E. Haddouti and M. D. Ech-Cherif El Kettani, 2019, "Analysis of Identity Management Systems Using Blockchain Technology," 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Issue April 2019, pg no. 1-7.
5. Shilpashree B N, Rohini Krishna Mohite, Sahana S, Rajesha, Rakesh K R, 2021, "Counterfeit Detection of Documents using Blockchain", International Journal of Engineering Research Technology, Volume 10, Issue 07, July 2021.
6. S. Paul, J. I. Joy, S. Sarker, A. -. A. -. H. Shakib, S. Ahmed and A. K. Das, "Fake News Detection in Social Media using Blockchain," 2019, 7th International Conference on Smart Computing Communications (ICSCC), pp. 1-5, September 2019.
7. M. Torky, Emad Nabil, Wael Said, 2019, "Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks." International Journal of Advanced Computer Science and Applications (2019), Vol. 10, Issue No. 12.
8. Yazed Alsaawy, Ahmad Alkhodre, Nour Mahmoud Bahbouh, Adnan Abi Sen, Adnan Nadeem Al Hassan, 2021, "Lightweight Chain for Detection of Rumors and Fake News in Social Media", International Journal of Advanced Computer Science and Applications, August 2021.