**A Literature Synthesis on spread of fake news**

**Abstract**

A dark side of social media is spreading fake news and propaganda with eye-catching captions or titles. Like every other digital innovation, social media has its ways of misuse like spreading fake news by which harm can be done to the society. It is very frequent due to open access of data. So, to identify and prevent misleading information in the digital platform has become a global issue. Social media is a complex network of users where any kind of data can be generated and propagated very easily in an unstructured and scattered nature. That’s why researchers are working very hard to find ways to automatically stop spreading misleading information from digital platforms. They have proposed several techniques like machine learning, neural networks, natural language processing, block-chain etc. and experimented them to classify and detect fake news, identify and trace news source, cross-match with original content, compare reviews by peers. Recent findings have shown promising results in their literature. In this report, a constructive review of those literature is presented with their promises, limitations along with the current research challenges.

**Introduction**

In this current era of modern technology, data is a powerful tool. Because of digital transmission, data can be generated and spread fast among the digital platforms. But as it is very frequent and fast, it became difficult to keep track of every bit of data, its source and authenticity. Also as the current generation is more relying on the internet and especially on social media, data is generating in a rapid and unstructured manner [(Kai Shu et al., 2017)](file:///C:\Users\Muiz%20Ahmed\Desktop\Xtra\Muiz\Block%20chain\Project%20Proposal.docx#r6). That’s why data integrity became a big question. News is a kind of data which also transmitted through the digital networks very frequently. Spreading fake news is one of the aspects of current society which is highly affected by unauthentic and fake data where internet and social media is playing a vital role.

Spreading of fake news essentially indicates manipulation of original content, misleading information, completely false or unsubstantial news which can highly impact society or any reputation [(Chengcheng Shao et al., 2017)](file:///C:\Users\Muiz%20Ahmed\Desktop\Xtra\Muiz\Block%20chain\Project%20Proposal.docx#r8). Social media is a virtual gathering of people where they can share ideas, information with each other (Leticia Bode, 2016). Spreading news is very easy in social media because anyone can share any kind of information of any forms such as text, audio, video etc. News can lose its authenticity in social media because it is now generating from uncountable sources. Literally, anyone can post a news and reach thousands of reader’s eye. And it is published without any verification most of the times.

Fake news can be identified as a social diseases. It is a really difficult job to distinguish between fake and real news. Even for humans. And that’s why it managed to attract global attention [(Antino Kim et al., 2019)](file:///C:\Users\Muiz%20Ahmed\Desktop\Xtra\Muiz\Block%20chain\Project%20Proposal.docx#r7) and mostly after US president election in 2016 (Hunt Allcott and Matthew Gentzkow, 2017). In recent years, many research methods using advanced technologies of automatically detecting fake news were established. Block-chain is one of the promising technologies proposed by several literature to prevent the spread of fake news on internet with its fundamental features. Machine Learning also showed promises in classifying fake news. Some literature proved to detect fake news from real-life digital data with hybrid models. Other researchers presented mathematical models (Kristina Lerman, 2007) to identify unauthentic news from the internet.

In this report, a broad review of recent literature is presented based on their strengths, weaknesses and possibilities along with current research challenges.

**Key Research Areas**

Focusing on the spread of fake news, researchers explored a few research areas to solve the problem by experimenting and implementing various technologies. In this section, two major research areas covered by the researchers is discussed.

**Machine Learning:** Machine learning itself is a broad domain of research with many techniques and methods. What a machine learning model does, is essentially learn from historical data, improve its predicting accuracy and then it can automatically predict on new data based on its knowledge. It requires historical data, also called as training data where the model learns from. Different machine learning models have shown good performance in classifying news articles, understanding their patterns and behavioral differences, tracking sources, context mining in form of linguistic cues, temporal analysis (Natali Ruchansky et al., 2017) etc. In machine learning approach, one of the few drawbacks, is the performance of the model is highly dependent on the availability and quality of dataset (Ray Oshikawa et al., 2018). And they usually require a large amount of well-organized and clean data to perform well. There are terms in order to evaluate a model such as overfitting when model performs very well in the training environment but performs poorly when it faces new or unseen data, and underfitting when model is not trained with sufficient data.

In order to overcome these problems, researchers used several techniques. Benchmark datasets are used to experiment the models such as Twitter, wiebo (Natali Ruchansky et al., 2017), Buzzfeed, LIAR (Shuo Yang, 2019) etc. A data repository is introduced called FakeNewsNet (Kai Shu et al., 2019) where multidimensional data is captured from news and social media context. Also preparation of dataset is important and many techniques are well-practiced such as data partitioning (e.g. train-test-validation, k-fold validation, cross-validation), data pre-processing (e.g. cleaning, tokenization, stemming, generalization, sampling). Authors have used different techniques to reduce overfitting problems such as dropout, regularization etc. And to evaluate their models they have presented performance comparison in different metrics (precision, recall, F1 score, accuracy) and graphical figures.

Supervised learning is one of the popular techniques to classify fake news.In supervised learning the model learns with knowing the targeted output. To classify fake news a few supervised learning algorithms are used such as Naïve Bayes Classifier, a probabilistic classifier based on Bayes Theorem (Mykhailo Granik and Volodymyr Mesyura, 2017), Logistic Regression, Support Vector Machine (SVM) (Kai Shu et al., 2019) etc. The problem of supervised learning is, the training data must be labeled with the targeted output. Dataset must be constructed with original and fake news and they should be labeled properly. The model is going to perform based on the labels of training data.

Other techniques such as anomaly detection, clustering, generative approaches are also proposed by many literature. They are mostly unsupervised, meaning the classified labels are not defined when the model is trained. Algorithms try predict the similarity or difference in their patterns and behavior, then separate into different categories. Clustering can make collections of similar data and that’s how unnatural or irregular data can be found. Fake news can be generated from a common source, or unknown, unfamiliar source which can be identified by these algorithms.

Natural language processing has many techniques. Recently Neural Network has showed brilliant results by trying to mimic how human brain works. In news data, it is really important to understand the temporal meaning or connection of each segment of the data because data is usually large and sequential. That’s why natural language is one of the most exciting techniques in machine learning domain. Recurrent Neural Networks, Long-Short-Term-Memory (LSTMs) are very popular algorithms with sequential data like text, audio and video. Convolutional Neural Networks can be used to identify social structure and propagation of the news which is important factors of spreading fake news (Federico Monti et al., 2019). But the drawbacks of these architectures, they are usually very complex models with a lot of learning parameters. And of course, a large dataset is needed. Which makes the model very expensive in terms of processing or learning. That’s why to perform these operations, high configured machines are required.

Authors also proposed hybrid models with multiple machine learning algorithms. Three different modules were shown in order to extract temporal representation, capture the source characteristics and integrate these two to classify the news as fake or original article (Natali Ruchansky et al., 2017). Because of literacy and cognitive limitations of machine-based approach, a solution is proposed to combine human interventions to find the truthfulness of data and reliability of source (E. M. Okoro, 2018).

* **Block-chain:**  Block-chain is still an emerging technology and growing its dominance over various domains. Block chain technology is a distributed data storage, which uses features like distributed ledger, decentralized peer-to-peer networks, and cryptography. In simple words, block-chain is a collection of blocks of information. A block consists of header which contains cryptographic hash of its previous block’s header, timestamp, cryptographic hash of its body content etc. and body containing the data. Since the block header contains the hash value of the previous block header, the information in each block changes, and the subsequent block changes accordingly. That’s how block-chain ensures tamper-proof, forgery and traceability of information in the process of information collection, transfer and sharing (Wenqian Shang et al., 2018).

In decentralized networks all the peers are connected to each other. Data is stored and validated in every nodes (Zonyin Shae and Jeffrey J P Tsai, 2019). That’s why data has transparency and authenticity in a block-chain. And as it stores data in blocks and they are cryptographically connected to each other, authors showed traditional data tracing technology to extract and evaluate source of the news. This feature is likely very much applicable to social media because it has uncountable nodes (Mohammad Torky et at., 2019). Creating a peer-to-peer secure platform for storing and exchanging information can combat against digital deception (Paula Fraga-Lamas and Tiago M. Fernández-Caramés, 2019)

There are different cryptographic techniques such as public-key cryptography, cryptographic functions, digital signature (Steve Huckle and Martin White, 2017). In public-key cryptography, data is hashed with a private key by which it can be decrypted. The private key belongs only to the owner of the data. It can protect original content of news from any alteration when propagating through internet. Cryptographic functions essentially means mathematically create a hash string based on the data. It is a unidirectional function (Adnan Qayyum et al., 2019). For creating the hash, a popular algorithm is used called SHA256 which produces 256-bit hash. By using cryptography, digital signatures can be generated. This provides data privacy, ownership and authenticity.

Researchers also incorporates Artificial Intelligence (AI) and block-chain in order verify and prevent fake news from social media (Tee Wee Jing and Raja Kumar Murugesan, 2019). AI used for fact-checking for a deeper linguistic comparison of differing types of fake news e.g. satire, propaganda etc.

Cryptographic mining of block-chain requires extensive computational power. That’s why, to encrypt all news on the internet is a very challenging task. Also the rate of illegal mining by hackers (like bit-coin mining) can be increased.

**Key Research Challenges**

Preventing the spread of fake news raised research challenges. Researchers are well identified and improving their methods to get rid of those challenges. A few of those research are pointed in this section.

* Availability, size and quality of data to train machine learning models.
* Predefined data with specific content and timeframe is not good to train machine learning model because news data is universal and generating every day.
* Identify authentic source.
* Extensive computational power requires for some machine learning and block-chain technologies.

**Conclusion**

Due to random use of internet and social media, data or news is generated and propagated very fast. And it is now going beyond human’s ability to keep track of authenticity and integrity. That’s why automatic prevention of fake news is a demanding topic in research. Though no benchmark tool has introduced yet but advanced technologies like machine learning and block-chain are showing promising results. There is possibility in future.

**References**

Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang and Huan Liu. 2017. Fake News Detection on Social

Media: A Data Mining Perspective. In *ACM SIGKDD Explorations Newsletter, Volume 19.*

Chengcheng Shao, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, and Filippo

Menczer. 2017. The spread of fake news by social bots. In *Nature Communications.*

Leticia Bode. 2016. Political News in the News Feed: Learning Politics from Social Media. In *Journal of*

*Mass Communication and Society, Vol 19, Issue 1.*

Antino Kim, Patricia L. Moravec and Alan R. Dennis. 2019. Combating Fake News on Social Media

with Source Ratings: The Effects of User and Expert Reputation Ratings. In *Journal of Management Information Systems, Volume 36*, Pages 931-968.

Hunt Allcott and Matthew Gentzkow. 2017. Social Media and Fake News in the 2016 Election. In *Journal*

*of Economic Perspectives, Vol, 31, No.2.*

Kristina Lerman. 2007. Social Information Processing in News Aggregation. In *IEEE Internet Computing.*

Natali Ruchansky, Sungyong Seo and Yan Liu. 2017. CSI: A Hybrid Deep Model for Fake News

Detection. In *ACM on Conference on Information and Knowledge Management*.

Ray Oshikawa, Jing Qian and William Yang Wang. 2018. A Survey on Natural Language Processing for

Fake News Detection. Available Online at: [*https://arxiv.org/abs/1811.00770*](https://arxiv.org/abs/1811.00770)

Shuo Yang, Kai Shu, Suhang Wang, Renjie Gu, Fan Wu and Huan Liu. 2019. Unsupervised Fake News

Detection on Social Media: A Generative Approach. In *Proceedings of the AAAI Conference on Artificial Intelligence.*

Federico Monti, Fabrizio Frasca, Davide Eynard, Damon Mannion and Michael M. Bronstein. 2019. Fake

News Detection on Social Media using Geometric Deep Learning. Available Online at: [*https://arxiv.org/abs/*](https://arxiv.org/abs/)*1902.06673*

Kai Shu, Deepak Mahudeswaran, Suhang Wang, Dongwon Lee and Huan Liu. 2019. FakeNewsNet: A Data

Repository with News Content, Social Context and Spatialtemporal Information for Studying Fake News on Social Media. Available Online at: [*https://arxiv.org/abs/1809.01286*](https://arxiv.org/abs/1811.00770)

Mykhailo Granik and Volodymyr Mesyura. 2017. Fake news detection using naive Bayes classifier. In

*IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON).*

E. M. Okoro, B. A. Abara, A. O. Umagba, A. A. Ajonye and Z. S. Isa. 2018. A hybrid approach to fake

news detection on social media. In *Nigerian Journal of Technology, Vol 37, No 2.*

Wenqian Shang, Mengyu Liu, Weiguo Lin and Minzheng Jia. 2018. Tracing the Source of News

Based on Blockchain. In *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS 2018).*

Steve Huckle and Martin White. 2017. Fake News: A Technological Approach to Proving the Origins

of Content, Using Blockchains. In *Big Data, volume 5,* pages 356-371.

Zonyin Shae and Jeffrey J P Tsai. 2019. AI Blockchain Platform for Trusting News. In *IEEE 39th*

*International Conference on Distributed Computing Systems (ICDCS).*

Tee Wee Jing and Raja Kumar Murugesan. 2019. A Theoretical Framework to Build Trust and

Prevent Fake News in Social Media Using Blockchain. In *International Conference of Reliable Information and Communication Technology*, pages 955-962.

Mohamed Torky, Emad Nabil and Wael Said. 2019. Proof of Credibility: A Blockchain Approach for

Detecting and Blocking Fake News in Social Networks. In *International Journal of Advanced* *Computer Science and Applications,* pages 321-327.

Paula Fraga-Lamas and Tiago M. Fernández-Caramés. 2019. Fake News, Disinformation, and Deepfakes:

Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. Available Online at: [*https://arxiv.org/abs/1811.00770*](https://arxiv.org/abs/1811.00770)

Adnan Qayyum, Muhammad Umar Janjua, Junaid Qadir and Falak Sher. 2019. Using Blockchain to

Rein in the New Post-Truth World and Check the Spread of Fake News. In *IT Professional volume 21,* pages 16-24.