FAKE NEWS DETECTION IN SOCIAL MEDIA USING BLOCKCHAIN TECHNOLOGY

#1**Dr. M.ANJAN KUMAR,** ***Professor*****, Department of Computer Science & Engineering,**

VIVEKANANDA INSTITUTE OF TECHNOLOGY & SCIENCE, KARIMNAGAR, TS, INDIA.

#2**KISHOR KUMAR GAJULA,** *Ph.D Scholar,*
Dept of CSE, Shri JJT University, Rajasthan.

ABSTRACT: News from social media can have a big impact on public opinion, both positively and badly. When there is so much incorrect information out there, it's difficult to know what to believe. False information has a harmful influence on individuals as well as entire communities. We urgently want a way to detect and block the spread of false information on social media. As a result, spotting false news is both an urgent concern and a substantial challenge. The suggested research project's goal is to find and stop the spread of fake news. Machine learning is used to detect false news in a blockchain architecture. First, supervised machine learning and a blockchain infrastructure work together to uncover reputable news sources. Through mining, smart contracts, and proofs of work, it is feasible to build a blockchain environment (PoW). Detecting fake news on social media is currently the topic of a comprehensive systematic review. Once the system has been largely constructed, the conventional blockchain framework was utilised to test its performance. In a P2P setting, transaction verification by consensus takes 10% less time than it does in a conventional system.

Keywords: Fake News, Social Media, Classification, Blockchain, Cryptocurrency, Mining, Hash generation, Consensus.

---

1. INTRODUCTION

There is an impact on society regardless of how the information is disseminated: social media, traditional media, or news channels. "Fake news" refers to information that is disseminated to the public via social media, television, and other digital media in a way that makes it appear true but is not supported by any facts or proof. Dishonest information is referred to as "fake news" in this context. False information disseminated via social media sites like Facebook and Twitter could quickly throw millions of people into confusion. Use of fake news distribution can influence the outcome of elections, incite racial animosity in the public sphere, and much more.

To make matters worse, the propagation of fake news becomes extremely impossible to stop once it has gone viral. Inadequate fact-checking has led to a broad lack of trust in the media and news organisations. Blogs, videos and other forms of digital content are becoming widespread. A person does not have to verify the source or authenticity of the material before publishing it on social media. When presented with inaccurate information, the general public can be easily misled into thinking or altering their thoughts about a variety of topics, such as a certain group, religion, or even an individual.

Fake news can have a negative impact on anyone's reputation, public or private, regardless of how well-known they are. This problem can easily be solved by establishing an information flow monitoring and control centre. A single authority wielding too much influence in a decentralised social network weakens both trust and anonymity. According to a number of studies, blockchain technology is well-suited for a variety of non-financial applications, including voting, healthcare delivery, supply chain management, and a digital rights management system.

Blockchain and watermarking are the foundations of a social networking system proposed in this study. If you use our method, you can trace the source of fake news, which helps you stop it from propagating on social media. In the proposed social networking platform's planned design, all transactions completed by registered users are logged in a blockchain. There can be no doubt about the source of information transferred on a blockchain because it is completely transparent. The news source can be tracked down using blockchain thanks to timestamping and chain connections between blocks. Identifying the source of a piece of maliciously altered or fabricated news is critical to determining how a social media platform's users propagate it.

The headers of blockchain blocks contain data such as pre-block hash values and current block hashes. Using these headers, it is possible to track down information. When social media data is stored on the blockchain, it becomes more difficult for criminals to modify the data because each time a new user publishes or attempts to edit that data, a transaction trail is created. Using timestamps, anyone may determine the order of transactions on the blockchain. Blockchain technology suffers tremendously as a result of its network's restricted scalability [8]. Scalability has been a major concern since the beginning of blockchain. This solution makes use of BloXroute as a means of increasing network scalability. In order to ensure that the information has not been altered, digital watermarking is performed.

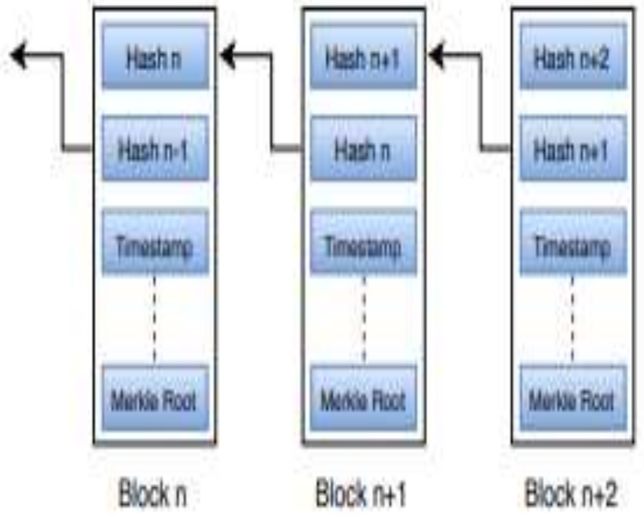

Fig. 1: Basic Blockchain Structure

2. BACKGROUND WORK

Rumor Iterative Spreading Process

To be able to spot fake news. It is vital to have a firm grasp on the mechanics of how rumours spread. The SIR model often requires individuals to make an immediate decision on whether or not to propagate the rumour [4]. Making a rapid and accurate judgement, on the other hand, necessitates careful consideration. Nobody has time to learn new things, let alone rationally think about them. Once the rumour is resisted, the user stops evolving until the rumour is extinguished. It is possible for the same event to elicit a wide range of emotions, from pleasant to negative, in different persons. On the other hand, those who have shaky beliefs are mostly undefined.

Many others are still sceptical and aren't spreading the rumour until they get more details. Many people could be fooled by this, but those who are close to the suspects might be able to get away with it. People who doubt the rumour will hear it again from their friends as a result. On the other side, the rumor's spreaders (both malicious and deluded) want to promote it and encourage others to believe it and circulate it. In order to convince the person who was first sceptical, a bigger group of friends would be brought in. People who doubted the rumours would be convinced to believe them and become propagandists for the rumour as the word spread.

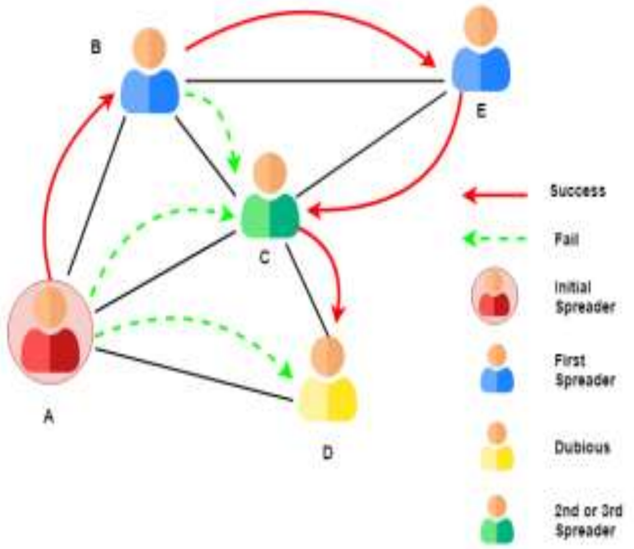

Fig -2: Rumor Iterative Spreading Process

As shown in Figure 2, malicious user A spread a rumour [1]. Users B and C heard the rumour, but they weren't convinced at first. User B's friends C and E then passed the rumour on to their friends D and F, who then passed it on to their friends. In this case, user C ignored it, while user E continued to pass it through to C. Finally, after hearing the rumours for the third time, User C decided to join the movement. User C sends a rumour to users D and E, who then share it to their friends. Except for user B, who became a spreader for the first time, every user became a spreader.

Distributed vs Centralize Architecture

Centralized software systems surround and link to a single central component. On the other hand, a distributed system is a collection of interconnected components with no central control or coordination centre.

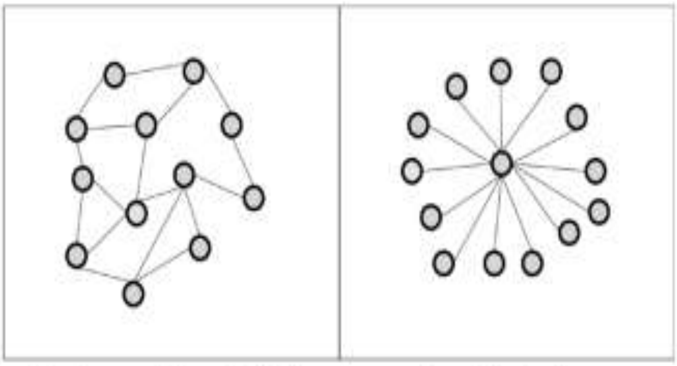

Fig -3: Distributed (left) vs. centralized (right) system architecture

Figure 3 illustrates these two opposing designs. The system's nodes and linkages are depicted in the diagram by the various circles and lines. A decentralised design is depicted in Figure 3. Keep in mind that no single part is interdependent with every other part. A must-know piece of information. It's important to remember that every part is interconnected in some way. Figure 3 on the right depicts a centralised architecture, in which each component is linked to a single central unit. The parts aren't connected in any way. They can only get to the core of the system by using one method.

3. REVIEW OF LITERATURE

To combat the growing problem of inaccurate information that makes it harder to discern the truth in any given piece of information, IEEE 2020 [6] examined the impact the Internet's power has had on disinformation. [6]. We need a device that can track news patterns and tell us whether or not something is true in order to find the remedy. The proposed method makes use of computer vision and hybrid models to detect fake news. This architecture significantly improved the performance of SVM classifiers. To put it simply, this hybrid model outperformed both RF and the Vector Support Operator.

Fake news in massive text datasets was detected using machine learning by Sharma et al. (IEEE 2019). Combining machine learning and natural language processing is the goal of this approach. It's a mix of the two. Even earlier studies in the exact same topic, which used a variety of methodologies, were factored into the design. Several tests were used to illustrate the fundamentals of various techniques for detecting fake news via the device. Taking into account the long-term consequences and difficulties of doing research in this subject is also a part of this study. "Fake Media," to use an everyday expression, is the broadcast of incorrect information to the public, whether intentionally or accidentally.

Jang et al. [10] have proposed a methodology to identify and evaluate bogus news sources. Studying how fake news spreads on social media was the goal of the researchers. An evolutionary tree modelling approach is used to look for internet-based fake news. In the suggested system, antecedent tweets and the origin of those tweets have been discovered. They also looked at how people decided whether or not a piece of news was fake. The findings showed that real news spread quickly and widely over the network, but fake material had to undergo a series of content modifications.

An interesting study in this area has just been published, authored by Qayyum et al [11]. Fake news is tackled in this article using a combination of deep learning and machine learning (ML). Other blockchain-based framework ideas for fighting fake news have also been proposed by the authors. There is a connection between fake news and blockchain research: [12]–[20]. Huckle and colleagues [21] developed a prototype for authenticating the origin of collected digital media. The authors proposed a technological method for detecting the reliability of media sources used in the dissemination of misleading news.

Blockchain technology was presented by Saad et al. [22] as a novel way to stop fake news from spreading on social media. There are many sources of news, and these sources may be manipulated by social media users, according to the authors. Because of its prototype work, fake news cannot spread on social networks. This study continues to employ the Saad et al. method, but adds bloXRoute and keyed-watermarking to increase network scalability and identify media tampering (as highlighted in the next section). The scope of the research has been expanded to include scenarios in which a regular social media user behaves as a media or news generator, which were not considered in the initial study.

Youngkyung Seo, Deokjin Seo, and Chang-Sung Jeong[11] presented a method for detecting fake news based on the credibility of the media. [12] Text-based analysis was utilised by Shivam B. Parikh and Pradeep K. Atrey to identify fraudulent news. As part of their research [14], researchers used an overlay-based cross-approval classifier and a vector space model to talk about fake news and unique stories in relation to recurrence terms, recurrence phrases, and recurrences turned around.

Kai Shu, Huan Liu, and Suhang Wang [15] fabricated the truth. For two different customer groups, they distributed two different sets of news (false and real). People who were knowledgeable about recognising fake news and those who were dumb enough to believe it were two distinct categories [16]. Each of these client groups was subjected to an identical inquiry, as evidenced by their confirmed and express profile details. Investigation found that they could discern the difference between true and fake news [18]. Machine Learning-based phoney news location techniques were tested on Facebook Messenger chatbots with an accuracy rate of 81.7 percent, which was obtained by combining news content and social context elements. [19].

Many blockchain-based methods have been developed by Wenqian Shang et al. (2018) to track and detect fake news. Source evaluation is used in a blockchain-based system [5] to ensure the integrity of the news article. Use of many nodes ensures that only genuine news stories are published online. You can use an online news reader to stay up-to-date on the latest developments with this approach. The header and body of a block defined by this system are separated by padding and padding, and the header contains the hash values of previous and current blocks. There is a block body that contains transaction information. Because they are linked, this chain of blocks can readily be used to determine the source of the news. The article's provenance can be verified using the blockchain network.

According to Wee Jing Tee et al. (2018) [6,] blockchain has the potential to solve a slew of pressing problems. Based on the conclusions in this article, blockchain and artificial intelligence (AI) are expected to advance in the next few years. Both of these technologies can be used to counteract the spread of false information. The paper examines how blockchain can be used to prevent the spread of incorrect information in great detail. Muhammad S. et al (2019) [7] improved on this prototype and developed a method for detecting, reducing and tracing bogus news. In the past, dummy blockchain systems advised retaining a blockchain for each social network member, which is not now possible in practise. There will be no need for social media users to maintain their own blockchains in order for this system to work correctly. It will be feasible to maintain the network with the support of news organisations and social media platforms. False information can be identified by the general population, and those responsible for disseminating it will be stopped. It has been possible to increase transactional throughput by using BFT consensus.

An entirely new architecture for authenticating transactions in a distributed social network is built on Software-Defined Vehicular Networks (SDVN) and Blockchain, according to Yahiatene and colleagues. Blockchain-based social networks can be used to combine fog computing and establish security architecture for controlling Internet of Things systems by creating tamper-proof digital identities within a trustless domain. Tweet-chain [16] is a blockchain-based addition to social media networks like Twitter and Facebook. Tweet-chain employs the Proof of Concept protocol [17] to manage public posts and assure the security of social transactions rather than depending on proof of labour. It is not required to make the trustworthiness assumption about the social network provider.

False news may be detected using the Fakechain [18] data mining techniques, which are also used for authenticating shared material on social media. It is possible to detect bogus news using the Breadth-First Search (BFS) algorithm with the Ethereum blockchain. [21]

Another poll found that David et al. presented a thorough explanation of how blockchain can be employed in modern information systems. The study says that various blockchain studies and applications, as well as their impact on blockchain and its deployment in other scenarios or applications, have been thoroughly evaluated according to the study. New members in today's dynamic global market must be able to adopt and produce blockchain technologies because of the structure of the blockchain and modern cloud and edge computing paradigms, according to this study.

False news can be identified by Arquam et al [5] by awarding credits and measuring the global and local levels of confidence that users have in it. According to Balouchestan et al. [7], false news can be detected using the blockchain, which contains three user profiles: reporters, analysts, and validaters. Reporters, raters, analysts, and validators of news can all be users. Rumors and fake news need to be analysed and managed. The Susceptible, Infectious, Recovered (SIR) model was further developed by Chen et al. [8]. Publishers could use Islam et al. [10] to collect news from reporters anonymously and without fear of compromising the data's integrity. [In their paper, Paul and colleagues [11] proposed using blockchains to detect fake news. By relying on the sources and publishers of news, Qayyum et al. [12] establish a news chain. It is possible for news organisations to publish false information. Shang et al. [13] proposed a system that included the original news chain in order to prevent news tainting. Publishers can do nothing to stop the spread of false information.

4. BLOCKCHAIN BACKGROUND

Blockchain

The blockchain is nothing more than a network of blocks. To describe a public database, use the words "block" and "chain" in the same sentence. There are blocks that store the most recent transaction's purchase price and the transaction date. Individuals that participated in these exchanges are also documented. Participants' Public Keys are used instead of their real names in this method. Fig-4 Instead of recycling data, blocks are uniquely identified by a hash code. A single block of data on the blockchain can hold up to 1 MB. You just need to click "Create" after you've navigated to a URL in your browser and entered your email address. App developers as well as other users gain from this. Decentralization is ensured, and personal information of users is safeguarded. The decentralised public ledger [21] is spread across nodes.

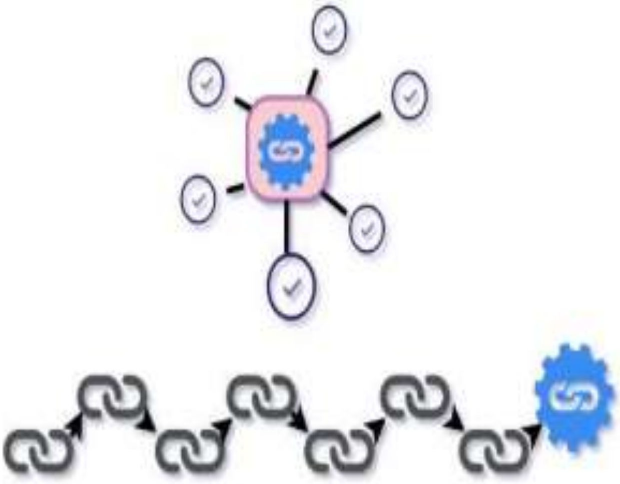

Fig. 4. Blockchain technology

Blockchain Architecture

The chain of connected and replicated data blocks that makes up the immutable peer-to-peer network known as the blockchain. [13] To make the blockchain safe, all network communications and updates are encrypted using public key encryption. The blockchain creates an unchangeable consensus using a decentralised system and encryption mechanisms.

Blockchains are distinct from central databases because of their lack of centralization. It is easier to trace the origins of data in a distributed database since each user has a copy of every record and alteration. Figure 5 depicts both an older third-party ledger and a more modern blockchain-based ledger (right). Most commonly, databases and ledgers are linked to a central ledger or a trusted third party. Even though each node has its own ledger, the central ledger serves as the master in this design. With the blockchain, each node has a duplicate ledger that is accessible to all other nodes in the network. There is no third-party trust required because all ledgers are synchronised and may communicate directly on the network.

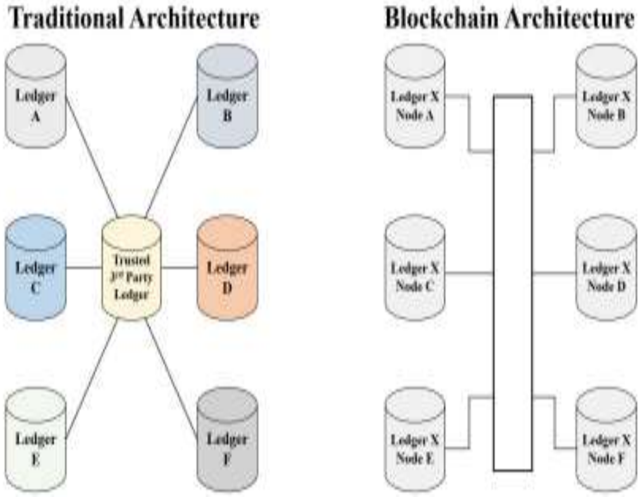

Fig. 5. Traditional vs blockchain architecture.

When it comes to attaining decentralisation and immutability in the blockchain, its unique design helps. Many businesses now make use of this technology because of its many advantages, including the capacity to share information among different parties while protecting the data's validity, secrecy, and long-term stability.

Working Procedure of Blockchain?

A blockchain is shown in Figure 6 as a series of linked blocks. In order to construct a new block, the hash of the previous block is merged with the hashed content of the current block and a timestamp. In this way, each following block is intertwined with the prior one.

When a chain is broken, a new, shorter blockchain is formed rather than a new, longer one (whose length is determined by which block is replaced). [15] Every non-interchangeable block will be thrown away (i.e., is no longer valid). A blockchain that is widely accepted will always have a place. To the maximum extent possible, nodes on a permissionless network or trusted nodes on a permissioned blockchain might be doing this. Consensus-based blockchains, on the other hand, will continue to operate in their current state. Changing the blockchain requires the consent of the majority of the system's nodes.

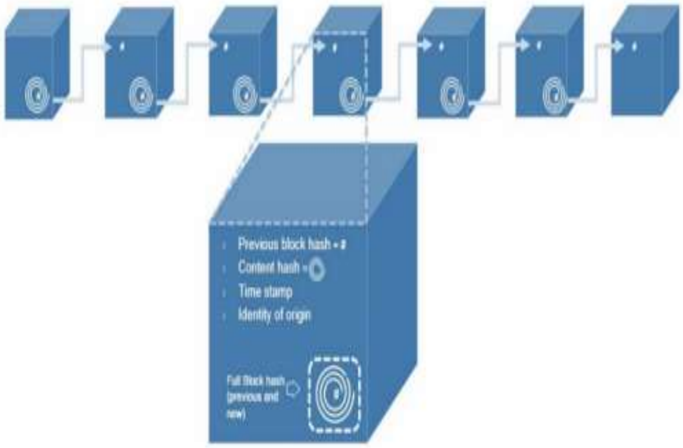

Fig. 6. Blockchaining.

Consensus Mechanism in Blockchain Networks

Blockchains rely on fault-tolerant consensus methods to keep the network's nodes aligned on a single state. Using these approaches, all nodes are kept in sync and all transactions are uploaded to the Blockchain. In order to verify that all transactions are legal and legitimate, it is their responsibility. Businesses and blockchain developers must be well-informed when choosing a consensus method for the blockchain.

When businesses and blockchain CEOs know what they want to achieve, they can work backwards from there to find a consensus mechanism that fits their goals exactly. So "mining" means building blocks that can be linked to a database, and so "mining." Since the network is able to verify blocks, nodes can create their own. As soon as a block is verified, it is added to the blockchain. The nodes that seek to construct blocks are known as mining nodes. As quickly as possible, you must validate transactions and produce new blocks if you want to receive the incentive. Consensus is achieved by a variety of processes, including PoS, Proof of Work (PoW), Proof of Interest (PoI), Proof of Space (PoSpace), and PBFT [15, 16].

5. CONCLUSION

Fake news was detected using a machine learning model built on top of a blockchain. The suggested system makes use of machine learning classification approaches that have been tested in the existing systems. Using a custom blockchain to process a module requires the least amount of time, according to our research. Although the system's framework is currently in place, it has yet to be put into action. Fake news detection and deletion will be the focus of our future research.

REFERANCE

- Ahuja, Nishtha, and Shailender Kumar. "S-HAN: Hierarchical Attention Networks with Stacked Gated Recurrent Unit for Fake News Detection." 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE, 2020.
- Ai, Songpu, et al. "Blockchain based Power Transaction Asynchronous Settlement System." 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring). IEEE, 2020.
- Antoun, Wissam, et al. "State of the Art Models for Fake News Detection Tasks." 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). IEEE, 2020.
- Akshay et al., “Fake News Detection,” IEEE International Students' Conference on Electrical, Electronics and Computer Sciences, 2018.
- G. Srivastava, S. Dhar, A. D. Dwivedi, and J. Crichigno, “Blockchain education,” in 2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019, Edmonton, AB, Canada, May 5-8, 2019. IEEE, 2019, pp. 1–5. [Online]. Available: https://doi.org/10.1109/CCECE.2019.8861828 .
- D. Dwivedi, “A scalable blockchain based digital rights management system,” IACR Cryptol. ePrint Arch., vol. 2019, p. 1217, 2019. [Online]. Available: https://eprint.iacr.org/2019/1217.
- M. Saad, A. Ahmad, and A. Mohaisen, “Fighting fake news propagation with blockchains,” in 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1–4.
- Q. Han, F. Miao and L. You, "Rumor Spreading Model Considering Iterative Spread on Social Networks," 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, 2018, pp. 1363-1367.
- M. Granik and V. Mesyura, "Fake news detection using naive Bayes classifier," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, 2017, pp. 900-903.
- S. Gilda, "Evaluating machine learning algorithms for fake news detection - IEEE Conference Publication," Ieeexplore.ieee.org, 2019.
- Dey, R. Rafi, S. Hasan, and S. Kundu, "Fake news pattern recognition using linguistic analysis," Dspace.bracu.ac.bd, 2019.
- H. Al-Ash and W. Wibowo, "Fake News Identification Characteristics Using Named Entity Recognition and Phrase Detection," Semanticscholar.org, 2019.