Social Media Governance and Fake News Detection Integrated with Artificial Intelligence Governance

Bhavani Thuraisingham and Teena Thomas
Erik Jonsson School of Engineering and Computer Science,
The University of Texas at Dallas
Bhavani.thuraisingham@utdallas.edu
Tmt160030@utdallas.edu

***ABSTRACT*—Social Media Systems such as Facebook, Instagram, and Twitter (i.e., X) are exploding. These systems need proper governance so that the users are safe and post accurate information. This paper focuses on social media governance with an emphasis on Artificial Intelligence. First, we discuss various aspects of governance of such policies, procedures and risk and then address a key topic which is detecting fake news on social media. In order for the users to be safe using social media we have to ensure that the governance aspects also include fake news detection. Many of the fake news detection techniques utilize Machine Learning (ML) and Artificial Intelligence (AI) and more recently Generative AI (GenAI) techniques. Therefore, the AI systems that implement the various techniques have to be trustworthy. That means these systems have to be secure as well as ensure fairness, privacy and integrity. Therefore, the paper will also discuss AI Governance as an integral part of Social Media Governance. Finally, to support the various applications and frameworks, both data and the cloud are critical. Large amounts of data are stored and managed by the social media systems as well as used to train the AI models. Furthermore, we need massive amounts of computing power that can be provided by the cloud. Therefore, we will also discuss data and cloud governance that provides the infrastructure for social media and AI governance.**

Keywords: Social Media Governance, Fake News Detection, Machine Learning, Artificial Intelligence Governance, Security, Privacy, Fairness, Integrity.

I. INTRODUCTION

Social media Systems now have billions of users. In order to protect the users and the information they post, it is vital that such systems are governed properly. This means appropriate policies have to be enforced and the procedures set in place for the governance of social media systems. One of the major aspects of Social Media Governance is Fake News Detection. The existence of fake news and false information has been around since the dawn of time. As with the growth of multiple user digital environments and modern day journalism, fake news has crossed new horizons. Detecting fake news in today's society has become a problem that researchers around the world hope to resolve. One of the objectives of our work is to provide an insight about the characterization of fake news as well as its impact on readers. This paper will also provide an overview of our work including some of the existing fake news detection approaches, challenges, as well as some of the popular fake news datasets.

While exploring fake news detection, we have also written a series of papers on computing systems governance. These include Cyber Security Governance [1], Cloud Governance [2], and Data and AI Governance [3]. At the same time, we have carried out extensive research on social media analytics and security [4]. In this paper we integrate our prior work on both social media and cyber systems governance and discuss social media system governance. The discussion also includes governance with respect to fake news detection. AI/ML plays a critical role in solving challenging problems in cyber security, social media, and fake news detection. However, these AI systems also have to be trustworthy. Furthermore, governance aspects of these AI systems have to be revisited within the context of social media. Therefore, this paper will also address aspects of AI governance extending the work discussed in [3].

Finally, for social media governance and AI governance to be effective we need data and the cloud, That is, massive amounts of data are generated by the social media systems. Data is also needed to train the AI models. Such data has to be managed effectively. High performance computing is also a necessity for handling massive amounts of data. One such system that is being is used is the cloud. Therefore, cloud and data governance are critical aspects for fake news detection and related applications. Therefore, we also revisit our prior work on data and cloud governance within the context of social media and AI governance.

The paper is organized as follow. In section 2, we discuss social media governance. In section 3 we discuss Fake news Detection. AI Governance will be discussed in Section 4. A note on Data and Cloud governance will be discussed in Section 5. The paper is concluded in Section 6.

II. SOCIAL MEDIA GOVERNANCE

In order to ensure that the social media systems enforce proper governance rules, first we need to analyze the impact of social media with respect to various aspects of computer

2835-5776/24/$31.00 ©2024 IEEE
DOI 10.1109/IRI62200.2024.00048

systems governance as discussed in [5]. These include: (i) Security Management, Administration and Governance, (ii) Policies, Standards, Guidelines, Procedures, (iii) Risk Management and Analysis, (iv) Roles and Responsibilities, (v) Best Practices, (vi) Information Classification, and (vii) Information Accuracy (Fake news, false information, disinformation, misinformation). We will discuss some of the key aspects with respect to the above topics and then pose questions for social media governance. It should be noted that much of the information about computing systems governance has been obtained from [5] and [15]. We need to examine the impact of social media on the various aspects of system governance.

Security Management, Administration and Governance: First, as discussed in [5] and [15], information security describes activities related to protecting information, information assets and infrastructures against threats and attacks. These threats could be malicious or due to catastrophic situations. Information security management describes controls that an organization must put in place to minimize the risks to the damage to the assets due to the attacks. As stated in [5] and [15] risks to these assets can be calculated by analysis of the following aspects:

- *Threats to your assets*: These are unwanted and/or malicious events that could cause damage or harm to the assets
- *Vulnerabilities*: This is the susceptibility of the assets to the threats and attacks.
- *Impact*: The magnitude of the potential loss to the asset due to the attack.

The question with respect to Social Media security administration is, what are the risks to social media systems? What are the vulnerabilities? What are the threats to the assets in a social media system (e.g., data), and what is the impact?

Standards that are available to assist organizations implement the appropriate programs and controls to mitigate risks include BS7799/ISO 17799, Information Technology Infrastructure Library (ITIL) and COBIT. Information Security Governance is a subset of Corporate Governance focused on Information Security systems and their performance and risk management. We need to establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with various regulations and laws that are relevant. The question we are interested in is, what is the impact of Social Media systems security on the Frameworks developed for information security governance? Do we need new kinds of frameworks? Also, how can the existing frameworks be extended? What are the relevant laws and regulations for social media systems that impact their governance?

As we have stressed in our earlier governance papers, we need to do the following for social media systems security governance.

- Develop the information security strategy for the social media systems supporting business strategy and directions.
- Obtain senior management commitment for the activities to securing the social media system.
- Ensure that definitions of roles and responsibilities throughout the organization (both the social media companies and also the companies that use social media) include information security governance activities.
- Establish reporting and communication channels supporting information security governance activities for social media systems.
- Identify various legal and regulatory issues affecting information security and assess their impact on the enterprise and the social media systems.
- Establish and maintain information security policies that support business goals and objectives that pertain to the social media systems.
- Ensure the development of procedures and guidelines that support information security policies for social media systems.
- Develop business case for information security program investments for securing social media systems (that also includes privacy).

All of the above have to be explained with Social Media systems in mind. For example, how can social media systems security be aligned with the company's business strategy? What are the legal and regulatory requirements for developing a strategy for social media security? These are some of the questions that need to be answered.

Policies: One major aspect that needs to be addressed is policy specification and implementation. Policies are high level documents/statements including for security. These high-level documents provide statements about the organization's assets and what level of protection they should have. For example, employee compensation data can only be accessed by the human resources department. Standards are tactical documents because they describe specific steps or processes required to meet a certain requirement. Standards do not specify how the various concepts are implemented. A guideline is a recommendation or suggestion of how things should be done. For example, three factor authentication is recommended but not mandatory. A procedure is a detailed step-by-step document that describes exactly what is to be done. This could be an implementation of a protocol. A question that needs to be answered is: What are the appropriate policies, standards, guidelines, and procedures for social media systems?

Risk: Risk is the likelihood that something bad will happen that causes harm or loss to an information asset. For example, what is the likelihood that the data posted by a social media user is corrupted? A vulnerability is a weakness that could be used to endanger or cause harm to an information asset. For example, does the social media system have a loophole that could be used to corrupt the data? A threat is anything (man-made or act of nature) that has the potential to cause harm. For example, can a malware enter the social media system? The likelihood that a threat will use a vulnerability to cause harm creates a risk. For example, what is the likelihood that the malware will exploit the loophole to corrupt the data and cause harm? When a threat does use a vulnerability to inflict harm, it has an impact. It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risks. The remaining risk is called the residual risk. We need to carry out a detailed analysis of the risks involved for social media systems and determine who is responsible to conducting risk analysis. Should the corporation that uses the social media systems carry out the risk analysis or should it be carried out jointly with the social media companies? If there is a vulnerability say in the Facebook or Twitter system and the company that uses the social media system is compromised, then who is responsible for the damage that results from the attack? Is it the company utilizing the social media system or is it the social media company?

Roles and Responsibilities: The question is, what is the responsibility of the various stakeholders in the governance of social media systems. With respect to the Social Media Companies, who decides the policies for Facebook or Twitter? Who decides how the social media system is governed properly? With respect to the organizations that have a social media presence, who in the organization is responsible for social media governance? Should there be a Chief Social Media Officer (CSMO)? Should this officer report to the CEO (Chief Executive Officer) or to the CMO (Chief Marketing Officer) or even the Chief Communication Officer (CCO)? With respect to social media users, should the users be allowed to post whatever information they want? How do you handle the balance between Free speech vs Offensive messages and even False messages?

Information Classification: It is essential to classify information according to its actual value and level of sensitivity in order to deploy the appropriate level of security solutions Information could be Private/Public or Secret/Unclassified, etc. How can information be classified in Social Media? Is everything public? Who determines this? Should we focus on developing multilevel secure social media systems to handle different security levels?

Best Practices: Usually best practices include Job rotation (move to different jobs within an organization), Job sharing (share a job within an organization). The questions are: What is the equivalent in social media? Social media companies could implement job rotation and job sharing. An organization can also implement such best practices. But it may not be a good idea to change say the Chief Social Media Officer or other key personnel every few months

Information Accuracy: Finally, the accuracy of the information posted is critical as incorrect information could lead to disastrous situations. This topic has received a lot of attention over the past eight years. Inaccurate information could result due to user errors or malicious corruption through malware or through disinformation and misinformation. We focus on information that is not true; which means information that is false. We also focus on false information due to malicious intent. This has come to be known as fake news. Because of the importance of fake news detection in social media governance, we will discuss this topic in Section 3. The work in section 3 resulted from a term paper for a class activity (Analyzing and Securing Social Media) by one of the co-authors of this paper and is cited in [7].

III FAKE NEWS DETECTION

III.1 The Problem

The topic of fake news has become more prevalent over the years, due to the growth of multiple user digital environments and modern day journalism. Fake news and false information are two commonly used words in today's society. Although the two terms seem to be synonyms of each other they actually mean two different things. Fake news information is the deliberate spread of misleading information/propaganda/hoaxes by means of online social media, traditional news media. False information is inaccurate information it may or may not have malicious intent.

There are billions of people using social media; in addition to that there are also millions (if not billions by now) of robots/bots amongst the real-human users. These bots also play a significant role in propagating fake news and boost the popularity of fake news on social media platforms. The bots do so by mimicking a legitimate user's behaviors so that others would believe them to be credible legitimate users. Once the bots establish this trust, the task of spreading false news is quite simple. Fake news aims to convince readers of the validity of content which is not true.

There are two key factors associated with fake news: title of the news and the cover image of the news. The creators of the fake news put great efforts into creating catchy headlines, in order to lure the readers into clicking and reading their content. Studies have shown that 70% of Facebook users skim through the headlines before deciding to read or share the content. The individuals who are unaware of the side story or the overall context of the news would most likely fall into the trap of fake news and not bother to check the validity of the news. The creators of the

fake news also put great efforts into fabricating the cover images of the news. There are many people, even in today's society, who take to heart "seeing is believing." What these individuals are missing is the whole idea of fabricated and photo shopped images. Furthermore, with the explosion of the advancement in AI technologies, the so called "deep fake" text, images, audio, and videos (that is, essentially multimedia fabrication) have become dangerous to society. Fake news creators will use their best tools and tricks into fooling the eyes. As a result of today's news being a combination of text and images, it is difficult to detect which is fake. Furthermore, with the growth of many social media platforms, the reachability and impact of fake news is extremely high.

Fake news on social media is essentially like a wildfire, once there is a spark, the news will spread uncontrollably, until it is detected and stopped; yet the damage will still be evident. As with the slow yet eventual death of traditional printed media, comes the rise of news through non-traditional digital/social media. Social media account essentially allows each account holder to be news journalist, editors, and writers. There is a caveat to this empowerment; the credibility of the news may be at risk. There may be many individuals who claim to be legitimate and credible individuals but they may be fake. Over the years researchers have been trying to produce tools which could help the readers in determining the legitimacy of the content as well as derive the type of content it is.

Fake news detection has been studied extensively in recent years [6]. Huan Liu and his team at the Arizona State University have pioneered techniques to address the challenges. They have also grouped information into different categories including disinformation and misinformation. Our discussion on this topic has been influenced by the work reported in [6]. Various surveys of fake news detection have also been published [10]. In addition we also prepared a paper for a course project that provided some key issues that needed to be addressed [7]. In this paper we summarize some of the key points on this topic and then provide an analysis.

III.2 Types of News

There are mainly three categories of news sources: standalone websites, social media, emails, broadcast networks, and radio service. Standalone websites are websites which are free and are independent from proprietary codes, systems, and other solutions. Within standalone websites themselves, there are three main types of news sites: popular news sites, blog sites, and media sites. The popular news sites are websites which have certain standards and are considered to be more reputable sources of content. Blog sites, due to its unsupervised nature, are a source of less authentic content. Lastly, the media sites are based on user-based content creation.

The social media category consists of the use of various social media networks as means of circulating the content. Emails are a distributed way of sending messages by means of the web. Broadcast networks are also known as Podcasts and this medium makes use of audio multimedia. Lastly, the radio service or radio talks are yet another popular source of news content. The four major types of format in which news is presented to the audience is through: text, multimedia, hyperlinks or embedded content, and audio. Based on previous research studies, there are multiple major categories of fake news that includes: visual-based (graphical representation), user-based, network-based knowledge-based, style-based, and stance-based [7].

III.3 Fake News Detection Methods

Various types of fake news detection methods have been discussed in the literature [6]. In this section we will discuss some of them.

Linguistic Features based Methods Linguistic feature methods are which make use of extracting key linguistic features from fake news. Such methods/ approaches include Ngram (in Ngram, unigram and bigrams which are extracted from a collections of words), punctuation (This approach collects different types of punctuation in order to differentiate between legitimate and illegitimate news), psycho-linguistic features (this approach allows for the determination of the tone of the language used within the news), readability (this approach allows for the extraction of content features such as the number of syllables, the types of words, the number of paragraphs, etc..), and syntax (this technique allows for the extraction of features which heavily rely on lexicalized production rules). Linguistic feature based methods are also referred to as grammar engineering as they try to simulate the human parsing of words/linguistic structure. The benefits of Linguistic feature based methods is that they work very well for handling short sentences or messages because grammar rules can help decode the meanings of the sentences. The drawback is that there needs to be the intervention of human expertise in addition to the algorithms.

A. **Deception Modeling based Methods** The deception modeling methods rely on theoretical approaches in order to decipher between legitimate and illegitimate news. There process of clustering legitimate and illegitimate news relies two main theoretical techniques:

- **RST:** As stated in [8], "*RST procedural analysis captures the logic of a story in terms of functional relations among different meaningful text units and describes a hierarchical structure for each story's theory uses rhetorical connections to systematically identify emphasized parts of text*."
- **VSM:** As stated in [8], "*VSM is used to identify rhetorical structure relations in RST resulted sets. VSM interprets every news text as vectors in high*

dimensional space, this requires the extracted text to be modeled in a suitable manner for the application of various computational algorithms."

The combination of the above two techniques, the RST-VSM provides a best of both worlds technique. The RST-VSM allows for a better curation of data and performs better than similarity cluster analysis.

Predictive Modeling based Methods The predictive modeling approach is based on a logistic regression model. According to this approach, negative coefficients increase the probability of deception while the positive coefficients increase the probability of legitimacy. As discussed in [8], according to an academic study, "*Clustering and Predictive Modeling has a success rate of 63% and 70%, respectively. However, the Predictive Modeling approach shows real promise to perform instant fake detection, machine learning techniques can be used to improve the coefficients in ongoing ways*."

Content Cues based Method Many of the fake news creators make use of the idea of what the readers want to read. As a result, the content cues based methods make use of what the fake news creator writes about as well as what the readers want to read about. The content cues based method make user of two different types of analysis:

- **Lexical and Semantic Levels of Analysis:** Automated methods are put to use in order to extract stylistic features from the textual content. This is because many fake news creators make use of many stylistic features in order to try to convince the readers of the legitimacy of the content they are creating.
- **Syntactic and Pragmatic Levels of Analysis:** In order to lure the readers into reading the news content, fake news creators would often employ pragmatic headlines which in turn invokes references to the impending news content. Syntactic and pragmatic levels of analysis also aim to measure which news sites have more content being shared when compared with other news sites which have more new content being produced.
- **Non-Text Cues based Methods** In order to lure readers into reading content on the web, the non-textual content is just as import as the textual content. The aim of non-text cues is to convince the reader of the validity of the image and try to persuade the reader of the importance of the content of the news story. There are primary two different analyses which are put to use for this method
- **Image Analysis:** This strategy focuses on analyzing digital image multimedia. Image analysis can be simple as reading image tags or as complex as identifying individuals based on their faces. The information can then be used for pattern recognition or other forms of analysis.
- **User Behavior Analysis:** This strategy aims to find patterns in users' behaviors and then apply algorithms and other statistical analysis to find any irregularities within the patterns.

III.4 Analysis

There is not a "one size fits all" solution for the detection of fake news. In essence there are two ways of detecting fake news online by means of linguistic cues and by means of non-linguistic cues or network approaches. As stated in [9], "*Essentially, Linguistic Cue approaches detect fake news by catching the information manipulators in the writing style of the news content. The main methods that have been implemented under the Linguistic Cue approaches are Data Representation, Deep Syntax, Semantic Analysis, and Sentiment Analysis*." As stated in [11], "*Network Approaches in which network information, such as message metadata or structured knowledge network queries can be harnessed to provide aggregate deception measures. Both forms typically incorporate machine learning techniques for training classifiers to suit the analysis*" There is still research being conducted in order to derive a potential "one size fits all" solution for this issue.

Fake news aims to convince readers of the validity of content which is not true. The creators of the fake news put great efforts into creating catchy headlines along with intriguing multimedia content, in order to lure the readers into clicking and reading their content. The existence of fake news and its rapid spread is something that cannot be eradicated as long as human civilization exists. Nonetheless there are many ways to detect and attempt to stop its spread. Detecting fake news in today's society has become a chronic issue which researchers hope to fully resolve one day. The purpose of this paper is to provide an insight about the characterization of fake news as well as its impact on readers. This paper will also provide an overview of some of the existing fake news detection approaches, challenges, as well as some of the popular fake news datasets. The methods described in this paper are not independent and may be used jointly. This helps in combining the strengths of each approach. For example "A support vector machine (SVM), which can be used interchangeably with a support vector network (SVN), is also considered to be a supervised learning algorithm. SVMs work by being trained with specific data already organized into two different categories. Hence, the model is constructed after it has already been trained."

Unfortunately, SVMs do not work with large datasets since their training time may be high. On the other hand "Naïve Bayes is a type of classifier considered to be a supervised learning algorithm, which belongs to the Machine Language

class and works by predicting "membership probabilities" for each individual class, for instance, the likelihood that the given evidence, or record, belongs to a certain class [12]. The biggest drawback of this approach is that all the features are to be separate and this may not always be the case. One proposed method is the hybrid algorithm that effectively minimized false positives as well as maximize balance detection rates (as stated in [9]). This algorithm and performed slightly better than SVM and Naïve Bayes classifier did individually. Even though thein the paper experiment was applied to Intrusion Detection Systems (IDS), it demonstrated that combining the two methods would be reasonably effective.

In summary, Machine learning techniques are being applied extensively for Fake News Detection. We can expect social media companies to use Large Language Models-based systems (e.g., ChatGPT) to detect fake news. We have applied such models for hate speech detection [16]. This is a critical areas and needs extensive research with respect to Social media Governance. But the challenge we have is that the AI systems that are vital for detecting fake news have to be governed. That is, the AI systems have to be trustworthy and need to ensure security, privacy, and fairness. In addition, we need to trust the results produced by the AI systems including the GenAI and the Machine Learning Tools. Therefore, we revisit AI Governance that we have discussed in [3] and extend some of the ideas and strategies that we have proposed with social media in mind.

IV ARTIFICIAL INTELLIGENCE GOVERNANCE

IV.1 Need for AI Governance

As stated in [3], Artificial Intelligence (AI) is affecting every aspect of our lives from healthcare to finance to transportation [17]. Sophisticated machine learning techniques with a focus on deep learning. And more recently the GenAI systems are being applied successfully from detecting serious illnesses to making optimum financial investments, to determining the weather patterns, as well as to ensuring the safety of autonomous vehicles. We expect AI to have even more influence as advances are made with technology as well as in learning, planning, reasoning, and explainable systems. Furthermore, with the advancement of generative AI techniques, we can expect AI to infiltrate in every aspect of our lives. This means the AI systems have to be secure, ensure privacy, and be fair to all. To ensure this we need appropriate governance frameworks for AI systems as well as approaches for carrying out risk analysis and well as criteria for evaluating, verifying, and accrediting such systems. The AI Strategy also has to be integrated with the corporation's business strategies. In addition we have stressed the need for a Chief AI Officer (CAIO) in our previous article [3].

There are some efforts that have been reported on Governance. Notable among them is Google's report on this subject [13]. For example, Google has examined the following areas that are part of AI Governance that advance the legal and ethical aspects of AI. 1. Explainability standards 2. Fairness appraisal 3. Safety considerations, 4. Human-AI collaboration, and 5. Liability frameworks. Additional areas that we included in our work in [3] include Accountability and Transparency. Organizations must examine these areas and produce an AI strategy that best suits their business needs and at the same time meets the fairness and other aspects discussed in the Google report. In Section 4.2. we will summarize some of the discussions in [3].

IV.2 Towards Developing an AI Governance Framework

We need to explore the governance aspects discussed in Section 2 for AI systems. These aspects include policies and procedures, threats, attacks, and solutions as well as risk analysis. Our discussion has been influenced by the discussions in [5] and [15]. Below are some of the key issues that need to be investigated further to develop an AI Governance Framework

Protecting AI against cyber-attacks and Privacy violations: This should be an extremely high priority for every organization and should be considered as important as showing profits to the shareholders. Has the company developed appropriate protection and detection methods for the cyber-attacks of the AI Techniques? Is it possible for the ML algorithms to analyze the vast amounts of data and subsequently violate the privacy of the individuals? Are appropriate cyber security and privacy measures being adopted so that the AI techniques are trustworthy?

Risk and Insurance: AS discussed in [3], before developing AI techniques and incorporating them to the areas such as product development and manufacturing, the company has to carry out an in-depth risk analysis. If there are no risks that the AI techniques will be unfair and untrustworthy, then we have a perfect situation, However, in the real-world people have biases and there is a lot of unfairness and discrimination. These biases can be transferred into the AI techniques. Therefore, it is important for the corporation to carry out a thorough risk analysis and take out AI insurance so that the company is not sued for unfair practices resulting from the AI techniques. Based on the risk analysis carried out, the company can then develop an AI strategy that address areas such as. 1. Explainability standards 2. Fairness appraisal 3. Safety considerations 4. Human-AI collaboration, 5. Liability frameworks, 6. Accountability, and 7. Transparency.

Evaluation, Certification, Accreditation and Standards: One of the success stories of the cyber security field is the operations of evaluation, certification, and accreditation of the secure systems. The first set of criteria for evaluating

secure systems was published in the early 1980s (called the Orange Book) [14] for the Department of Defense; and now we have the Common Criteria that is used to evaluate systems around the world. Once the systems are evaluated, then they are certified for use and then accredited by management. We need a similar approach for AI Systems. That is, we need criteria for evaluating them and subsequently certifying them for use and then accrediting them. This way the systems can be evaluated for security, privacy, explainability, fairness, bias, and other criteria. Also related are the development of standards for AI Systems. We need efforts in this area and NIST, together with other agencies, is in an excellent position to develop criteria as well as standards.

Integration with Social Media Governance with AI Governance: We are proposing two frameworks; one is the Social Media Governance Framework and the other is the AI Governance Framework. First, the social media system must conform to the social media governance framework. Whenever fake news is suspected and AI techniques are applied to detect the fake news, then these AI techniques must adhere to the policies and procedures enforced by the AI framework. That is, the two governance frameworks are closely intertwined.

V DATA AND CLOUD GOVERNANCE

Our previous papers have addressed both data and cloud governance [2], [3]. Social media systems need to manage large amounts of data. Such data can also be used to train the AI models for fake news detection as well as for other applications. Furthermore, we need massive computing power such as the cloud to process the data. Therefore, this section briefly discusses the issues related to data governance and cloud governance. Some useful information on these topics are discussed in [18] and [19].

With respect to data governance, a challenge is to develop a data lifecycle framework. This includes activities such as data collection, data storage, data manipulation, data analytics and data sharing [20]. Policies have to guide every step of the way. Furthermore, quality of the data also has to be maintained. Some related questions include where did the data come from? What is the provenance of the data? Who is responsible within an organization for the data? Should there be a Chief Data Officer (CDO) or is his/her job integrated with the CAIO?

Cloud systems are increasingly used by organizations to store and manage their data. Social media systems could also be hosted on the cloud. For example, social media companies could host their products on the cloud. Also, organizations that utilize social media could host their platforms on the cloud. Furthermore, cloud may be utilized to execute the complex AI/ML algorithms [21]. These clouds could be public clouds such as the Amazon web services or private clouds developed by organizations or a mixture of the public and private clouds (i.e., hybrid clouds) [22]. A cloud can support numerous customers. This results in challenges with respect to governance, Who is responsible for managing the cloud? Is it the responsibility of the Cloud Service Provider (CSP) or is it that of the organization who is using the cloud? We have argued that both have a role. The organization must ensure that only authorized users access the cloud. The CSP must ensure that the cloud is available as specified in the contacts. The CSP must also ensure that the customer's data is protected. With social media and the increasing need for massive processing power for AI systems, both data and cloud governance will be important components of Social Media and AI Governance.

VI SUMMARY AND DIRECTIONS

This paper has focused on integrating Social Media Governance and AI Governance for Fake News Detection. It first discussed aspects of social media governance. In particular, computer systems governance issues were explored for social media systems. This was followed by a discussion of fake news detection. In particular a Machine learning perspective for fake news detection was discussed. We then argued that for the Artificial Intelligence and Machine Learning techniques to be effective, they have to be trustworthy. For example how can we trust the results products by the various AI systems including the Generative AI systems? We discussed various aspects such as security, privacy, and fairness. We then discussed issues towards developing a framework for AI Governance. Finaly, we discussed data and cloud governance aspects that are needed both for social media governance and AI governance.

Many of the strategies and techniques discussed in this paper have to be explored future. That is. we need to develop frameworks for both social media governance and AI governance. These frameworks have to be integrated. More importantly, how do we know that the AI systems that are we are applying for numerous applications including for social media are trustworthy? How can we develop AI systems that are secure and ensure privacy, fairness, and integrity and at the same time produce results that are accurate? This is an enormous challenge for us. Therefore, while we are developing Trustworthy AI systems, we also need to develop criteria similar to the TCSEC (Trusted Computer Systems Evaluation Criteria) for evaluating the AI systems.

REFERENCES

[1] Bhavani Thuraisingham: Cyber Security and Data Governance Roles and Responsibilities at the C-Level and the Board. IEEE ISI 2019: 231-236

[2] Bhavani Thuraisingham: Cloud Governance. IEEE CLOUD 2020: 86-90

[3] Bhavani Thuraisingham: Artificial Intelligence and Data Science Governance: Roles and Responsibilities at the C-Level and the Board. IRI 2020: 314-31
[4] Bhavani Thuraisingham et al, Analyzing and Securing Social Media, CRC Press, 2016.
[5] Shon Harris, CISSP All in One Exam Guide, McCraw Hill 2018.
[6] Fake News Detection on Social Media: A Data Mining Perspective, SIGKDD Explorations, Volume 19, 2017
[7] Teena Thomas, Fake News Detection in Social Media. Term Paper, Analyzing and Securing Social Media. The University of Texas at Dallas, Summer 2021 (unpublished manuscript)
[8] Parikh, Shivam B., and Pradeep K. Atrey. "Media-rich fake news detection: A survey." *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*. IEEE, 2018.
[9] K. Stahl, "Fake news detection in social media." California State University Stanislaus 6 (2018, https://www.csustan.edu/sites/default/files/groups/University%20Honors%20Program/Journals/02_stahl.pdf
[10] Zhou, Xinyi, and Reza Zafarani. "A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities." *ACM Computing Surveys (CSUR)* (2020).
[11] Conroy, Nadia K., Victoria L. Rubin, and Yimin Chen. "Automatic deception detection: Methods for finding fake news." *Proceedings of the Association for Information Science and Technology* 52.1 (2015): 1-4.
[12] A. Yerlekar, et al, A multinomial technique for detecting fake news using the Naive Bayes Classifier, Proceedings International Conference on Computational Intelligence and Computing Applications (ICCICA), 2021
[13] Perspectives on Issues in AI Governance, Google Report, https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf
[14] TCSEC Trusted Computer Systems Evaluation Criteria, Department of Defense, 1983
[15] ISC2 CISSP Lecture Notes, March 2010, Dallas, TX.
[16] Sadaf Md. Halim, Saquib Irtiza, Yibo Hu, Latifur Khan, Bhavani Thuraisingham: WokeGPT: Improving Counterspeech Generation Against Online Hate Speech by Intelligently Augmenting Datasets Using a Novel Metric. IJCNN 2023: 1-10
[17] How AI Is Uprooting Major Industries, Jia Rizvi, Forbes Magazine, March 2024.
[18] S. Mezzio, M. Stein, and V. Campitelli, Cloud Governance: Basic and Practice, DE GRUYTER Publishers, 2023.
[19] John Ladley, Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program, Academic Press, 2019.
[20] B. Thuraisingham et al, Secure Data Science: Integrating Cyber Security and Data Science, CRC Press, 2022.
[21] Mohammad M. Masud, Tahseen Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han, Bhavani Thuraisingham. Cloud-based malware detection for evolving data streams. ACM Trans. Manag. Inf. Syst. 2(3): 16:1-16:27 (2011)
[22] B. Thuraisingham, Developing and Securing the Cloud, CRC Press, 2013.

ACKNOWLEDGEMENT: "This material is based upon work supported in part by the National Science Foundation under Award No. (FAIN): DGE-1723602. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation."