Transparent and Genuine Charity Applications based on Blockchain

Rushabh Mavkar[1], Kartik Abuj[2], Nikhil Sapre[3], Prof. Sagar Dhanake[4]

Student, Computer Engineering, DYPIET, Pune, India[1, 2, 3]

Assistant Professor, Computer Engineering, DYPIET, Pune, India[4]

Abstract: Blockchain technology has opened the gate of creating decentralized applications, where security is a big concern. Here, any transaction ever held is recorded permanently. Over the years, some non-reputable sources have been publishing fake and attractive news stories. Due to the lack of any regulatory systems, this news cannot be verified. Hence, these unreliable sources can publish whatever they want, and even in some cases, it causes chaos in society. In recent times due to the ease in internet availability and social media, inappropriate news can spread more quickly than ever before. In some cases, fake news is more attractive than the real one. Thus, people become misguided. Using the advantages of Blockchain's peer-to-peer network concepts, we will discuss a way to detect fake news in social media

Keywords: Fake News, Social Media, Classification, Blockchain, Cryptocurrency.

I. INTRODUCTION

An enormous amount of data is produced on social networking in different formats of social media. Many people discuss it on the web through social networking when some event has occurred. They are searching for or retrieving and discussing news incidents as part of their daily routine. However, very big volumes of news or posts caused users to face the issue of overloading data during search and retrieving. Unreliable sources of data expose individuals to a dose of false news, hoaxes, rumors, theories of conspiracy and fake news. Social media is the source of all kinds of global and local news for most of the people in this generation. But it backfires when an individual/organization uses it to spread fake news. Because, in social media, clickbait stories take a brief time to spread exponentially. The news becomes viral worldwide just within days. These opportunist organizations or individuals are taking advantage of people's tendency to share appealing news without knowing its authenticity or consequences.

Based on the concept of blockchain in social media, our system will exploit the advantages of blockchains security, immutability and transparency to create trust among shared news. We will provide a hypothesis, which could be implemented in a decentralized social media and provide authenticity of some news among users.In this present context, it is tough to determine if a news is phony. No authority will certify valid news. If this task is given to an organization, there is a chance that the organization will be biased. Besides, the organization will have to carry out the whole responsibility of validation. In some extreme cases, the government might pressurize them. Whereas in Blockchain, we can offer a system where this validation can be done anonymously. The idea is that we will integrate social media in a Blockchain in such a way that random users (including journalists) will act as news validators. Because of anonymity, they can validate news without any external pressure. Therefore, they cannot be biased nor pressurized by any other person or organization. After publishing news, the news will deploy as a transaction in a chain. After a certain level of virality, the validator users will get a request to verify the news. As a validator, they will assign a correctness value for the news. The mean of those values will be the authenticity of that news. Because of the decentralized and anonymous system, their verification will be more transparent and trustworthy. After the verification is done, the news will have an authenticity rating on the top. This rating will be added wherever the news is shared.

II. MOTIVATION AND PROBLEM DEFINITION

Motivation

Sharing newsworthy information on social media platforms like Facebook, Twitter, and Instagram without evaluating its credibility has popped out a big challenge. Disseminating Misleading information and fake news across social networks represent a big dilemma against researchers and Social Network Service Providers (SNPs). Although AI has the best opportunity of recognizing misleading information, it is seriously able to create fake content on social media. Unfortunately, recently, the power of AI algorithms for identifying fake news is lower than its ability to create it. Therefore, it has become an essential need to search for an alternative robust and efficient technology for handling this

problem. Developing blockchain-based solutions have the potential to change the way of information creation and propagation. Blockchain can provide trustable, immutable, verifiable, reliable, and transparent transactions for designing a trusted social system.

Problem Definition

The extensive spread of fake news has the potential for extremely negative impacts on individuals and society. Therefore, fake news detection on social media has recently become an emerging research that is attracting tremendous attention. Therefore there is a need to build a platform to detect fake news.

III.   LITERATURE REVIEW

[1] Sharma, Sunidhi, and Dilip Kumar Sharma. "Fake News Detection: A long way to go." 2019 4th International Conference on Information Systems and Computer Networks (ISCON). IEEE, 2019
In this article they explored the system of fake news detection from large text data using machine learning. This approach is the collaboration of machine learning and natural language processing techniques. The numerous techniques used by prior studies in the very same field were even included in the scheme. Use several experiments as examples, and the device studied the fundamentals of specific strategies used in detecting fake news. In this study, the future implications are also included together with the obstacles one faces and doing research here in this area. The propaganda of the world, Fake Media refers in laymen's terms to the deliberate or accidental distribution of misleading info also on a public forum.

[2] Fitwi, Alem, Yu Chen, and Sencun Zhu. "A lightweight blockchain-based privacy protection for smart surveillance at the edge." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019
In this article they discussed a Confidentiality Security Compact (CSC), a cryptocurrency framework for edge cameras. This helps the VSS to carry out monitoring before violating the privacy of individuals caught in the videos. The Lib-Pri system converts the VSS implemented into a design that acts as a nonfederal bitcoin blockchain consisting of integrity testing, maintenance of obscuring keys, exchanging of functionality, and penalizing of video access. The policy-based implementation of privacy provisions is carried out without burdening the system at the edge of actual video monitoring devices. Concerning security cameras, a variety of claims and opinions are being raised in support of and those against.

[3] Bhoir, Smita Vinit. "An Efficient FAKE NEWS DETECTOR." 2020 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2020.
In this article they discussed the strength of the Internet which has grown massively over the past decades, thereby giving paws to disinformation, which is a rising issue as it is the misinformation that makes it all too harder to discern the truth in material. Therefore, the panacea is to provide a well thought and total proof device that tracks the various trends in the news that really can help us decide if it is true or not. With the assistance of computer vision, the proposed approach aims to recognize fake news leveraging hybrid models. This design significantly decreased learning time and improved SVM classifiers. This hybrid model performed well in comparison to the Random Forests (RF) algorithm and Vector Support Operator when designed separately.

[4] Xu, Ronghua, et al. "Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.
In this article they present a Cryptocurrency Decentralized Infrastructure for Smart Community Safety Kubernetes. A protection framework based on micro-services is implemented inside a licensed public blockchain to protect data access control in an SPS framework. Intelligence services technology is decoupled into independent container-based microprograms that are designed using a consensus protocol and implemented on nodes of edges and cloud technology. A comprehensive observational design confirmed that the theoretical BlendMAS is capable of offering a distributed IoT-based SPS framework with hierarchical, scalable, and stable sharing data and intrusion detection. Smart National Security systems store multichannel audio from the edge of surveillance and use multiple embedded technologies. Cloud services deployed on the private Cryptocurrency blockchain are converted into digital form to the hash index user authentication experienced numerous times. Smart monitoring and intelligence services functionality is decoupled into the distinct container-based microservice architecture and distributed on decentralized edge or cloudlet nodes.

[5] Traylor, Terry, Jeremy Straub, and Nicholas Snell. "Classifying fake news articles using natural language processing to identify in-article attribution as a supervised learning estimator." 2019 IEEE 13th International Conference on Semantic Computing (ICSC). IEEE, 2019

In this article they discussed a software defect prediction in which records the output of a Russian propaganda classifier. To create a new Russian propaganda tracker that uses referenced acknowledgement in a Probabilistic machine learning method as a defining aspect for estimating the probability that a news piece is fake, the Text blob, Artificial Intelligence, and SciPy Development tools were used. The resulting method accuracy is 63.33% successful in determining the probability that an essay with quotations is fake. This approach is called digging pressure, but this new method is portrayed as a methodology that can be used to detect false news and sometimes even misinformation. The qualitative research, advanced analytics, technical anthropology work, and reliability and results of classifiers are discussed in this paper. The pieces end with a summary of how the existing system can grow into an impact computing system.

[6] Wang, Weiwei. "Data Security of SaaS Platform based on Blockchain and Decentralized Technology." 2020 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2020

In this article they developed two dimensions. First, to help SaaS infrastructure, the centralized SaaS service platform focused on public cloud needs to recognize the functionality of virtualized environments, automated implementation and distribution, centralization of structured data, exchanging of knowledge, and efficient user and strategic efficiency. The centralized support network for the service is a way for computing. Third, our systems utilize P2P networks for data distribution in part in response to the cryptocurrency system. The findings are appropriate. Bitcoin has been the most rudimentary and essential implementation of the network, as an authenticated cryptocurrency. Every node reproduces and updates the position of all cryptocurrency transactions in the Bitcoin protocol. Still, each time an order is created; all processors migrate to the next new state which records all purchases throughout the upgrade process.

IV. SYSTEM DESIGN AND FLOW
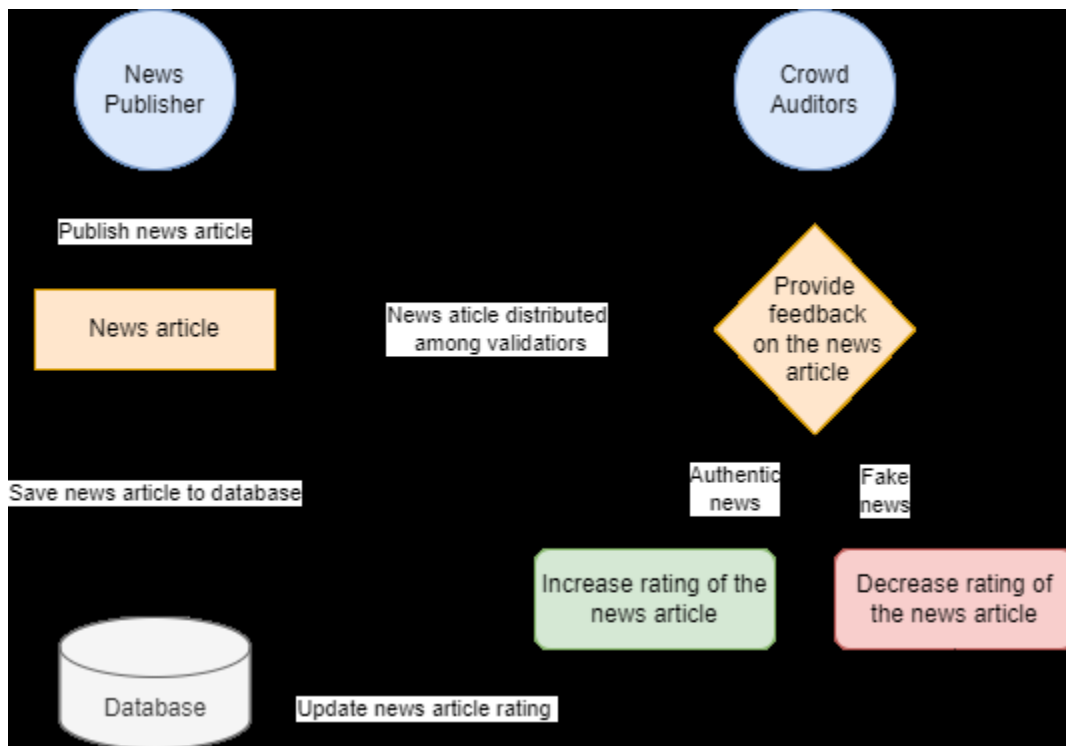
Fig.: System Architecture
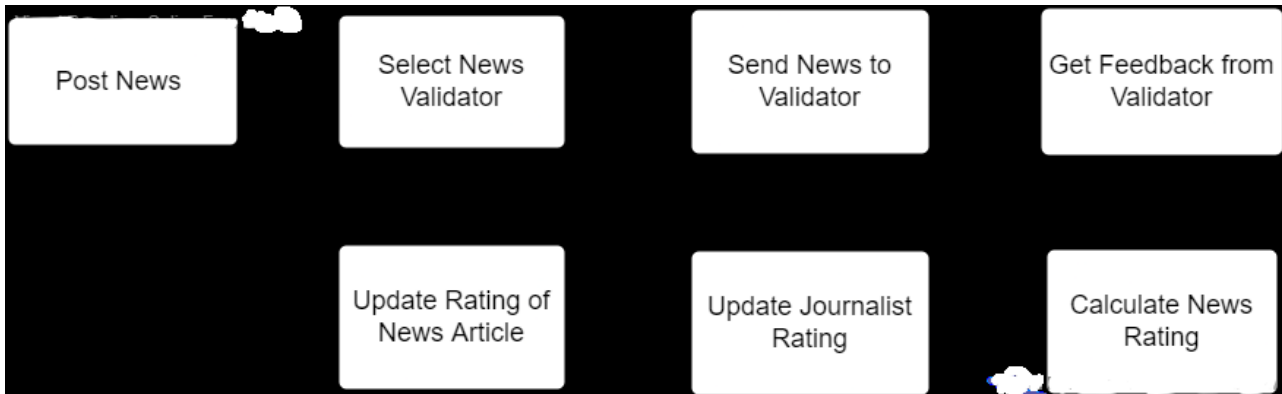
This model is categorized into five main parts:

• Whenever news has been created, it will be broadcast through the chain by the transaction .

• As time passes by, validators will provide their reviews, and then the news will pop up with a rating to the users. This rating represents the correctness/authenticity of particular news.

• Here, we propose a weight-based validation. There will be two types of weights. This weight determines the probability of being selected as a validator. This will also have a further effect on the rating of a particular person.

• If someone from validators makes a mistake while detecting the fake news, their weight will be reduced. This reduction will be based on their rating. The more their rating deviates from the average rating of the news, the more their biases will reduce. If their rating is close to the actual rating of the news then their weight or biases will not be reduced.

V. PROJECT IMPLEMENTATION

A. Blockchain
The blockchain is merely a chain of blocks. When the words "block" and "chain" are said it is assumed that a block contains digital information and the information is stored in a public database (chain) as well.Blocks store information about transactions, e.g., transaction date, transaction time, and dollar amount of most recent purchase and also store information about participants in those transactions. Instead of using participants' real name it uses 'digital signature,' e.g., participants' Public Key. Blocks don't repeat the same information among them; instead they use unique hash code to distinguish information. A single block on the blockchain can store up to 1 MB of data. Anyone can set-up a node that replicates all the data necessary for all nodes to reach an agreement on a Blockchain. Thus, being compensated by the other users and the application developers. This conforms to the privacy of users' data and lets the applications become truly decentralized.

B. Ethereum
The Ethereum is a decentralized platform featuring smart-contract. Smart-contracts are very effective to facilitate, verify or negotiate a contract agreement in Blockchain. Basically, smart-contracts a set of conditions and promises. To initiate a contract, the users involved in the contract will agree to the conditions. Once the required conditions are met, the promise will automatically be carried out by the system. Using the Ethereum chain, the transaction done is undoubtedly trustworthy. This method makes it bound to conduct the transactions honestly.

Algorithm Details:
SHA256 Algorithm:
Secure Hashing Algorithm (SHA) -256 is the hash function and mining algorithm of the Bitcoin protocol, referring to the cryptographic hash function that outputs a 256 bits long value. It moderates the creation and management of addresses, and is also used for transaction verification. With each iteration, the final output of the block serves as the input for the next block. The entire cycle keeps repeating until you reach the last 512-bit block, and you then consider its output the final hash digest. This digest will be of the length 256-bit, as per the name of this algorithm.
Haversine Distance Calculation Algorithm:
The Haversine formula is an equation important in navigation, giving great circle distances between two points on a sphere from their longitudes and latitudes.

– Calculate Distance:
Step 1: Get Latitude and Longitude coordinates of both location

Step 2: Multiply each coordinate with pi (3.14) and divide the result by 180
Step 3: Calculate distance between Longitudes of city
Step 4: Calculate distance between Latitudes of city
Step 5: Use Haversine Formula to calculate the distance
Haversine Formula =>
distance = 2 * sin(sqrt(sin(latitude_diff / 2)**2 + cos(lat1) * cos(lat2) * sin(longitude_diff / 2)**2))

– Calculate Article Rating:
Step 1 : Get Article Rating Given by Verifier
Step 2 : Get the validator rating and normalize it to 1.
Step 3 : Calculate the product of Article Rating and validator Rating.
Step 4 : Calculate the distance between article location and verifier location.
Step 5 : Multiply the calculate distance by 0.005 to normalize it.
Step 6 : Subtracts the updated Article Rating and the normalized validator rating to get the result.
new article rating = Given article rating * (User rating / 5) - (Location Distance * 0.005)

-- Calculate Validator Rating
Step 1. Get Previous Validator rating
Step 2. Get Previous Article Rating
Step 3. Get Article Rating given by Validator
Step 4. Calculate difference between previous rating and new rating
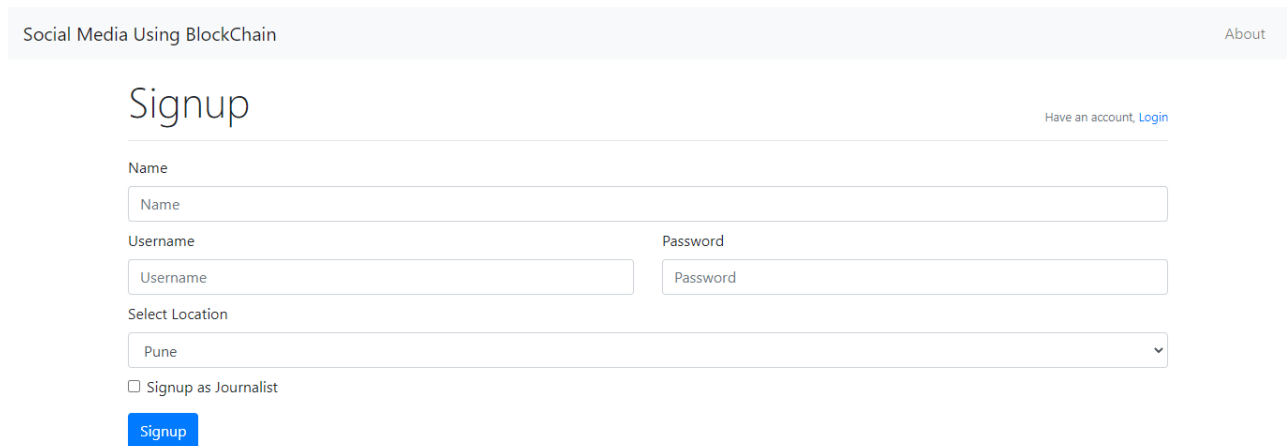**Step 5**. Normalize the difference to be within 1
Step 6. If the article has no previous rating do not change the difference
Step 7. If the difference is greater than standard deviation decrease the Validator rating by the difference
Step 8. If the difference is less than standard deviation increase the Validator rating by the difference
New user rating will be = Previous user rating - Normalized Difference

VI.   RESULTS
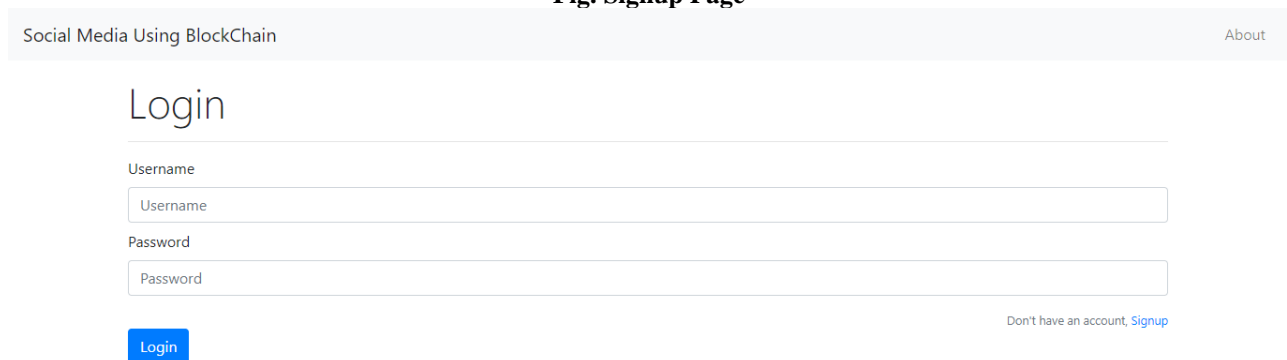
Fig. Signup Page

Fig. Login Page

Social Media Using BlockChain   Profile   About   Logout

Create New Article

Title

[Title]

Description

[Description]

[Submit]

Fig. Create New Article Page

Social Media Using BlockChain   Profile   About   Logout

[Create New Article]   [Show My Articles]

Total articles - 2

Rating : NaN ⭐ [0 users]   5/24/2022

Mumbai court remands four 1993 blast accused from Gujarat ATS to 7-day CBI custody

CBI took custody of four 1993 blast accused from Gujarat ATS and produced them before special court in Mumbai. The court remanded them 7 days CBI custody.

[View]

Rating : NaN ⭐ [0 users]   5/24/2022

Rs 1.5-crore forex seized at Kolkata airport

The Enforcement Directorate has recovered Rs 1. 5 crore unaccounted for forex from a domestic traveller at Kolkata airport and booked him for violations under Foreign Exchange Management Act. The passenger had arrived from Gorakhpur. The recovery was made after a search on the basis o...

[View]

Fig. Article Page

Social Media Using BlockChain   Profile   About   Logout

Rs 1.5-crore forex seized at Kolkata airport   [Vote]

NaN ⭐ by 0 users.

Written by Rushabh R Mavkar on 5/24/2022, 2:51:51 PM

[Pune]

The Enforcement Directorate has recovered Rs 1. 5 crore unaccounted for forex from a domestic traveller at Kolkata airport and booked him for violations under Foreign Exchange Management Act. The passenger had arrived from Gorakhpur. The recovery was made after a search on the basis of an information received from the Airport Intelligence Unit and the Customs at the airport on May 21. "During search, foreign currencies of $1,65,000 and 30,460 Euro were seized from him," said an officer.

Fig. Article Detail Page

Fig. News voting page

Fig. Validator Detail page

VII. ADVANTAGES AND APPLICATIONS

- **Traceability of the news:** Blockchain enabled applications can trace the authenticity of news from the start till the present and in future as well. It will prevent the readers from falling for the fake news.
- **Decentralized Approach:** With the approach of decentralized news platforms, the problem of fake news can be resolved. Moreover, an absence of centralization to store the data ensures no single points of failure.
- **Immutable Approach:** News content, videos or images saved on the Blockchain is immutable as they cannot be altered, changed or deleted.
- **Transparency in the news:** As the blockchain can provide transparency, the world would be able to discover if the news is fake or not. The authenticity of the news will be based on specific criteria defined in the smart contracts, generating trust and transparency amongst the whole world

VIII. LIMITATIONS

There are some significant challenges to the adoption of the blockchain. For example, political obstruction for publishing solid news against govt., so the regulatory of govt. is the real challenge. Sometimes if the minors are under the political influence, they may remark fake news to be valid which has been published in their political party's support. So, using the Ethereum blockchain, it's difficult to detect the news based on politics and religion. For its veridical verification system, journals and news portals have to face job risk as it drives them to a competition of obtaining ratings.

Although blockchain & Ethereum chain can save users from being misguided by reading fake news in social media, the consumption of computational power is also can't be neglected.

IX. CONCLUSION AND FUTURE SCOPE

Despite having some limitations, the proposed method will undoubtedly be helpful for detecting fake news in social media as spreading fake news via social media is a huge issue. This news misguides people just to achieve more page views to earn extra money dishonestly. Whereas, our hypothesis makes us bound to do these wrong doings.

REFERENCES

[1] D. Covucci and E. Ioanes, "The Complete History of Social Media," The Daily Dot, 2019. [Online]. Available: https://www.dailydot.com/debug/history-of-social-media/. [Accessed: 25- Mar- 2019].

[2] "Social media", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Social_media. [Accessed: 25- Mar2019].

[3] A. Mosseri, "Addressing Hoaxes and Fake News | Facebook Newsroom", Newsroom.fb.com, 2019. [Online]. Available: https://newsroom.fb.com/news/2016/12/news-feed-fyi-addressinghoaxes-and-fake-news/. [Accessed: 25- Mar- 2019].

[4] "EuroPCom 2018: 9th European Public Communication Conference", Cor.europa.eu, 2019. [Online]. Available: https://cor.europa.eu/en/events/Pages/EuroPCom-2018.aspx. [Accessed: 25- Mar- 2019].

[5] Investopedia. (2019). Blockchain, Explained. [online] Available at: https://www.investopedia.com/terms/b/blockchain.asp [Accessed 22 Mar. 2019].

[6] M. A. A. Mamun, J. A. Puspo and A. K. Das, "An intelligent smartphone based approach using IoT for ensuring safe driving," 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, 2017, pp. 217-223.

[7] A. K. Das, T. Adhikary, M. A. Razzaque and C. S. Hong, "An intelligent approach for virtual machine and QoS provisioning in cloud computing," The International Conference on Information Networking 2013 (ICOIN), Bangkok, 2013, pp. 462-467.

[8] S. Gilda, "Evaluating machine learning algorithms for fake news detection - IEEE Conference Publication," Ieeexplore.ieee.org, 2019.

[9] M. Granik and V. Mesyura, "Fake news detection using naive Bayes classifier - IEEE Conference Publication," Ieeexplore.ieee.org, 2019.

[10] A. Dey, R. Rafi, S. Hasan, and S. Kundu, "Fake news pattern recognition using linguistic analysis," Dspace.bracu.ac.bd, 2019.

[11] A. K. Das, A. Ashrafi and M. Ahmmad, "Joint Cognition of Both Human and Machine for Predicting Criminal Punishment in Judicial System," 2019 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 2019.

[12] FaNDeR: Fake News Detection Model Using Media Reliability - IEEE Conference Publication. [Accessed 22 Mar. 2019].

[13] S. Parikh and P. Atrey, "Media-Rich Fake News Detection: A Survey," Semanticscholar.org, 2019.

[14] Wang, Weiwei. "Data Security of SaaS Platform based on Blockchain and Decentralized Technology." 2020 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2020.