International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

FAKE NEWS DETECTION USING ML APPROACHES: A SYSTEMATIC REVIEW

V.KESAVA KUMAR MURTHY [1], Dr.V.Bhaskara Murthy[2]

[1]MCA Student, B V Raju College, Kovvada, Andhra Pradesh, India.
[2]HOD & Professor, B V Raju College, Kovvada, Andhra Pradesh, India.

ABSTRACT

The rise of ubiquitous deepfakes, misinformation, disinformation, and post-truth, often referred to as fake news, raises concerns over the role of the Internet and social media in modern democratic societies. Due to its rapid and widespread diffusion, digital deception has not only an individual or societal cost, but it can lead to significant economic losses or to risks to national security. Blockchain and other distributed ledger technologies (DLTs) guarantee the provenance and traceability of data by providing a transparent, immutable, and verifiable record of transactions creating a peer-to-peer secure platform for storing and exchanging information. This overview aims to explore the potential of DLTs to combat digital deception, describing the most relevant applications and identifying their main open challenges.Moreover, some recommendations are enumerated to guide future researchers on issues that will have to be tackled to strengthen the resilience against cyber-threats on today's online.

INTRODUCTION

GARTNER PREDICTS THAT the majority of individuals in developed economies will consume more false than true information by 2022.1 Digital deception is commonly recognized as deceptive or misleading content created and disseminated to cause public or personal harm (e.g., post-truth, populism, and satire) or to obtain a profit (e.g., click baits, cloaking, ad farms, and identity theft). In the context of mass media, digital deception originates either from governments or non-state actors that publish content without economic or educational entrance barriers. As a consequence, these horizontal and decentralized communications cannot be controlled or stopped with traditional centralized tools. In addition, this lack of supervision allows for security attacks (e.g., social engineering). Moreover, the veracity of information seems to be sometimes negotiable for the sake of

profit, as the competition is increasingly tough.

While trust in mass media and established institutions is declining, the use of social media is rising sharply and it has become an important source for the distribution of digital deception. Today, social media platforms miss an adequate regulation and their responsibilities are still not clearly defined. A number of issues are open, 2 such as the application of adequate data protection rules [e.g., General Data Protection Regulation (GDPR)] along with the market concentration in just a few social media companies worldwide.

Advances in artificial intelligence (AI) have recently been used to create sophisticated disinformation. As a result, a number of research projects as well as regulations have been launched to detect digital deception. 3 Nevertheless, researchers claim that ubiquitous content can be hardly supervised.

Today, distributed ledger technologies (DLTs) and specifically block chain present challenges, but also opportunities for stakeholders and policymakers as potential technologies that can help to combat digital deception. These technologies enable privacy, security, and trust in a decentralized peer-to-peer (P2P) network without any central managing authority. DLTs ability to combat digital deception is focused on controlling the traceability of the media, the communications architecture, and the transactions. However, the problems involved in developing effective ways to identify, test, transmit, and audit information are still open.

There are only a few articles of the literature that use block chain to combat digital deception and counterfeit reality, and they are mostly focused on tracing the source of the information. To the knowledge of the authors, this is the first article that proposes a global vision on how to confront fake news and deep fakes through DLTs with the aim of guiding researchers and managers on future developments. Thus, this article provides a comprehensive overview on the applicability of DLTs to tackle digital deception, showing the potential o DLTs for revolutionizing the media industry.

The rest of this article is organized as follows. The “State-of-the Art” section provides an overview of current digital deception and the involved technologies. The section, “DLT-Based Applications to Combat Digital Deception,” lists different DLT-based applications to combat digital

deception and counterfeit reality. In the section "Challenges and Recommendations," the main challenges of the application of DLT to tackle digital deception are analyzed and some recommendations are proposed. the "Conclusion" section is devoted to conclusions.

EXISTING SYSTEM

- Pang *et al.* [20] showed the progression of reviews as an important part of the decision-making process with the advent of Web 2.0 and studied them from retrieval perspective. Since it is difficult for the buyer to wade through volumes of reviews, researchers have conducted studies on summarizing reviews based on user sentiment [11] and other features [12]–[14] as well under the umbrella of opinion summarization. All these studies indicated that product reviews are an invaluable resource for determining the quality of a product.
- Various marketing studies have also shown that reviews play an important role in maintaining the online reputation of a brand as well [15], [16]. A review usually consists of a star rating that helps to influence a product's overall ratings, but a review becomes even more impactful when people read it. It has been found that people read a review only when it is perceived as helpful by them, which may be through various means—the helpful up votes by other consumers, the length of the review, star ratings, readability, and so on. [17], [22].
- Jindal and Liu [7] made a pioneering effort to detect fake reviews. They introduced the problem of opinion spam and analyzed online reviews in three varieties—untruthful opinions, seller/brand only reviews (no product involved), and non reviews using near-duplicate content as an indicator of fake reviews. Other studies dealing with the detection of review-level spam explored linguistic features of text [39], handmade rules [10], and combination of review and reviewer features [11]. A probabilistic framework for the same has also been proposed in [12].
- Ott *et al.* [19] synthesized fake hotel reviews using Amazon Mechanical Turk, whereas Jindal and Liu [18] worked on data

scraped from Amazon and used content duplicity as ground truth. Both of them worked with features at a review level. Jindal *et al.* [10] and Li *et al.* [11] mentioned the role of brands briefly, but the main focus was on fake reviews rather than extreme reviews.

Disadvantages

- In the existing work, the system is not implemented Distributed Ledger Technologies which is less effective
- This system does not aim to find behavioral characteristics of fake newsier.

PROPOSED SYSTEM

Decentralized Content Moderation: Conventional content moderation processes (e.g., flagging, notice and take down) rely on a centralized regulator with immediate content removal capabilities. In DLTs, especially in the case of permissionless ledgers, anyone can participate or become a transaction validator and there is no central authority, therefore additional consensusmechanisms should be implemented.

_ Trustworthiness Checkers: Qayyum et al.8 introduced the concept of proof-of-truthfulness, where any node in the network can verify whether a content is or not part of a blockchain. Content is stored in a Merkle tree, a binary tree built using hash pointers in which nodes at the n _ 1 level contain hash pointers to the content stored at the n level. Given a specific content, its trustworthiness could be verified by searching throughout a single tree branch from the content to the root (level 0)

_ Fact-Checking Incentivized dApps: Reliable factcheckers 9 can be identified (since they are interested in validating content) so they can get financial rewards (e.g., tokens), as well as increase their reputation for high-quality work. The amount of received rewards increases as the fact-checker improves his/her/its reputation.

In such a system, content creators will be also interested in submitting their content for validation in order to build their reputation.

_ Reputation Systems: A score can be used for measuring the credibility of a publisher and warn readers when the content shows traits that may indicate biases. In Qayyum et al.,8 a dynamic reputation set is proposed: an initial zero score is assigned to each non-verified media and the score evolves as the entity shares trustworthy verified news.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Registered consumers provide feedback through the platform or score the credibility of the content, like in the case of Bit- Press.10 Nevertheless, the problem of subjectivity, bias, and the risk of malicious actors have to be further studied.

Advantages

- Unlike other studies that majorly focus on fake news detection, we here focus on deepfake detection, which may not be fake.
- The system attempts to identify "group of fake news" instead of detecting "individual fake."

IMPLEMENTATION

News Server

In this module, the Admin has to login by using valid user name and password. After login successful he can perform some operations such as List all users and authorize, Register with News channel name and login, Add News Categories, Set news quantization date, Select category and add news, List all news post and give option to update and delete, List all news post by Distributed Ledger Technologies, List All News Posts by blocks based on news cat, List All Users News transactions by keyword, View online product Distributed Ledger Technologies by chart, View all news post rank in chart.

User

In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user can perform some operations like View your profile, Search news by content keyword, select hash code to show all news titles, Show all your search transactions based on keyword and view all fake news.

CONCLUSIONS

Provenance, consensus, and traceability can be guaranteed with DLTs when creating a P2P platform for tackling digital deception. This article analyzed some applications currently under development and proposed a number of additional mechanisms to control content. Although there are technological and practical limitations of the DLT technology when combating digital deception, the trust mechanisms provided by DLT can make it more adequate than other technologies for ensuring authenticity and auditing, enabling accountability and eliminating

counterfeit reality. Moreover, future researchers are encouraged to develop joint AI and DLT solutions in an enhanced coordinated effort to address all the aspects of digital deception.

REFERENCES

1. K. Panetta, Gartner Top Strategic Predictions for 2018 and Beyond. Gartner, Stamford, CA, USA, 2017.

2. J. Bayer, N. Bitiukova, P. B^ard, J. Szak^acs, A. Alemanno, and E. Uszkiewicz, Disinformation and Propaganda—Impact on the Functioning of the Rule of Law in the EU and its Member State. HEC Paris Research Paper LAW-2019-1341, 2019.

3. C. Wardle and H. Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making," Council of Europe Policy Report DGI(2017)09, 2017.

4. Z. Shae and J. Tsai, "AI blockchain platform for trusting news," in Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst., Dallas, TX, USA, 2019, pp. 1610–1619.

5. S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," Science, vol. 359, no. 6380, pp. 1146–1151, 2018.

6. H. Kim et al., "Deep video portraits," ACM Trans. Graph., vol. 37, no. 4, p. 163, 2018.

7. A. Shahaab, B. Lidgey, C. Hewage, and I. Khan, "Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review," IEEE Access, vol. 7, pp. 43622–43636, 2019.

8. A. Qayyum, J. Qadir, M. U. Janjua, and F. Sher, "Using blockchain to rein in the new post-truth world and check the spread of fake news," IT Professional, vol. 21,
no. 4, pp. 16–24, 1 Jul./Aug. 2019.

9. X. Zhang and A. A. Ghorbani, "An overview of online fake news: Characterization, detection, and discussion," Inf. Process. Manage., vol. 57, no. 2, 2020, Art. no. 102025.

10. BitPress Official Webpage, Feb. 2020. [Online]. Available: https://bitpress.news/

11. Solid Official Webpage, Feb. 2020. [Online]. Available: https://solid.mit.edu/

12. Content Blockchain Project Official Webpage Feb. 2020. [Online]. Available: https://irights-lab.de/en/launch-of-the-content-blockchain-project/