DIGITAL DECEPTION

UNCOVERING THE DARK SIDE OF AI IN SOCIAL NETWORKS

Editors:
Rupa Rani
Prashant Upadhyay
Rohit Sahu
Satya Prakash Yadav
Hardeo Kumar Thakur

Bentham Books

Federated Learning for Internet of Vehicles: IoV Image Processing, Vision & Intelligent Systems

(Volume 4)

Digital Deception: Uncovering the Dark Side of AI in Social Networks

Edited by

Rupa Rani
Department of Computer Science & Engineering Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India

Prashant Upadhyay
Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India

Rohit Sahu
GL Bajaj Institute of Technology and Management, Greater Noida, U.P., India

Satya Prakash Yadav
Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur, U.P., India

&

Hardeo Kumar Thakur
School of Computer Science Engineering and Technology (SCSET), Bennett University, Greater Noida, U.P., India

Federated Learning for Internet of Vehicles: IoV Image Processing, Vision & Intelligent Systems

(Volume 4)

Digital Deception: Uncovering the Dark Side of AI in Social Networks

Editors: Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur

ISBN (Online): 979-8-89881-003-0

ISBN (Print): 979-8-89881-004-7

ISBN (Paperback): 979-8-89881-005-4

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA.

First published in 2025.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

The book "Uncovering the Dark Side of AI in Social Networks" explores the ethical, societal, and psychological implications of artificial intelligence (AI) deployed within social networks. It delves into the potential negative consequences and hidden dangers that arise from the intersection of AI algorithms, social media platforms, and user behavior. The book aims to shed light on the often unseen and unacknowledged issues that arise when AI is employed in social networks. It provides an in-depth analysis of the impact of AI-driven algorithms on user privacy, information manipulation, polarization of online communities, mental health, and the overall well-being of individuals.

This preface is a "must-read" for individuals and professionals across various fields who are interested in or directly involved in the intersection of AI, social networks, and ethics. Some of the key audiences who will benefit from reading this book include researchers and academics, technology developers, policymakers and regulators, social media companies, privacy and data protection experts, ethicists and philosophers, social activists, and advocacy groups. Overall, the book caters to a wide range of readers who seek a comprehensive understanding of the ethical challenges and potential harm that AI algorithms pose within the realm of social networks. Also, this book will be of interest to lecturers and advanced students seeking additional resources, developers, and designers to enhance their understanding of the ethical considerations in AI development, as well as that of standard bodies and regulators involved in formulating guidelines and regulations related to AI and social networks.

This book employs a multidisciplinary approach, drawing on research and insights from various fields such as computer science, psychology, sociology, ethics, and law. The book combines theoretical analysis with real-world case studies, providing a comprehensive understanding of the complex interplay between AI, social networks, and human behavior. It also offers practical recommendations for individuals, policymakers, and technology companies to promote a more responsible and beneficial use of AI in the realm of social networks.

Rupa Rani
Department of Computer Science & Engineering
Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India

Prashant Upadhyay
Department of Computer Science & Engineering, School of
Engineering & Technology, Sharda University, Greater Noida, U.P., India

Rohit Sahu
GL Bajaj Institute of Technology and Management, Greater Noida, U.P., India

Satya Prakash Yadav
Department of Computer Science & Engineering,
Madan Mohan Malaviya University of Technology, Gorakhpur, U.P., India

&

Hardeo Kumar Thakur
>School of Computer Science Engineering and Technology
(SCSET), Bennett University, Greater Noida, U.P., India

List of Contributors

Archana Sharma	Department of Computer Science & Applications, Sharda University, Greater Noida, U.P., India Department of CSE, ABES Institute of Technology, Ghaziabad, U.P., India
Ayush Gupta	Department of Computer Science & Applications, Sharda University, Greater Noida, U.P., India Department of CSE, ABES Institute of Technology, Ghaziabad, U.P., India
Aryan Kumar Pandey	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Atul Kumar Rai	Computer Science & Engineering, Kotiwal Institute of Technology and Professional Studies, U.P., India
Abha Kiran Rajpoot	School of Computer Science & Engineering, Galgotias University, Greater Noida, U.P., India
Amit Upadhyay	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Chitra	Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India
Deepti Sahu	Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, U.P., India
Deepika Yadav	Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, Delhi, India
Garima Srivastava	Department of Computer Science & Engineering, Mangalmay Institute of Engineering & Technology, Greater Noida, U.P, India
Gunjan Aggarwal	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Harnit Saini	Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India
Hoor Fatima	School of Computer Science Engineering and Technology (SCSET), Bennett University, Greater Noida, U.P., India
Kajol Mittal	Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India
Kajal Gupta	CSE (Data Science), Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India
Manu	Computer Science and Engineering- Data Science, ABESIT, Ghaziabad, Uttar Pradesh 201001, India
Manoj Singhal	Department of Information Technology, GL Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India
Mandeep Singh	School of Computer Science Engineering, Bennett University, Greater Noida, U.P., India
Neha Varshney	Computer Science and Engineering- Data Science, ABESIT, Ghaziabad, Uttar Pradesh 201001, India
Neelaksh Sheel	Moradabad Institute of Technology, Moradabad, U.P., India

Nikiema Flavio	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Preeti Dubey	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Pushpendra Kumar Rajput	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Pooja Chaudhary	CSE (Data Science), Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India
Prashant Upadhyay	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Pawan Kumar	Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad. U.P., India
Ritika Binjola	Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India
Rupa Rani	Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India
Ruchi Patira	Department of Computer Science and Engineering, World College of Technology and Management, Gurgaon, Haryana, India
Rajani Singh	Department of Information Technology, GL Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India
Sushant Sharma	Department of Computer Science & Applications, Sharda University, Greater Noida, U.P., India Department of CSE, ABES Institute of Technology, Ghaziabad, U.P., India
Shivansh Soni	Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India
Sana Anjum	Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, U.P., India
Shikha Agarwal	Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India
Soniya Sharma	Department of Computer Application, Mangalmay Institute of Management & Technology, Greater Noida, U.P, India
Swati Singal	Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India
Sachin Jain	Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India
Sudeep Varshney	Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India
Tripti Singh	Department of Computer Science & Applications, Sharda University, Greater Noida, U.P., India Department of CSE, ABES Institute of Technology, Ghaziabad, U.P., India
Tejaswi Khanna	Department of Computer Science and Engineering, IMS Engineering College, Ghaziabad, U.P., India
Veena Bharti	Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India

CHAPTER 1

AI Deception Detection: Behavior Model and Techniques

Manu[1,*] and **Neha Varshney**[1]

[1] *Computer Science and Engineering- Data Science, ABESIT, Ghaziabad, Uttar Pradesh 201001, India*

Abstract: Nowadays, it has become very common for the message to reach the receiver in the wrong way by spreading false information. In every field, passing wrong information by pretending it is right has become easy since everyone is using recent technologies. It is often seen that the person is not involved, but his credentials and personal details are shared indirectly. One thing used behind this technology is artificial intelligence, which is not based on emotions but can cause harm by using false methods. Experts caution against giving artificial intelligence (AI) executive control because its lack of emotions can do unthinkable harm. Due to the absence of understanding and an ethical compass, it can ultimately result in choices that have terrible emotional repercussions. The importance is to be given to the implications of AI and cover the vulnerabilities of social networks, possible ethical issues on privacy, and automated cyberattack case studies. The effects of a breach can reverberate for years as cybercriminals use the information they have stolen. The potential risk is only constrained by the creativity and technological abilities of malevolent persons. Sophisticated artificial intelligence (AI) systems are capable of operating deceit on their own to avoid human oversight, such as avoiding safety tests that regulators have mandated of them. However, despite topical developments, social media platform administration will continue to face a number of ethical difficulties.

Keywords: Automation, Artificial intelligence, Cybercrime, Deception, Deep fake, Ethical.

INTRODUCTION

"Artificial Intelligence could help make it easier to build chemical and biological weapons." "In a worst-case scenario, society could lose all control over AI completely through the kind of AI sometimes referred to as super Intelligence." All the above statements are said by Prime Minister, UK, Rishi

[*] **Corresponding author Manu:** Computer Science and Engineering- Data Science, ABESIT, Ghaziabad, Uttar Pradesh 201001, India; E-mail: manu@abesit.edu.in

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

Sunak, before hosting the AI safety summit on 26 October 2023. Undoubtedly, AI is a governing field with its pros and cons everywhere. As AI is acknowledged by all of us in each domain, we need to understand its dark side with consequences.

The word deception has the meaning of demonstration of making somebody acknowledge as substantial what is invalid, but when the term is added with the word digital, it makes a broad sense with different domains. Also, it is the purposeful control of data in a mechanically intervened message to create a deception in the collector of the message. No matter what the various likely advantages, there are, without a doubt, many unfortunate results of simulated intelligence. Digital deception, a significant issue in our personal and professional lives, arises from the intersection of deception and communication technology. Digital deception is the deliberate act of misleading or tricking individuals or groups using digital technologies. This can manifest in various forms, such as spreading false information through social media, creating counterfeit websites, and manipulating digital content. Digital deception exploits the widespread use of digital technologies and the ease with which information can be disseminated and manipulated online, often for purposes such as spreading misinformation, influencing public opinion, or perpetrating fraud. Online gaming bullying, also known as cyberbullying, refers to harassment, intimidation, or aggressive behavior directed towards other players. In addition to delivering a peer-to-peer secure platform for information exchange and storage, distributed ledger technologies (DLTs) such as blockchain ensure the provenance and traceability of data by offering a transparent, immutable, and verifiable record of transactions.

When we talk about deception in the context of artificial intelligence, we usually mean the creation or dissemination of false or misleading information through the use of AI or machine learning techniques, frequently with the goal of tricking or controlling individuals or systems. AI deception can be used maliciously; AI can also be used to recognize and combat deception. Artificial intelligence might prompt gigantic dangers at the singular level, association level, and society level. Critically, these three angles are considered the main components of digitalization. We mainly discuss the dark sides of AI in various fields shown in Fig. (**1**).

Electronic Market

An electronic market alludes to a virtual exchanging climate that incorporates purchasers and vendors through unique web applications and also different applications in view of web correspondence innovation. Various advanced business organizations and retailers, for example, Amazon, influence artificial intelligence to upgrade deals, draw in and hold clients, and further develop

productivity through improved promotion techniques and smoothed-out business processes [1].

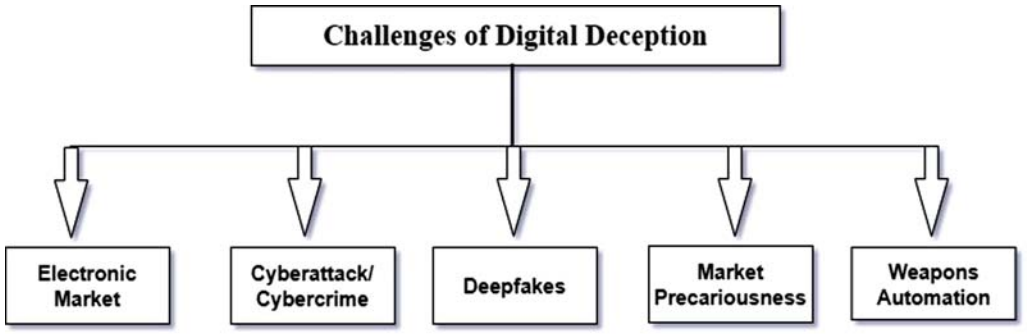

Fig. (1). Challenges of digital deception.

The rising reception of another generative artificial intelligence innovation, ChatGPT, in the electronic market, is remarkable because of its groundbreaking effect on client communications and general business tasks [1]. While ChatGPT offers huge potential for the electronic market — like better client support, smoothed-out deals and exchanges, adaptability, cost-adequacy, and upper hand—it is fundamental to perceive that it can likewise present explicit antagonistic impacts.

In the first place, ChatGPT's capacity to produce text can be taken advantage of to spread disinformation or control economic situations [2]. Noxious actors can utilize the innovation to disperse deluding item portrayals, control stock costs, or misdirect clients. Second, while ChatGPT can give mechanized client assistance, it might miss the mark on compassion and nuanced understanding that human specialists have. This can prompt baffled clients and negative encounters, possibly influencing trust and steadfastness in the e-market. From the individual's perspective, the detrimental effects of AI are mainly reflected in privacy concerns and content and product recommendations in electronic markets [3].

Cyberattack/Cybercrime

AI may be used in cyberattacks to mask harmful behavior, such as obfuscating malware or avoiding intrusion detection systems. Malicious actors are beginning to understand the potential applications of artificial intelligence. Not every AI tool will have the proper safeguards to prevent misuse, and malicious actors will constantly search for new ways to exploit vulnerabilities [4]. Cyberattacks are turning out to be progressively refined and designated.

CHAPTER 2

Navigating the Digital Frontier: An In-depth Exploration of Social Network Vulnerabilities and the Impact of Artificial Intelligence

Archana Sharma[1,*], Ayush Gupta[2], Sushant Sharma[2] and **Tripti Singh[2]**

[1] *Department of Computer Science & Applications, Sharda University, Greater Noida, U.P., India*

[2] *Department of CSE, ABES Institute of Technology, Ghaziabad, U.P., India*

Abstract: As digital interactions dominate our lives, social networks have become both a cornerstone and a breeding ground for vulnerabilities. "Understanding Social Network Vulnerabilities" dives into this complex landscape, exposing the weak points we face and the double-edged sword of artificial intelligence (AI) – a technology that can both amplify and mitigate these risks. This study goes beyond mere identification, delving into the intricate web of vulnerabilities, from privacy concerns to cybersecurity threats, while exploring the impact of AI on both sides of the equation. Utilizing a comprehensive approach that blends expert insights, real-world case studies, and thorough research, it unveils practical solutions and underscores the urgency of addressing these vulnerabilities. Ultimately, this work serves as a crucial roadmap for individuals, companies, and governments alike, navigating the evolving digital landscape with the knowledge that AI's transformative potential holds the key to both challenges and solutions.

Keywords: Artificial intelligence, Malware, Security, Social network, Threats, Vulnerability.

INTRODUCTION

In our ever interlinking on- and offline lifestyles, social networks have rapidly become the glue. They have transformed the nature of communication, information of public trust friends, and commerce. Social networks now carry considerable weight, and the more powerful they become, the bigger the risks of being exploited for ill gains that involve [1]. This study is necessary to formulate strategies that will protect people, organizations, and society as a whole against the continually shifting risks that come from digital environments. This view

[*] **Corresponding author Archana Sharma:** Department of Computer Science & Applications, Sharda University, Greater Noida, U.P., India; E-mail: archanasks1976@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

takes the importance of such work even further. If we were to analyze the vulnerabilities in social networks in full detail, we would find a complex web of problems and need to come up with both practical solutions for mitigation. We aim to uncover the latent faults that allow this to happen, evaluate their impact, and suggest remedies [2]. We cannot overstate the importance of such research. Our communication, ability to obtain information, and interface with the world all depend on social networks. This prominence gives a major reason to get over shortcomings that may affect data security, the integrity of online interactions, and trust. The vulnerabilities of social networks carry profound social, economic, and political implications, requiring immediate recognition and response. In a world of rapid technological change, we must understand and tackle the risks inherent in social networks. We need to make these platforms robust, reliable, and safe as we rely on them increasingly more for different parts of our lives [3].

This paper explores the darker side of AI in social networks, focusing on how it contributes to challenges like misinformation, privacy breaches, and cybersecurity threats. It examines the vulnerabilities created by AI, analyzes their impact on users and society, and evaluates potential solutions. Through detailed research, the paper aims to uncover the root causes of these issues, propose mitigation strategies, and highlight the importance of a collaborative approach to building safer and more secure digital platforms. To identify suspicioususers, we proposed a model that used decision tree and support vector machine (SVM) for classification and metaheuristic algorithms like particle Swarm Optimization (PSO) and Differential evolution (DE) for feature selection. The rationale behind proposing this model hinges on the availability of a dataset that includes not only all user activity but also activity that pertains to the other users- such as the content of their posts, comments, and the posts that they have interacted with. As such, the data is firmly gatekept by social networks and cannot be used for research without violation of privacy ethics. Therefore, this system, however successful, is hypothetical until this information becomes available.

This chapter consists of various sections. Section 2 defines the social network and provides us with some of its insights, Section 3 defines some of the types of vulnerabilities of social networks, Section 4 defines the solutions to mitigate the vulnerabilities of social networks, Section 5 defines the proposed methodology/model to implement mitigations methods in the best way, and lastly, Section 6 concludes the article.

SOCIAL NETWORK AND ITS INSIGHTS

In the Internet context, a social network is an online place that enables people to encounter others who have the same connections, experiences, or identities. The

public can ensure that their ideas, news, and assorted knowledge by way of these computer-mediated forums get the responsiveness of friends, family members, colleagues, and clients. TikTok, Facebook, Instagram, and WhatsApp are the best-known social media platforms at present. Such platforms provide opportunities to chat with people who share the same goals, interests, or experiences. These hands-on social networks can allow people to connect with new friends who have similar interests and goals. To keep in touch with other users, they can follow groups, lists, hashtags, or all other sorts of ways depending on their interests. Users can also set up their profile values, add pictures and videos, or make news and notes. Social media sites are a nearly indispensable resource for public relations campaigns. Companies and institutions are using social media platforms not only to communicate with current or prospective customers but also to publicize their brands, products, and services. Besides being valuable sources of feedback and insight, such outlets also offer opportunities for conversion, client retention, and branding. It is important to remember that social networking sites are a part of the larger discipline of network science, which explores the complex dynamics and intricate structure of networks.

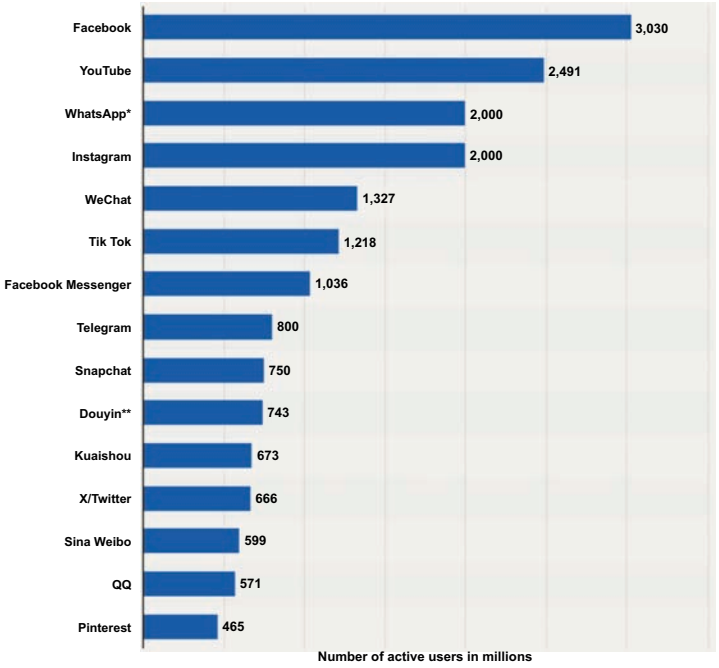

Fig. (1). The Statistics of Social Network Sites Users [4].

Fig. (**1**) states the latest statistics on the popularity and usage of social network sites worldwide as of October 2023. It shows that Facebook is the most widely

CHAPTER 3

Federated Learning for Enhanced Intrusion Detection: Combating Digital Deception in IoT-Enabled Social Networks

Shivansh Soni[1,*], **Ritika Binjola**[1] and **Kajol Mittal**[1]

[1] *Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India*

Abstract: The Internet of Things has completely changed the way we interact with our surroundings. The upsurge in the use of IoT devices has helped us to do and monitor our day-to-day tasks with ease. With the increasing use of IoTs, there also comes their own set of security issues that need to be considered. IoT devices generate vast amounts of data, most of which can be shared or connected to social networking sites or online platforms. Due to malicious activity or attacks in the network, the data can be manipulated. Digital deception poses a significant threat in the era of AI-driven social networks, enabling the spread of misinformation and cyber intrusions at an unprecedented scale. Here comes the role of the intrusion detection system, which helps us to detect and prevent security breaches in IoT. In recent years, it has become a critical issue to secure IoT systems as they are more prone to be hacked. So, it has become very important to develop and optimize our traditional intrusion detection systems. Previously used intrusion detection systems suffered from several limitations, such as centralized data storage, privacy, and security concerns. They require a significant amount of processed data to work effectively according to our criteria. This can be challenging to us in case of very few historical attacks that are not enough to train our systems. To overcome these issues, federated learning-based IDS for IoT systems has been proposed. Federated Learning is a machine learning technique that provides a system that can collaboratively learn a model without sharing its data. In federated learning, the machine learning model is trained on the device itself, and only the updates are pushed to the central server for improvement of the central model. It helps us preserve the privacy of the device and, at the same time, enables us to build and train the central model server that can detect any intrusion attacks. This can also reduce the computational cost of machine training by distributing the work across several devices. Federated learning models can adapt to the changes in the environment as they are designed to continuously learn from the recently generated data from servers and devices in the network. This way, the model can progress over time to better detect the changes in the network traffic.

[*] **Corresponding author Shivansh Soni:** Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India; E-mail: s.shivansh94550@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

Keywords: Aggregation functions, Federated learning, Intrusion detection, IoT-enabled social networks, Machine learning.

INTRODUCTION

Social networks integrate day-by-day IoT devices, from smart homes to wearable devices. As social networks grow increasingly intertwined with IoT, the need for scalable and intelligent security frameworks like federated learning becomes essential to combat deception and safeguard user integrity. As a result of digitization, the amount of data generated and stored has increased dramatically. With the cheapening of storage devices and technological infrastructure, it has become a common practice to store and analyze every possible data that is passed through a network, which has caused a sudden surge in database instances. On the other hand, the number of IoT devices is increasing in our environment due to their establishment in smart cities, domestic appliances, *etc*. The information generated by these devices is highly valuable for the big business industries and intelligence departments [1] as it helps them to analyze the current trends and flaws of a product and also helps a lot in improving the current technology. As a result, data has become a highly appreciable asset that needs to be secure and in safe hands. Security systems have become a very important element to avoid data loss, intrusions, malicious code injections [2], *etc*. The area involving security measures is ambiguous and needs constant updates and reform to cope with the new attacks. As an important aspect of security infrastructure, intrusion detection systems play a very crucial role by monitoring system activity and alerting the system in case any malicious or suspicious activity is detected. Threat detection techniques have evolved with the evolution of new machine-learning models. In the initial phase of IDS, they were quickly able to detect severe attacks and critical data leaks, but they failed to detect new threats that were not in the database. Also, the gap between the detection and mitigation of threats was lengthy, which gave the attack enough time to succeed in most cases. With the second generation of the intrusion detection system, they were capable of learning about new attacks using various machine learning models like Support Vector Machines [3] (SVM), Random Forests [4] (RF), Multilayer Perceptron [5] (MLP), *etc*. These systems further aggregated deep learning models within them, which further increased their accuracy and performance. Now as they are capable of detecting the activities, it is now important to secure the whole network rather than focusing on individual devices. To address this issue, we need to allow devices to share information about newly detected attacks so that it is globally recognized and this will create a global impact in reducing the damages due to attacks. Sharing data is infeasible with the centralized learning [6] approach as it deals with data in a raw way, and it can cause traffic data flow problems within the network. In this context, federated learning [7] has emerged as a promising

tool to deal with the information exchange between different devices that are physically isolated and deal with the problem of sensitive data exploitation.

FEDERATED LEARNING

Federated learning [7] is a machine learning technique that provides a system that can collaboratively learn a model without sharing its data. In this technique, the model is trained on the device itself, and only the updates are pushed to the central server for improvement of the central model. It enables the development of machine learning models on a decentralized data [8] pool, such as smartphones, IoT devices, edge servers, *etc*. In the standard federated learning settings, every device has its local storage and its local data using which they train their local machine learning model; then, these individual local models are sent to the central server where they are accumulated into a global model. The global model is then sent back to the devices where it is taken as a reference to improve and modify individual local models accordingly. This process is repeated again and again until the central model reaches the desired level of training and accuracy.

Advantages of federated learning over traditional techniques:

- Distributed Learning [9] - FL helps the devices interact and collaborate on a task or training, even when they are globally and physically isolated from each other, thereby enabling efficient learning in a decentralized system [10].
- Reduced Communication Costs – FL does not require or require very minimal data transfer between servers and devices, so it reduces communication costs and increases efficiency.
- Improved Scalability – Federated learning-based models can continue to learn from new data and information as they are made available. FL algorithms can easily scale to a large number of devices due to their low communication overhead, and hence, they are more scalable than a traditional system.
- Data Privacy - FL-based models ensure user data privacy as they take care that the user data remains on the local device itself and reduce the chances of data breaches and privacy violations.
- Decentralization [10] – Federated learning ensures that there is no central server where user data is stored and hence provides a promising decentralized machine learning model that provides greater scalability, flexibility, and performance.

RELATED WORK

The use of federated learning has significantly generated interest in recent years due to its strengths and use cases, which can be implemented in different IoT scenarios. We have considered various aspects to classify the recently proposed

CHAPTER 4

AI-Driven Identity Manipulation

Sana Anjum[1,*] and **Deepti Sahu**[2]

[1] *Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, U.P., India*

[2] *Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, U.P., India*

Abstract: Identity theft refers to the illegal act of using someone else's personal information for fraudulent transactions. Perpetrators employ various techniques, ranging from sifting through discarded materials like credit cards and bank statements to more sophisticated methods like hacking into organizational databases to access consumer data. While identity thieves continuously develop new tactics, individuals can significantly mitigate the risk by exercising vigilance on social media platforms and practicing caution when dealing with unfamiliar emails. Identity theft remains a persistent and escalating issue, impacting a growing number of individuals and inflicting direct and indirect harm on victims. In this chapter, we are going to highlight some common types of identity theft and the role of artificial intelligence in this manipulation. Also, we will review various research papers to find solution for problems related to identity theft, such as fake profile identification using ML-based algorithms. Furthermore, the chapter will also discuss the future possibilities in this field.

Keywords: Artificial intelligence, Cyberattacks, Deepfakes, Identity manipulation, Machine learning.

INTRODUCTION

In the past, individuals like Juliet were known for their vigilant online presence, practicing strong cybersecurity measures. One day, while scrolling through her social media feed, Juliet stumbled upon a profile eerily similar to her own. It was a case of an AI-driven digital clone, part of a growing trend where identities were replicated with astonishing precision. This AI-driven identity manipulation had become a widespread issue, leading to impersonation, identity theft, and fraudulent activities on an unprecedented scale. These digital doppelgangers were not mere imitations; they evolved, adapting seamlessly to their digital surroun-

* **Corresponding author Sana Anjum:** Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, U.P., India; E-mail: sana.anjum02@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

dings and infiltrating social, financial, and professional networks. Juliet's journey to unmask her digital clone mirrored the larger battle against this emerging threat. As victims united to protect their identities and uncover the perpetrators, they confronted the evolving challenges posed by AI-driven identity manipulation.

This anecdote illustrates the rise of AI-driven identity manipulation, which forms the backdrop for our exploration of cloned accounts, impersonation, identity theft, and fraudulent activities in the digital age. Fig. (**1**) illustrates the percentage of people affected by identity theft [1] according to their age group.

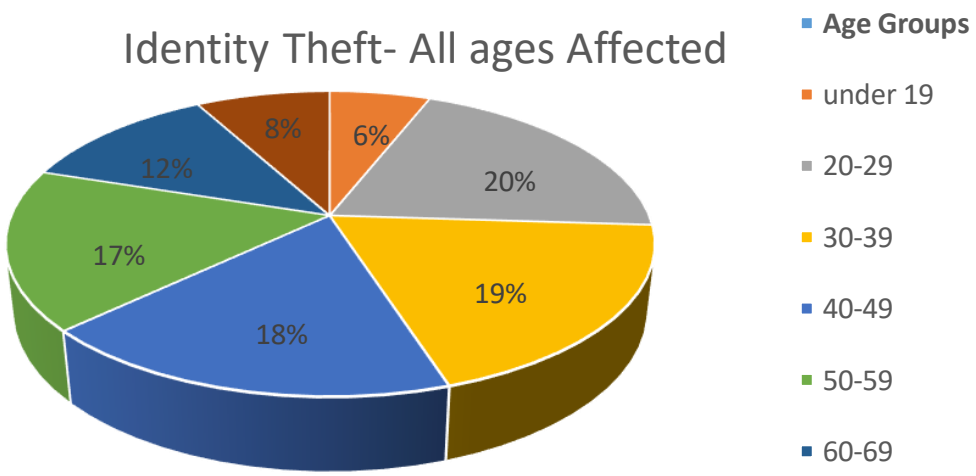

Fig. (1). Identity theft ratio in different age groups of people [1].

Identity manipulation has a rich historical evolution. It began with handwritten forgeries and seal impersonations in the pre-modern era. The advent of photography in the 19th century allowed for photographic manipulation, while the late 20th century saw the rise of digital manipulation and social engineering techniques like phishing. In the 21st century, AI, particularly deep learning and GANs, has empowered sophisticated identity manipulation, including deepfakes. Social media and cybercrime have further fueled this issue. These actions share a common characteristic: they involve the intentional manipulation of digital identities for unlawful purposes. A comprehensive grasp of these tactics is imperative as we strive to shield individuals and organizations from the burgeoning threats posed by cybercriminals and malicious entities. Regulations and cyber security measures have been introduced to combat identity manipulation, which continues to evolve with technology.

In the era of digital interconnectedness, we find ourselves confronted with a diverse array of deceptive strategies and illicit maneuvers that erode trust and compromise security. This chapter is dedicated to delving into the intricate domain of digital deception, which encompasses a spectrum of malicious behaviors, including the creation of cloned accounts, impersonation, identity theft, and other types of deceitful conduct. This chapter's goal is to review the theories and research on identity manipulation. The chapter covers different types of manipulation techniques in section 1.1 and the role of AI in section 1.2. The rest of the chapter is organized in the following sequence. Section 2 reviews empirical work that has been done by different researchers to find out the solution for this theft. In section 3, we discuss the impact of this manipulation on society, followed by section 4, which contains the proposed approach and section 5, which discusses future scope for further investigation. Finally, section 6 concludes the chapter.

Cloned Accounts and Impersonation

Fake accounts, commonly known as clone accounts in the digital space, are fictitious online profiles created to deceive or mislead others. These accounts often mimic real individuals or organizations, using stolen or fabricated personal information, photos, and other details. The motivations behind these fake accounts can vary widely, including impersonation, identity theft, spreading misinformation, and engaging in fraudulent activities.

The growing prevalence of fake accounts poses significant risks to online trust and security. They can lead to reputational damage for individuals and brands, as impersonators may spread false information or conduct scams under the guise of authenticity. This not only confuses users but can also result in financial losses and legal issues for those affected.

To combat this issue, it is crucial for users to be cautious about sharing personal information and to verify the authenticity of profiles before engaging with them. Additionally, social media platforms must implement effective measures to detect and remove fraudulent accounts. Understanding the characteristics and risks associated with fake accounts is essential for maintaining a secure online environment.

Fake accounts serve multiple purposes, ranging from deceptive actions such as blackmail and extortion, which erode trust within social networks, to more sinister activities like disseminating false information, recruiting individuals into terrorist organizations, and, tragically, even contributing to instances of self-harm. It is worth emphasizing that fake accounts are not solely employed for harmful intentions; they also serve various personal agendas that may not directly impact

CHAPTER 5

Understanding the Dynamics of Misinformation and Disinformation: A Comprehensive Review

Veena Bharti[1,*], **Chitra**[1] and **Shikha Agarwal**[2]

[1] *Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India*

[2] *Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India*

Abstract: The quick spread of information in the digital era can be both a benefit and a drawback. The production of misinformation and disinformation has become apparent as a significant societal confrontation facilitated by the interconnected world of the internet and social media. Misinformation, often unintentional, spreads due to errors or misunderstandings, while disinformation, driven by deceitful intent, aims to manipulate or deceive. The propagation of false information is fuelled by the dynamics of the digital landscape. The internet community and digital platforms, in particular, have developed into conduits of swift outspread of both misinformation and disinformation. These platforms offer an unparalleled level of connectivity and engagement, making it easier for misleading content to reach a vast audience quickly. The virality of such content is heightened by its ability to evoke strong emotions, playing on fear, anger, or excitement, which drive users to share and engage. Mutual admiration societies, wherein communities interact and shore up their beliefs, have further perpetuated the spread of deceiving information, hindering efforts to discern fact from fiction. Additionally, polarized societies can exacerbate the issue, with individuals being more receptive to information that aligns with their existing viewpoint. This paper delves into the main key aspects of the propagation of misinformation and disinformation.

Keywords: Conflict, Disinformation, Echo chambers, Economic impact, Misinformation, Social unrest, Virality.

INTRODUCTION

In a modern era characterized by unprecedented entrance to information and worldwide connectivity, the propagation of misinformation and disinformation has emerged as a pressing and complex challenge. The digital revolution, with its array of communication platforms and social media networks, has granted individuals the power to disseminate information to a vast and diverse audience

[*] **Corresponding author Veena Bharti:** Raj Kumar Goel Institute of Technology, Ghaziabad, U.P., India; E-mail: bharti.veena@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

with remarkable speed. While this capability has the potential to enhance knowledge sharing, it has also opened the floodgates to the spread of falsehoods, inaccuracies, and manipulative narratives. To combat this challenge, fact-checking organizations work tirelessly to validate the accuracy of news in mass media [1]. The goal of media literacy education programs is to give people the solemn thoughts and abilities necessary to assess material critically. Social media companies have implemented content monitoring and reporting tools to prevent the spread of inaccurate or dangerous content.

It is the fight against misinformation and disinformation and is an ongoing, multi-faceted effort demanding the collective engagement of individuals, technology companies, and society at large. Recognizing the mechanisms of the propagation of misinformation and disinformation is crucial in advancing tactics to promote further informed and discerning people in the digital era [2]. Misinformation, a term used to describe inaccurate or false information that is shared lacking the deliberate plan to delude, often emerges from legitimate errors, misunderstandings, and misinterpretation of facts. In contrast, disinformation is a more insidious phenomenon involving the creation and propagation of fake data with the explicit purpose of fraud, influencing individuals or groups for various agendas [3]. Together, misinformation and disinformation represent a spectrum of untruths that can have wide-ranging and profound consequences on society, politics, public health, and more.

This introduction explores the propagation of misinformation and disinformation, examining the mechanisms underlying their spread and the effects they have on people as individuals, communities, and the broader global landscape. In doing so, it underscores the urgency of addressing this issue and highlights the multifaceted strategies employed to combat the spread of false information in our increasingly interconnected world.

The spread of false information and deception has reached previously unheard-of heights in our era dominated by social media and mathematical connections, drastically altering the public debate and information distribution landscape [4]. Fig. (**1**) illustrates the intricate web through which false information proliferates, highlighting the multifaceted mechanisms that contribute to its rapid spread.

Fig. (**1**) depicts the interconnected pathways through which misinformation and disinformation traverse various online and offline channels. It seeks to give a visual representation of intricate dynamics immersed in the dissemination of false information, capturing the key stages and influencing factors.

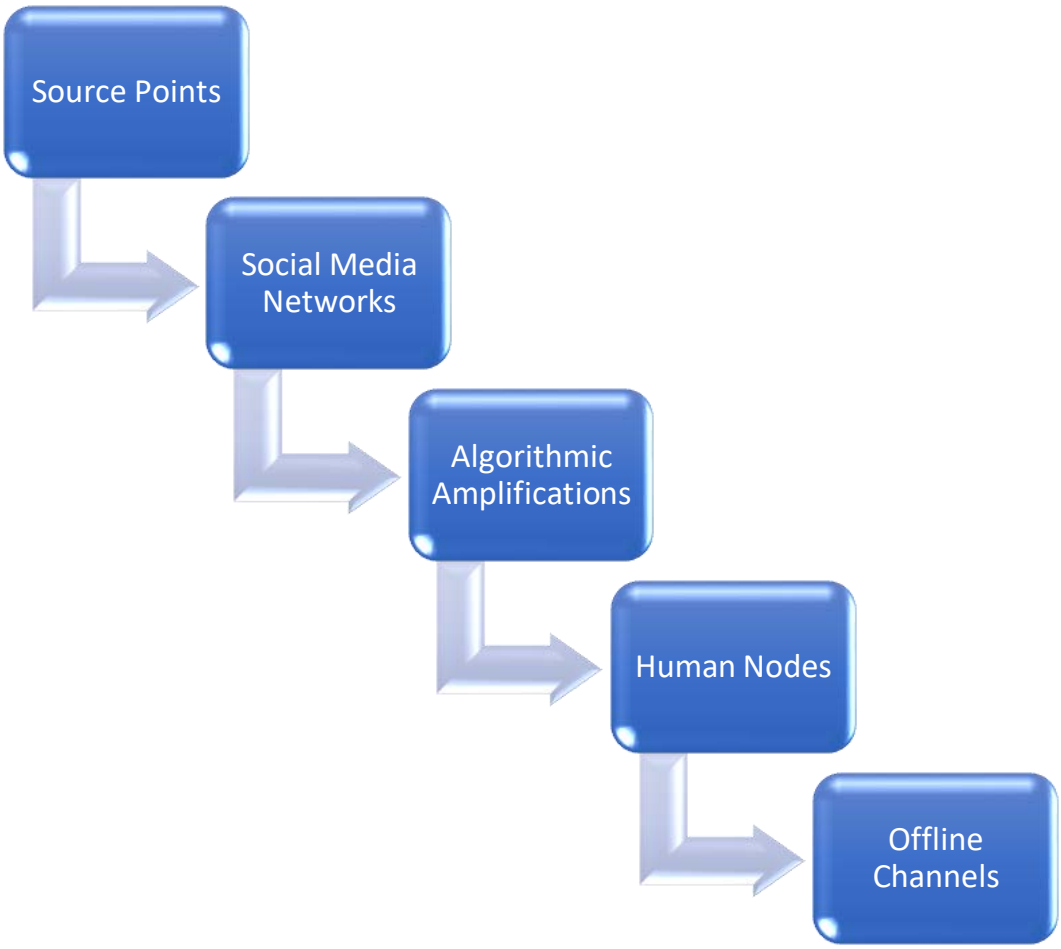

Fig. (1). The Propagation of Misinformation and Disinformation.

Key Components of the Figure

Source Points

At the core of the figure are the source points, representing the origins of misinformation and disinformation. These sources may include individuals, organizations, or automated bots with malicious intent.

Social Media Networks

Arrows emanating from the source points extend towards social media networks, emphasizing the significant role these platforms play in amplifying false information. The intricate connections symbolize the rapid and widespread nature of dissemination within these digital ecosystems.

CHAPTER 6

Privacy Concerns in AI-Powered Social Networks

Garima Srivastava[1,*] and **Soniya Sharma**[2]

[1] *Department of Computer Science & Engineering, Mangalmay Institute of Engineering & Technology, Greater Noida, U.P, India*

[2] *Department of Computer Application, Mangalmay Institute of Management & Technology, Greater Noida, U.P, India*

Abstract: Artificial Intelligence (AI) is a field within computer science that studies a machine's capacity to mimic intelligent human behavior. Artificial intelligence (AI) exhibits significant potential in tackling present-day socioeconomic challenges. Nowadays, social media—also referred to as social networking—consists of Facebook, YouTube, Pinterest, Instagram, and Twitter. AI has a major role in the way today's social networks function. This chapter covers the privacy issues that arise when AI is integrated with social networking platforms, specifically in user data gathering, profiling, and algorithms that make decisions. While AI technologies like facial recognition, machine learning, and natural language processing allow social networks to provide individualized experiences, they also face serious concerns about data privacy, consent, and surveillance. AI systems often rely on large-scale personal data sets. Artificial intelligence (AI) is becoming more and more prevalent in social networks, radically changing social media in the process but also raising some issues related to data. The legal implications of AI in social media are also explored, including the possibility of bias, manipulation, and loss of control over personal information. This chapter explores how AI-powered services, such as content recommendation engines, automated content moderation, and targeted advertising, may unintentionally jeopardize user privacy by gathering and using private data. We also talk about the real case study related to it, as well as the usage of AI in social networks, the kinds of privacy issues that can develop, and how to address them.

Keywords: AI, Artificial intelligence, Data privacy, Online social networks (OSNs), Social networks, Surveillance, Tracking.

INTRODUCTION

Artificial intelligence (AI) refers to technological progress wherein machines or robots emulate human intelligence in performing various tasks. AI is becoming

[*] **Corresponding author Garima Srivastava:** Department of Computer Science & Engineering, Mangalmay Institute of Engineering & Technology, Greater Noida, U.P, India; E-mail: versatilegarima@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

more and more common in streaming services, healthcare systems, and online commerce; chances are, you have used it inadvertently [1].

Recently, discussions about AI have extended to topics like cybersecurity, information, and data privacy. This manual will go into deeper detail about the effects of AI on data privacy and explore measures for its protection. Concerns over the privacy of personal data have surfaced as artificial intelligence (AI) advances. AI systems often depend on substantial collections of personal data for learning and making predictions. This situation gives rise to concerns regarding the acquisition, processing, and storage of this data.

These days, online social networks, or OSNs, are a big part of our everyday lives and society. This is not shocking, considering the platforms, tools, applications, and services of this kind enable us to easily gather, exchange, and disseminate data, information, and knowledge on a far greater scale and without regard to location. Additionally, it has influenced developments such as the emergence of AI-powered, human-centered frontier computing, which is driven by the massive volumes of big data produced by social media. Novel computing paradigms aimed at facilitating social data mining and knowledge discovery, such as aware computing and (social) situation analytics, are included in this. However, there are issues with security, privacy, and reliability that need to be addressed. Artificial intelligence theories and techniques, such as those based on machine learning, deep learning, and causality inference, must be integrated in order to address these problems. In addition, addressing these issues requires online social networks to integrate hardware-controlled and human-centric elements [2].

Artificial intelligence privacy concerns mainly focus on the potential for data breaches and unauthorized access to personal data. The vast amount of data that is gathered and processed raises the possibility that it could fall into wrong hands due to hacking or other security lapses.

ARTIFICIAL INTELLIGENCE IN THE PUBLIC SECTOR

Artificial intelligence (AI) is being used in more and more aspects of our lives, usually in undetectable and invisible manners. AI is used in the background by many digital platforms and services to improve user experiences, manage procedures, and give customized services [3]. Here are a few examples of how AI is commonly used without always being immediately apparent:

Use as a Recommendation System

AI algorithms are used by streaming services like YouTube, Netflix, and Facebook, music apps like Spotify, and online retailers like Flipkart, Amazon, and

Myntra to analyze customer behavior and interests. This helps suggest videos, movies, songs, or products that you might like based on your past choices and searches the products.

Client Support Chatbots

AI-powered chatbots are widely used on websites and customer support portals to answer routine questions from users, offer information, or help with troubleshooting. Natural language processing, or NLP, is what these bots use to understand and reply to user questions.

Illegal Activity Identification

To identify abnormal trends in transactions that can point to fraudulent activity, financial institutions frequently depend on AI systems. This aids in protecting user accounts and avoiding unauthorized access.

Medical Diagnostic Testing

By examining medical images, identifying patterns within patient data, and making suggestions for possible treatments, AI algorithms help healthcare professionals detect diseases.

Social Network

Smart enterprises are also using artificial intelligence (AI) in social networks for e-commerce, advertising, marketing, customer service, and other purposes. There are various uses for artificial intelligence in social media businesses.

These examples demonstrate how AI has impacted various industries, making tasks more efficient and personalized. SAI technologies, such as machine learning, robotics, computer vision, and natural language processing, continue to evolve and have applications in various fields like healthcare, finance, social networks, entertainment, and more. Artificial intelligence has quickly changed a lot of our lives, such as everyday routines, healthcare, and commerce. Its applications have made shopping easier, improved healthcare, and made people's lives much more convenient overall. Businesses are adopting AI widely across industries as a result of realizing its enormous potential and benefits. The fact that over 80% of business executives are using AI and finding benefits from it is a stated statistic that highlights the increasing recognition of AI's potential to boost productivity, efficiency, and creativity within enterprises [3, 4].

CHAPTER 7

AI Algorithmic Bias and Manipulation in Social Networks

Rupa Rani[1,*] and **Harnit Saini**[1]

[1] *Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India*

Abstract: Algorithms are increasingly being employed in our daily lives to make decisions, and the manipulation of algorithmic bias is becoming a serious worry. Because these decisions greatly impact people and society, they must be neutral and fair. The purpose of this study is to raise awareness of the potential drawbacks of algorithmic bias reduction. Algorithmic bias manipulation can have a wide range of negative social consequences. It has the potential to discriminate against or favor specific outcomes for certain groups of individuals. This method may result in inequity and social injustice. Biased algorithm manipulation can have serious repercussions for persons and society. To lessen the impact, steps need to be taken. Algorithmic bias modification has a wide range of applications. It can be used to target certain racial or ethnic groups, or it can be used to promote specific results, such as higher earnings. One disadvantage is that algorithmic bias manipulation might be difficult to identify and prevent. It might be difficult to determine whether or not algorithms are prejudiced because they are often highly complicated and advanced. The manipulation of algorithms to introduce bias has serious ramifications for people and society. It is critical to implement mitigation measures. Algorithm manipulation to introduce bias is a critical issue that can hurt both society and individuals. Understanding and protecting against the possibility of manipulating algorithmic bias are crucial.

Keywords: AI algorithms,, Algorithms bias, Manipulation, Machine learning, Society, Social network.

INTRODUCTION

An algorithm is a set of principles or actions that is used to execute a computation or address a problem. It is the precise understanding of how to complete a task successfully, which is characterized as a succession of behaviors that lead to the intended output. Algorithms, which are ubiquitous in our lives, have a significant impact on our daily decisions and experiences. The frameworks that power our

[*] **Corresponding author Rupa Rani:** Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India; E-mail: rupachoudhary2010@gmail.com

devices, drive our online discussions, and even speed up our regular routines are infused with the invisible designers of our digital environment. Algorithms are at work controlling the flow of information and molding our views from the moment we wake up to the moment our smartphone screens light up. When we search the internet, algorithms [1] scan through huge volumes of information to offer the most relevant and engaging material. They handpick updates and posts from our social media feeds that are most likely to keep us scrolling. They fuel systems of recommendations by recommending things, films, and music based on our preferences and interests. Algorithms are also useful in business because they manage supply chains, optimize pricing tactics, and make transactions *via* the Internet faster. They serve as the foundation for fraud detection systems, examining trends and weaknesses to detect suspicious activity to safeguard clients. Algorithms are also changing transportation routing, facilitating self - driving cars in traversing the city's overcrowded network of highways. Algorithms have far-reaching consequences on our physical and digital lives [2]. They influence our financial choices by assessing loan eligibility and creditworthiness. They help with diagnosis and therapy planning, which benefits medical treatments. In the criminal justice system, algorithms are employed for evaluating risk and determining restrictions. Despite their enormous promise to improve efficacy, precision, and customization, algorithms raise concerns about prejudice and discrimination. When algorithms are created inequitably or trained on biased data, they run the danger of providing inequitable results and perpetuating existing imbalances. As we become more reliant on algorithms in our daily lives, they must be created and used appropriately. We need to raise awareness of algorithmic bias, provide tools for identifying and mitigating bias, and encourage the development of impartial and egalitarian algorithms. We can take advantage of the power of algorithms while limiting their exploitation by detecting the potential for harm and taking appropriate action (Fig. **1**).

Algorithms are rapidly affecting decision-making processes ranging from social media platforms to criminal justice systems in today's data-driven society. Algorithms can improve both efficiency and precision, but they also raise issues about algorithmic bias, which can result in unfair and discriminating outcomes [3]. The deliberate act of building or exploiting prejudice in algorithms, known as algorithmic bias manipulation, poses an important threat to individuals and society. Algorithms are all around us [4], influencing our decisions and changing our experiences. They are linked to systems that assess their financial standing, filter news feeds, and recommend products. Algorithms, while capable of automating activities and providing important data, can be biased, which can have serious [5] and far-reaching consequences. The deliberate modification of algorithms to introduce or exploit bias is referred to as “algorithmic bias manipulation”, and it can have negative repercussions for both individuals and

society. It has the potential to erode public trust in institutions, discriminate against specific groups, and perpetuate socioeconomic imbalances. Prejudiced algorithm manipulation has far-reaching implications for everything from opportunity access to justice administration. Creating detection and prevention tools, assisting in the creation of impartial and fair algorithms, and raising public awareness are all critical components of a multifaceted strategy to combat algorithmic bias manipulation. We can ensure that algorithms are utilized responsibly and ethically by understanding the potential of prejudice and taking proactive steps to limit its negative consequences, building a more just and equal society. We must be aware of the risk of algorithmic bias and take proactive measures to address it. By enhancing awareness, determining effective detection and prevention mechanisms, and supporting fair algorithmic growth, we can benefit from the power of algorithms while avoiding the possibility of damage.

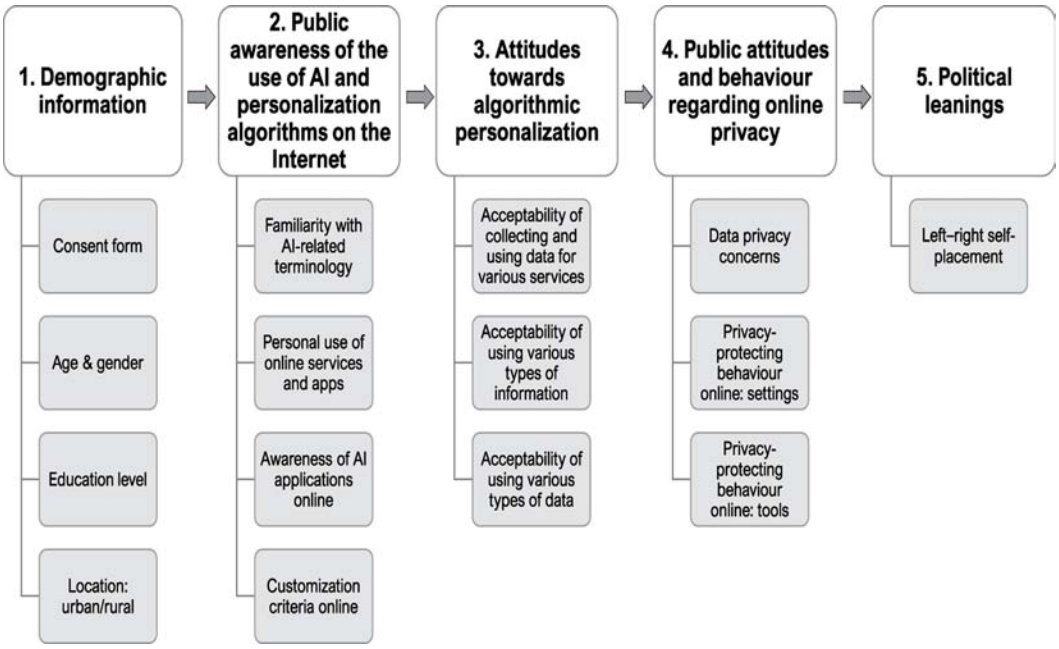

Fig. (1). Survey on artificial intelligence for AI algorithmic bias and manipulation in online environments [21].

The digital world is built on algorithms, which power social networking sites and search engines. They are also becoming more and more prevalent in our daily lives, influencing everything [7], from the way we spend our money to the quality of our medical care. Fig. (**2**) shows a few popular algorithms and how they are used in everyday circumstances:

CHAPTER 8

Automated Cyberattacks and Social Engineering

Gunjan Aggarwal[1,*], **Aryan Kumar Pandey**[1] and **Swati Singal**[1]

[1] *Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India*

Abstract: Social engineering attacks are a prevalent and cunning method employed by cybercriminals to exploit the very essence of human psychology and behavior. These attacks are becoming increasingly common and exploit human vulnerabilities. These attacks do not follow any specific methodology and are thus difficult to identify. This makes them highly efficient, easy to execute, and capable of compromising any organization. Scams based on social engineering are built around how people behave and react to situations of fear, excitement, curiosity, *etc*. Once an attacker understands the person's psychology, they can plan and influence the user effectively to believe in fake news, messages, *etc*. In addition, the attackers also exploit persons' lack of knowledge and awareness about cyber security and attacks. The attacker's goal is generally financial gain or to gain access to restricted areas or confidential documents. As a preventive measure, it is important to be aware of cyberattacks and how they work. To combat social engineering attacks, it is crucial to educate individuals and employees about the risks, enhance their awareness, and encourage healthy skepticism when dealing with unsolicited requests for information or actions. Technical security measures, like multi-factor authentication, the use of updated software and antivirus software, email filtering, *etc*., may help protect individuals or organizations from social engineering attacks, making it harder for cybercriminals to succeed in their manipulative endeavors.

Keywords: Cyber security, Cyberattacks, Deepfake, Social engineering, Phishing baiting, Tailgating, Waterhole.

INTRODUCTION

Social engineering is a technique to manipulate and exploit human behavior for money or to gain access to restricted areas or confidential documents. Social engineering attacks can take place through face-to-face interaction or through technical means of interaction or interaction through social media. Cybercriminals often use these techniques to trick naïve individuals into revealing personal information, disseminating malware, or granting access to systems that are

[*] **Corresponding author Gunjan Aggarwal:** Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India; E-mail: gunjan.aggarwal@sharda.ac.in

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

forbidden. By obtaining simple information such as name, associated organization, date of birth, school name, places visited, internet browsing history, *etc*., the attackers can easily plan to trick the user [1, 2].

Social engineering attacks have seen a dramatic surge within contemporary network environments, posing a significant threat to cybersecurity. These nefarious tactics are geared toward exploiting both individuals and businesses, coercing them into revealing invaluable and confidential information, all in the pursuit of malevolent objectives.

The reason why social engineering is successful is because of human psychology [5]. The attackers collect information about the target person and exploit their fear, excitement, anger, sadness, guilt, and curiosity to trick the person. Sometimes, they create urgency in situations by sending fake messages, and henceforth, the person clicks on fake links or reveals personal credentials.

Social engineering presents an escalating challenge to the security of an organization's networks, irrespective of the strength of their security in terms of firewalls, encryption protocols, intrusion detection systems, antivirus software, *etc*. Humans, by nature, are more inclined to place trust in fellow friends and colleagues as opposed to computer systems and other technologies. Consequently, they emerge as the most vulnerable element within the security framework. Malicious actors skilfully manipulate human interactions, targeting the psychological vulnerabilities of individuals in order to coerce them into divulging sensitive information or bypassing established security protocols. This underscores the critical role that human awareness and education play in fortifying cybersecurity defenses [3, 4]. In other words, we can say that *Social Engineering* comprises an array of deceptive methods that exploit human interactions, relying on psychological manipulation to induce security lapses or the release of confidential data.

This paper will provide the comprehensive automation of cyberattacks as well as social engineering techniques implemented, highlighting the unique methods through which attackers exploit human psychology for malicious gains. More basically, it introduces the social engineering attack life cycle with adequate detail on how attackers manipulate human emotions based on fear and curiosity in bypassing traditional security measures. It addresses the emerging challenges in the form of AI-driven phishing, deepfakes, and IoT vulnerabilities, with which evolving technology brings further sophistication to social engineering attacks. The novelty lies in the paper's focus on the integration of psychological manipulation with advanced technologies, such as AI, machine learning, and

quantum computing, in the context of cyberattacks that increase the complexity of detection and mitigation strategies.

The research contributions of the study are as follows:

Detailed Life Cycle Analysis

The study contributes an in-depth analysis of the life cycle of social engineering attacks, describing the stages from information gathering to execution, which helps in understanding the attacker's approach and identifying potential points of intervention.

Preventive Measures Framework

It proposes a structured set of preventive measures aimed at individuals and organizations, focusing on education, awareness, and technical solutions such as multi-factor authentication and anti-phishing tools. This practical framework is intended to enhance preparedness against social engineering.

Emerging Threat Landscape

By identifying future challenges like AI-driven social engineering, deepfakes, and IoT vulnerabilities, the paper contributes to the cybersecurity field by anticipating new forms of threats. It suggests that these emerging technologies significantly expand the scope and scale of social engineering risks.

Behavioral Analysis Integration

The study also delves into human behavior analysis, using probabilistic and graphical models to create user vulnerability profiles, a contribution that underscores the role of behavioral science in enhancing cybersecurity defenses.

Cybersecurity Awareness and Education Programs

Emphasizing the role of awareness and training, the paper highlights the need for continuous cybersecurity education tailored for both general users and specialized organizational environments.

Consequences of Social Engineering

Social engineering attacks represent a significant cybersecurity threat with potentially devastating consequences for both individuals and organizations. These attacks rely on manipulating human behavior rather than exploiting technical vulnerabilities, which makes them particularly effective and challenging to detect. When attackers gain access to critical data such as user passwords,

CHAPTER 9

Deepfake and Erosion of Trust

Preeti Dubey[1,*], Hoor Fatima[2] and **Pushpendra Kumar Rajput[1]**

[1] *Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India*

[2] *School of Computer Science Engineering and Technology (SCSET), Bennett University, Greater Noida, U.P., India*

Abstract: Deepfake technology's rapid growth has ushered in a new era of digital manipulation, which has led to serious worries about how it may affect people's ability to trust different aspects of modern society. This abstract provides a thorough examination of the various effects of deepfakes on trust, including how they affect media consumption, interpersonal relationships, and the integrity of social institutions. The emergence of deepfake technology has changed the digital content ecosystem and sparked worries about the decline in trust across a number of domains. With the use of complex algorithms for machine learning, deepfakes may produce incredibly lifelike and misleading multimedia content, such as pictures, audio files, and movies. This study examines the complex effects of deepfakes on media consumption, interpersonal relationship trust, and institutions of society. The authenticity of human communication in interpersonal relationships is challenged by the ease with which deepfakes can modify aural and visual clues. Relationships are built on trust, which is compromised when people struggle with the unknown of real communication. The psychological and social effects of deepfakes on interpersonal trust are investigated in this research. The consumption of media is another area where deepfakes have a significant impact. The legitimacy of information sources is called into doubt by the blurring of the boundaries between reality and fiction. The public's trust in internet and conventional media channels is eroded by misinformation spread through altered content. The study looks into how deepfakes affect media literacy, how misinformation spreads, and how this affects society's confidence in information.

Keywords: Democratic procedures, Genuineness, Integrity, Institutions, Openness, Political conversation, Public trust.

INTRODUCTION

The conventional notion of reality and authenticity in the digital sphere has been upended by the prevalence of deepfakes, which are powered by advanced machine learning algorithms. This introduction lays the groundwork by explaining how

[*] **Corresponding author Preeti Dubey:** Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India; E-mail: preetidubey.research@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

deepfakes can be used to create multimedia material that is both incredibly realistic and misleading. The main theme that emerges as we make our way through the complex web of interpersonal relationships, media environments, and institutional frameworks is the threat that deepfakes pose to the basic trust that is the cornerstone of our globalized society [1]. The authenticity of human communication in interpersonal relationships is challenged by the ease with which deepfakes can modify aural and visual clues. The foundation of meaningful connections, trust, is more vulnerable than ever as people struggle to distinguish sincere exchanges from staged ones.

As a secondary focus [2], media consumption turns into a battlefield where deepfakes conflate reality with fabrication. Public confidence in traditional media outlets and digital platforms is weakened as a result of the confusion surrounding the differentiation of manipulated content from reliable information. This essay explores the profound effects of deepfakes on media literacy, the spread of false information, and the resulting decline in public confidence in news sources. The study also looks into the wider effects of deepfakes on public figures and institutional integrity. The fundamental foundation of confidence in societal institutions and leadership is put in jeopardy by the possible abuse of this technology for financial, political, or social manipulation.

As we continue our investigation (Fig. **1**), it becomes clear that tackling the problems caused by deepfakes calls for a sophisticated comprehension of their ramifications. In an increasingly digital and linked world, interdisciplinary cooperation between engineers, legislators, and the general public is essential to creating effective policies that protect trust. By providing insights into the various ways that deepfakes contribute to the deterioration of trust and suggesting strategies for reducing their detrimental effects, this research seeks to advance our understanding of the subject.

LITERATURE SURVEY

This review of the literature explores the emerging area of deepfakes and how they affect the decline in trust in a variety of contexts. This survey, which draws from a wide range of academic works, synthesizes important findings, approaches, and viewpoints to offer a thorough grasp of the relationship between deepfakes and the fragile fabric of trust in social media, interpersonal relationships, and institutional trust in society.

The investigation starts with a review of early research that clarifies the workings and development of deepfake technology. Digital media studies, artificial intelligence, and computer science provide the foundation for understanding the

technical complexities involved in producing and distributing hyper-realistic modified information [1, 3].

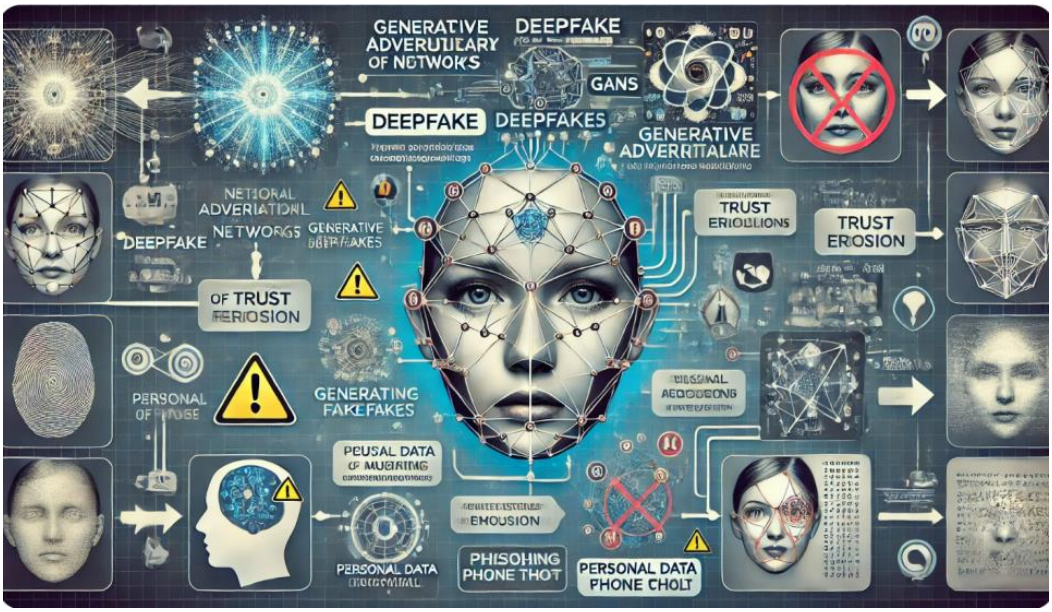

Fig. (1). Illustration of various areas exploring the process of deepfakes and their impact on trust.

Moving on to the domain of interpersonal relationships, the review of the literature examines psychological and sociological research examining how deepfakes affect the dynamics of trust [4]. Research on the cognitive dissonance brought on by artificial visual and aural cues illuminates the difficulties people encounter in recognizing real-life interactions, which in turn contributes to the breakdown of trust in interpersonal relationships [5-7].

The survey summarizes research on the impact of deepfakes on the spread of information in the context of media consumption. The debate about how deepfakes undermine conventional ideas of credibility and undermine public confidence in news sources and online platforms is informed by studies on media literacy, disinformation, and the dissemination of modified content [8, 9].

In order to comprehend the effects of deepfakes on public figures and institutional integrity, the survey also explores the fields of politics and communication studies. Research on the use of deepfakes as weapons for political influence and the effect this has on democratic processes sheds light on the weaknesses this technology introduces into a larger societal context [10].

CHAPTER 10

Ethical Implications of AI in Social Networks

Atul Kumar Rai[1,*] and **Neelaksh Sheel**[2]

[1] *Computer Science & Engineering, Kotiwal Institute of Technology and Professional Studies, U.P., India*

[2] *Moradabad Institute of Technology, Moradabad, U.P., India*

Abstract: The ethical implications of artificial intelligence (AI) in social networks encompass a spectrum of complex issues. Key concerns involve user privacy and data security, algorithmic bias leading to discrimination, transparency in AI operations, and the spread of misinformation. Additional ethical considerations include user manipulation, striking a balance between freedom of speech and content moderation, and addressing the impact of AI on emotional well-being. Inequities in AI access, user addiction, and the treatment of AI-driven entities are also pressing issues. The ethical challenges necessitate ongoing dialogue, transparency, and the development of ethical guidelines to ensure AI benefits users while mitigating harm and promoting fairness in social network interactions. Artificial intelligence machines demonstrate the remarkable capability not just to perceive, articulate, listen, process, and transcribe information but also to acquire these skills at a pace surpassing that of human counterparts. These advanced tools find application across industries, enhancing and automating various activities on the internet to improve overall efficacy. The main objective of the chapter is to highlight privacy, algorithmic bias, user manipulation misinformation, and emotional well-being. It emphasizes the need for ongoing dialogue, transparency, and the development of ethical guidelines to ensure that AI in social networks promotes fairness.

Keywords: Artificial intelligence, machine learning, chatbot, learning, perception, social media.

INTRODUCTION

Cognitive artificial intelligence (AI) deals with intelligent behavior by analyzing the outside environment and taking the best action decided by the machine according to the situation to some degree to achieve the goal. AI concerned with the task given to computing machines requires understanding, knowledge, perception, experience and cognitive abilities [1]. Present AI tools have the

[*] **Corresponding author Atul Kumar Rai:** Computer Science & Engineering, Kotiwal Institute of Technology and Professional Studies, U.P., India; E-mail: atulrocks@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

capability to train the machine regarding the power of understanding individual behavior, his/her personal interest, and preferences. AI machine possesses the remarkable capacity to not only perceive, articulate, listen, process, and transcribe information but also exhibit the ability to acquire these skills at an accelerated pace compared to human counterparts. These sophisticated tools and applications are being used in industries for enhancing and automating the efficacy of diverse activities on the internet.

A digital scientific study of the spread and control of social media disorder has evolved into a fundamental aspect of our daily existence. Individual consumers constantly engage with different social media platforms like Facebook, Twitter, LinkedIn, Pinterest, and Instagram. It is a major sector where marketers can hit both the roof performance and potential efficiency by using artificial intelligence. With this, consumer activities on social media and e-commerce websites are continuously being accumulated and analyzed. Currently, social media is being used to understand social behaviors and derive the inclinations of consumers by collecting information on day to day activities with the help of big data analyzing tools [2, 3].

ARTIFICIAL INTELLIGENCE GOALS

Artificial intelligence (AI) is the intelligence of machines given by engineers with the help of powerful algorithms. It is also the field of study in computer science and is widely used in industry, government, and science. Advanced web searches like Google, recommended systems (YouTube, Amazon, Netflix), Human Speech understanding (Alexa, Siri), Automotive Vehicle (Waymo), and Creative/ Generative tools (ChatGPT, AI art) are some prominent applications of AI [4].

In software development, the general problem of simulation has been broken down into sub-problems. Researchers expect an intelligent system to solve these sub-problems and keep the attention on the following:

Reasoning/problem-solving

To solve the puzzle problems or make logical deductions, researchers develop algorithms and work on step-by-step reasoning. By the late 1980s and 1990s, researchers had developed a method that dealt with uncertain or incomplete information and found solutions based on probability.

Knowledge Representation (KR)

KR or knowledge engineering allows AI to answer questions intelligently on the basis of real facts. It is used in content-based indexing, knowledge discovery,

clinical decision support, *etc*. Knowledge represents things as objects, their properties, categories, relationships between objects, events, state and time, effects and causes, and many more.

Planning and decision making

Within the realm of artificial intelligence, an 'agent' refers to any entity capable of perceiving its environment and initiating actions based on that perception in the outside world. The decision-making agent assigns a number of situations called utility. For every possible action, the agent calculates the expected utility and then chooses the best action for the outside world.

Learning

It is the training of programs that improves the automated execution of a designated task with optimal efficiency. *Unsupervised learning* analyzes the data, detects patterns, and creates predictions without the supervision of others. *Supervised learning* uses classification and regression techniques. It needs labelled input data for training the machine. *Reinforcement learning* chooses responses that are classified as “Good” and “Bad” actions of an agent. Agents are rewarded for good responses and punished for bad responses.

Natural Language Processing

It enables programs to write, read, and communicate in any human language, including Hindi, English, German, French, *etc*. Contemporary methods in deep learning techniques for Natural Language Processing (NLP) encompass advancements such as word embeddings. Since 2019, Generative Pre-trained Transformer (GPT) language models have emerged to demonstrate the ability to generate coherent text. It is anticipated that by 2023, these models will be able to achieve human-level performance in various real-world applications, including the bar exam, SAT, GRE, and more.

Perception

It is the capability of a machine to utilize responses from sensors, cameras, microphones, radar, and many more to presume the features of the outside world. Computer vision is used to analyze visual inputs and encompasses a range of tasks, including speech recognition, facial recognition, classification of images, and object recognition.

CHAPTER 11

Regulating Artificial Intelligence in Social Networks

Abha Kiran Rajpoot[1,*] and **Sana Anjum**[2]

[1] *School of Computer Science & Engineering, Galgotias University, Greater Noida, U.P., India*

[2] *Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, U.P., India*

Abstract: The growth of artificial intelligence (AI) in social media has brought significant improvements in user experience, content delivery, and personalization. But this also raises privacy concerns, ethical considerations, and the potential for algorithmic bias. This chapter highlights the urgent need to manage social intelligence by focusing on striking a balance between innovation and ethical considerations. While regulation is necessary, striking the right balance between supporting AI innovation and addressing ethical issues is critical. Regulators should promote creativity and technological advancement and support responsible AI development and deployment. Managing social skills is a complex task that requires thoughtfulness and balance. It is essential to strike a balance between new technologies and ethical considerations to make social relationships safe, fair, and beneficial for all. Lawmakers, tech companies, and civil society must work together to create regulatory frameworks that support responsible intelligence while maintaining critical engagement capability. Artificial intelligence (AI) in society requires a balance between innovation and ethics. This principle encourages greater transparency by requiring platforms to demonstrate smart strategies to improve user understanding and create accountability.

Ethical rules: They are important for fairness, diversity, and inclusion and aim to reduce the bias inherent in AI-driven content selection and recommendations. Privacy measures must be in place to protect user data from illegal AI-powered surveillance and ensure compliance with strict data protection laws. Fighting misinformation requires using algorithms to quickly and effectively combat false content generated by AI. The effectiveness of the framework is under constant evaluation and modification, enabling rapid changes in management models with the rapid development of artificial intelligence technology. Collaboration between governments, science and technology organizations, researchers, and civil society is essential to create policy changes that encourage innovation while supporting standard practices. Ultimately, this policy aims to support the artificial intelligence ecosystem in dialogue and improve relations while protecting people's interests and rights.

[*] **Corresponding author Abha Kiran Rajpoot:** School of Computer Science & Engineering, Galgotias University, Greater Noida, U.P., India; E-mail: akrajpoot@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

Keywords: Artificial intelligence, Digital marketing, Machine learning, Online advertising, PPC advertising, Social media marketing.

INTRODUCTION

In an era where the digital landscape intertwines with our daily lives, the role of artificial intelligence (AI) in shaping social networks has become undeniable. As AI algorithms take center stage, orchestrating content dissemination, shaping user experiences, and steering interactions within these digital realms, the need for a thoughtful and comprehensive regulatory framework becomes increasingly evident. This chapter sets the stage for a profound exploration of the complexities and necessities of regulating AI within social networks. This chapter explores the complex influence of AI, focusing on its role in content curation, user privacy, and the ethical challenges it presents. By analyzing the current landscape, it emphasizes the urgent need for transparent, ethical, and user-centered AI deployment. It sets the stage for an in-depth examination of the strategies, challenges, and essential measures required to govern AI in social networks effectively. Through this exploration, we embark on a journey to establish an informed and responsible approach that safeguards user rights, fosters innovation, and cultivates a digital ecosystem that thrives on ethical AI principles.

LITERATURE SURVEY

Social intelligence management provides an overview of the current state of research and debate in this field. It helps identify key issues, challenges, and insights. Below is a literature review of social intelligence management, including research and findings:

Privacy and Data Protection

The study [1] highlighted the importance of regulatory controls to protect customer privacy in the context of intelligence-driven relationships. They discussed the risks associated with data collection and emphasized the need for stricter data protection.

Algorithmic Transparency and Bias

The study [2] provided a comprehensive review of algorithmic transparency and bias in networking. They emphasized the need for transparency management in the AI algorithms used for recommendations to address issues of bias and discrimination.

Content Analysis and Speech Development

Authors examined the problems of AI-based content moderation and social media discrimination. They discussed the balance between freedom of expression and content moderation and suggested that there should be clearer rule [3].

User Authorization and Control

The research [4] user authorization in intelligence-based relationships. They believe regulations should focus on giving users control over their experience, allowing them to personalize content and privacy.

Ethics and Responsibility

The study [5] conducted a survey of social network users to understand their expectations regarding the use of artificial intelligence. The results of the research show that social relations desire to adopt and follow ethical principles in the use of intellectual property.

International Cooperation and Standards

According to the study [6], the authors examined the importance of international collaboration in managing social intelligence. They emphasized the need to harmonize regulatory frameworks to address the cross-border nature of these platforms.

Integrity and Accountability

The authors [7] discussed policy issues regarding the integrity and accountability of AI algorithms. They issued a policy to ensure that social media use fair and responsible intellectual processes for their actions.

Information Security and Compliance

The study [8] described the intersection of information security and compliance management in the context of intelligence-driven relationships. They emphasized the need for strong cybersecurity measures and compliance monitoring to protect user data.

AI Innovation and Ethical Considerations

A study [9] explored the balance between supporting AI innovation and solving ethical issues. They proposed a framework for regulators to support AI development that is responsible for hindering innovation.

CHAPTER 12

User Empowerment and Digital Literacy

Pooja Chaudhary[1,*] and **Kajal Gupta**[1]

[1] *CSE (Data Science), Raj Kumar Goel Institute of Technology, Ghaziabad, U.P. India*

Abstract: Youth must be encouraged to take the lead in community development by providing them with programs that build their competence and capacity in response to the demands of the age of digital technology. Youth empowerment through instruction in digital literacy was the goal of the PPM program. Its objectives were to raise youth knowledge of and comprehension of ITE Law, enhance the youth's proficiency in utilizing information technology for educational purposes, and elevate the youth's aptitude in utilizing information technology for conducting online business. The three strategies used in this PPM program's implementation were young capacity building through seminars, digital technology training, and web-based company advising. Through training sessions, seminars, and mentorship in the application of computer technologies, the PPM strategy was executed effectively. PPM exercises improved the youth's comprehension and knowledge of ITE Law, as well as their capacity to use a variety of online business and learning resources, including information technology.

Keywords: Comprehension and Knowledge of ITE Law, Digital literacy, Educational and Online business strategies, ITE law, Objectives, PPM program, Web-based company mentorship, Youth community empowerment.

INTRODUCTION

The modern world is changing quickly, and digital skills are becoming essential for success in both personal and professional arenas. Conventional wisdom was upended by the COVID-19 pandemic, which made people use digital tools for online learning, distant work, and virtual communication. As a result, there has occurred an unparalleled increase in the need for digital skills, as businesses are looking for qualified applicants who can quickly adjust to the ever-changing digital landscape.

There is a low culture of technological literacy among Indonesians. Low passion for reading and writing are examples of how the low literacy environment

* **Corresponding author Pooja Chaudhary:** CSE (Data Science), Raj Kumar Goel Institute of Technology, Ghaziabad, U.P. India; E-mail: poojafds@rkgit.edu.in

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

manifests itself in day-to-day life. Individuals like to watch TV, listen to music, *etc*. Their identity as learners may be weakened by the low literacy environment in this age of technology and the internet. In today's world of quick and unprecedented progress in communication and information technologies, a low literacy culture can lead to stuttering. It is simple for the general population to get and spread false information. Direct and indirect causes of situations like bullying, fraud, and pornographic acts are low literacy rates [1]. Individuals who are not tech-savvy and who are not aware of the information presented by the media may be the source of a number of issues, including psychological and physical issues. When students use digital media carelessly, it can result in consumptive behaviors, including binge-watching TV, playing video games online or off, using social media without realizing when to stop, visiting pornographic websites, and accessing other pointless content. In order to promote autonomy, radicalism, and a greater tendency to exist in a virtual environment than the physical one, the majority of students are more inclined to absorb media messages and incorporate them into their self-formation. A lot of students think about what they see themselves in; therefore, they see themselves as singers or other characters in everything from their daily conduct to their hair and clothing choices [1]. Digital literacy refers to a person's interest in, aptitude for, and attitude toward using technological and digital tools for information management, analysis, and evaluation, as well as for communication with others and the acquisition of new knowledge. By these abilities and attitudes, they can participate effectively in society. Digital knowledge is an approach that a person actively uses to acquire and interpret the messages that media conveys. One essential component of contemporary media, digitalization, is referred to as “digital literacy” [1]. Regarding the growth of digital literacy, the digital world gave rise to two opposing perspectives. There are opportunities and challenges associated with the development of digital resources and channels for information. One issue that has come up is the enormous number of young people—roughly 70 million—who use the internet. They spend about five hours a day on the internet, whether on laptops, desktop computers, or mobile phones [2]. In the contemporary digital world, parents' potential for involvement is tremendously influential. It is influenced by the idea that digital literacy is a life skill that encompasses not just the use of information and communication technologies tools but also learning and thinking in a critical, creative, and inspirational way as a digital competency [3]. Digital skills are essential for both individual achievement and the advancement of the country in the digital age, which ushers in a new era of opportunities and challenges. Adopting digital literacy is now a must, not an option. All parties involved—governments, academic institutions, businesses, and individuals—must support and encourage digital education as a whole, which

opens the door to a flourishing digital society in which every person has the ability to realize their greatest potential in the age of technology.

People's mindsets are being significantly impacted by the extraordinary political, financial, social, cultural, and technical developments that the globe has recently witnessed. People are being forced to adapt and give themselves more power, so they may use everything at their disposal to take greater command of their lives as a result of the general sense of uncertainty. More independent and transparent behaviors are being produced by this mentality change, and this has an effect on how consumers make decisions about what to buy and interact with media and brands.

People are really interested in seeing how generative AI, such as ChatGPT, can transform education and content production. They are also intrigued by the possible advantages of worlds that are virtual, such as the metaverse, which builds an entire ecosystem using digital goods and currencies. With the help of these technologies, we are entering a new era where customers have more control and can navigate a future with more advanced technology. But even with the widespread use of devices and the internet, there is a gap in the world because of economic, social, and infrastructure disparities. According to a Mindshare study, one in two individuals worldwide believe that a shortage of digital resources is more important during a financial crisis.

For Customers To Navigate Uncertainties And The Economic Crisis, Digital Knowledge And Empowerment Are Essential.

Rising inflation and difficult financial circumstances for people everywhere make digital empowerment essential for consumers to successfully manage the crisis and get the information and skills necessary to advance (Table **1**).

Table 1. Representation of the number of people and their beliefs regarding digital literacy.

Percentage	Beliefs
57%	Essential Commodity
56%	Confident and Control
65%	Societal Progress

- A world without the conveniences that digital technology provides is unimaginable for 57% of people [4].
- In these uncertain times, 56% of people think using digital technologies gives them a sense of increased confidence and control over their lives [4].

CHAPTER 13

AI-Driven Solutions for Filtering Unwanted Posts from Online Social Networks (OSN)

Sachin Jain[1,*], Sudeep Varshney[2] and **Tejaswi Khanna[3]**

[1] *Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India*

[2] *Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India*

[3] *Department of Computer Science and Engineering, IMS Engineering College, Ghaziabad, U.P., India*

Abstract: There has been an explosion in the popularity of OSNs in recent years. Users can communicate and share any data through these services. The primary drawback of these OSN services is the invasion of the user's privacy. For precise filtering outcomes, we employ sample matching and textual content class sets of rules. We advocate for a system that gives OSN users complete editorial control over the content of their wall posts. There may be a grey area in which the usage of rule-based mobile devices permits customers to personalize the filtering process applied to their user profiles. A learning system can automatically label messages to aid with content-based filtering keywords: online social networks, filtering rules, devices, content-based filtering, and system learning. Globalization is reaching a significant level. In this study, we propose a more robust filter in PHP, based on the Validation Laravel framework, to circumvent the insufficient protections offered by OSN. We sort messages into desirable and unwanted groups in the first stage. In the second stage, spam messages are again sorted by kind. Both communications and users might be banned from being sent or received. If a user is blocked, they cannot post again until the blocklist is removed.

Keywords: Artificial intelligence, Clustering, Message filtering, Machine learning, Online networking, Security, Social network.

INTRODUCTION

There is a significant and unique impact on today's social media, such as many social websites like Facebook, Google, Plus, Twitter, *etc*. Millions of people can talk to their friends and relatives worldwide through these social sites. Artificial intelligence (AI) has revolutionized the functioning of Online Social Networks

* **Corresponding author Sachin Jain:** Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India; E-mail: sachincs86@gmail.com

(OSNs), enabling personalized experiences, efficient content moderation, and targeted advertising. However, this transformation has also exposed several challenges, often referred to as the "dark side" of AI in social networks. Social sites have become a significant part of the digital world worldwide. It has made a profound impact on people's lives. It has completely changed the way people live and communicate with each other. Online social networking (OSN) is primarily human. The primary use of OSN is to calculate unique types of content through textual content, video, audio, hyperlinks, *etc*. Online social networking is a medium where people can share all the information about themselves and build social relationships with people. They share their photos, videos, locations, and real-time conversations with people they do not know much about.

Social links manage a range of services with extensive links, such as finding new people with the same interests. OSN is a core web-based service that allows each person to create their profile users list, add all their friends, family, and relatives, and connect with famous social networking services, mainly to connect with people who Use Facebook, Google+, Twitter, and YouTube. There are many types of social sites around the world [1], according to Facebook statistics. This popular networking website has over 750 million users [2]. It interacts with over 900 million items, such as a Facebook page with many people. Still, many people will never consider these facts, nor will they create a situation of controversy because logging in on Facebook has become a routine of daily life for most people. The statistics have raised many questions. First, "What did people value in their daily routine before Facebook, that is, what was their routine? We have an all-site; when it is not there, what will people do without it [2]?"

How do we react when we suddenly disappear from Facebook for a day? Then do people care about us? Great organizations like Single Grain have tried to find answers to these questions, which are obtained through informative info-graphic mediums that let us identify the role Facebook plays in our lives [2]. The simple answer is that people have become increasingly addicted to social media these days.

The main reason for creating a social site is to create a social network so people can meet and find new people. Almost every social site user can set up a network to find new people. Users can find new people from all over the world, or they can focus on specific social people through the social site.

Friends can be searched even in certain places. Users make as many friends as they can preserve. It all depends on the user. Everyone has a different approach to making friends online [3].

Here are some real-world examples of AI-driven solutions for filtering unwanted posts from online social networks (OSNs):

Facebook's DeepText and RoBERTa Models

Facebook uses DeepText, a deep learning-based text understanding engine, to filter spam, hate speech, and other unwanted content. They also utilize RoBERTa (a variant of BERT) for understanding the context of posts, helping detect subtle nuances of the harmful or abusive language across multiple languages and cultural contexts [3].

Instagram's Offensive Content Detection Using AI

Instagram employs machine learning algorithms to detect offensive language, bullying, and harassment in posts and comments. It uses NLP models to assess both captions and comments, providing warnings to users before they post potentially offensive content and removing comments that violate policies.

Twitter's Machine Learning for Abusive and Spam Content

Twitter uses machine learning models to detect and remove hate speech, harassment, and spam in real time. Their models analyze textual content, images, and user behavior to identify accounts promoting abuse, misinformation, or spam, often flagging content before users report it [4].

YouTube's Machine Learning Models for Detecting Harmful Content

YouTube employs machine learning to detect inappropriate videos and comments, including spam, hate speech, and misinformation. Algorithms analyze video metadata, transcriptions, and comments, automatically flagging content for human review or direct removal based on its severity [5].

LinkedIn's Spam and Scam Filtering System

LinkedIn uses AI to monitor and remove spam, scams, and other malicious content from its network. Machine learning models detect patterns associated with unwanted content, such as unusual posting frequency or repetitive language often used in spam messages, helping to maintain a professional environment [6].

RESEARCH OBJECTIVES

Here are four key objectives of AI-driven solutions for filtering unwanted posts from online social networks (OSNs):

CHAPTER 14

The Dark Side of Digital Surveillance: India's Cybersecurity in the Age of Artificial Intelligence

Ruchi Patira[1,*], **Rajani Singh**[2] and **Manoj Singhal**[2]

[1] *Department of Computer Science and Engineering, World College of Technology and Management, Gurgaon, Haryana, India*

[2] *Department of Information Technology, GL Bajaj Institute of Technology and Management, Greater Noida, Uttar Pradesh, India*

Abstract: This article provides an overview of cyber security, a topic that has risen in importance since the end of the Cold War due to a confluence of technological advancements and shifts in geopolitical dynamics. The paper uses securitization theory to conceptualize cybersecurity as a separate industry with its own unique set of risks and reference points. It is believed that the collective referent objects of "the state", "society", "the country", and "the economy" provide "network security" and "individual security" their political significance. Through hypersecuritization, daily security procedures, and rectifications, these referent objects are formulated as threats. Next, a case study of what has been called the "first cyber war" against Estonian governmental and commercial organizations in 2007 is used to demonstrate the theoretical framework's practicality. In the realm of IT, cyber security is a crucial component. One of the greatest difficulties now is ensuring the safety of sensitive data. Although the concept of cyber security is more important, it remains elusive. The notions of privacy, information sharing, intelligence collection, and monitoring are often muddled with it in improper ways. This study argues that proper risk management of information systems is essential for adequate cyber security. Threats (who is attacking), vulnerabilities (how the assault will be carried out), and effects (what will be damaged) are the three determinants of the risks involved in any attack (what the attack does). In terms of cyber security, the government's responsibility extends beyond only safeguarding its own networks to also include helping to safeguard private networks.

Keywords: Cybersecurity, Cyber risk, Hypersecuritization, Information security, Network security.

[*] **Corresponding author Ruchi Patira:** Department of Computer Science and Engineering, World College of Technology and Management, Gurgaon, Haryana, India; E-mail: rpatira@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

INTRODUCTION

Internet crimes are a relatively new phenomenon. In accordance with the Information Technology Act, this term refers to any illegal behavior that is conducted *via* or facilitated by the use of electronic devices such as computers, the Internet, or other similar technologies. In today's India, cybercrime has become the most common kind of crime and has a terrible impact on society. In addition to wreaking havoc on people's lives and budgets, thieves are sometimes able to keep their identities under wraps. Criminals with technological expertise use the internet to engage in a wide range of unlawful operations. Suppose we expand the definition of "cybercrime" to include any wrongdoing in which a computer or the internet is used in any way (either as a tool or a victim). In that case, we obtain the following [1]. While the phrase "cybercrime" may have a judicially construed meaning in certain Indian court rulings, it lacks a formal legislative definition. The root of the unstoppable evil that is cybercrime lies in the abuse of our ever-increasing reliance on technology. The widespread use of computing and related technologies has become an urgent need for many people. This medium is both limitless and immeasurable. The internet has both positive and negative effects on our lives [2]. New forms of cybercrime include acts like cyberstalking, cyberterrorism, email spoofing and bombing, cyberpornography, cyberdefamation, and so on. If they are carried out *via* a computer or the Internet, even seemingly "normal" crimes might be considered cybercrimes. For example, A series of big data breaches were observed in India in the monetary segment, an ATM malware attack, and a phishing attack on the state of the popular banks of India such as State Bank of India and Punjab National Bank. The breaches led to losses of customers' money as well as indicated the need for better enforcement of laws and policies on security in financial organizations. These examples show that threats are still imminent in the Indian financial market and that cybersecurity regulation is indispensable for protecting financial information.

DEVELOPING TRENDS IN CYBERCRIME LITERATURE SURVEY

Everyone who uses a palmtop or a microchip today would be shocked to learn that the first functional computer was constructed in the 1950s when such devices were impractically large (they required a full room) and costly to run. Most people did not understand how these computers worked, and only a small number of persons with specialized understanding had direct access to them. Until IBM came along in 1981 with the introduction of their standalone "personal computer", the benefits of easy access to and manipulation of large amounts of data had been available to only a select few. At the turn of the 21st century, personal computers in India became more reasonably priced and widespread [3]. After WWII, the US Department of Defense had the notion of creating a network that could function in

times of tragedy or conflict and securely transfer information; this was the genesis of the Internet.

ARPANET was the first network, and advancements in technologies like TCP/IP, the WWW, and hypertext led to its meteoric rise to prominence throughout the globe. As the Internet expanded, as shown in Fig. (**1**), so did the quantity and quality of available data. No one, however, could have predicted the possibilities the internet would open up for cybercriminals at the time. Internet service in India was first provided by the government-owned Videsh Sanchar Nigam Limited (VSNL) in 1995; the monopoly of VSNL was broken, and the market was opened to private operators in 1998 [3]. Even while just 0.1% of the population was online then, that number has now grown to 33.22%, making India the second most-populated nation online after China.

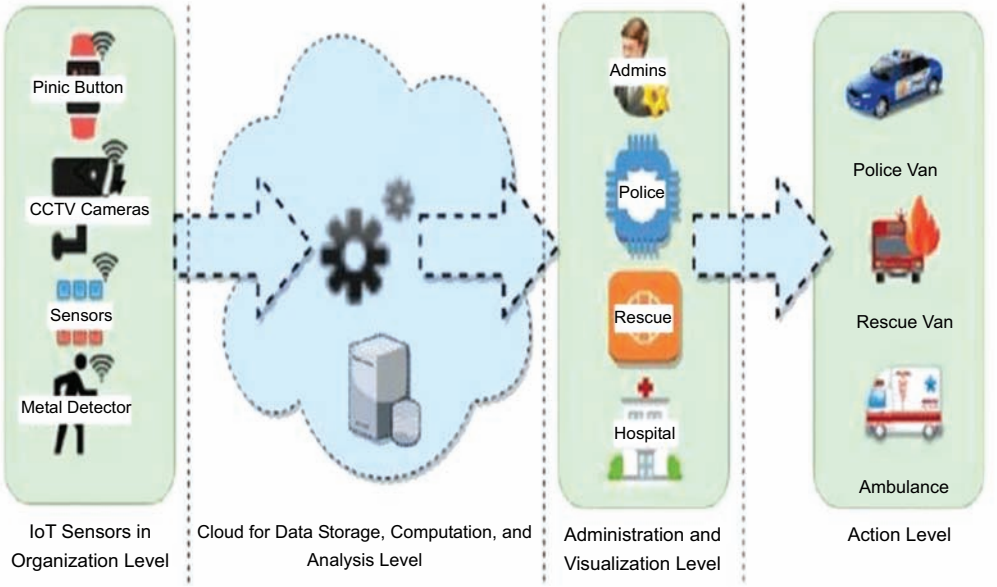

Fig. (1). Smart Security Framework [4].

CYBERSECURITY RISK MANAGEMENT

Threats (who is attacking), vulnerabilities (how the assault will be carried out), and effects (what will be damaged) are the three determinants of the risks involved in any attack (what the attack does). It is widely agreed that one of the cornerstones of reliable cyber security is the control of risks to data and computer networks.

CHAPTER 15

Framework to Uncover Threats in Social Networks Through Network Packet Visualisation

Prashant Upadhyay[1], Preeti Dubey[1], Amit Upadhyay[1] and **Nikiema Flavio[1]**

[1] *Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India*

Abstract: With the increasing volume and complexity of network traffic in social networks, extracting meaningful insights from this data has become increasingly challenging. This paper presents a lightweight approach for analysing network traffic for social networks that enables the identification of patterns and anomalies that may indicate malicious activity. The paper starts by discussing the importance of network traffic visualisation and the challenges associated with it. It then provides an overview of the key components of network traffic data and various visualisation techniques that can be used to gain insights into network behaviour. The focus is on lightweight visualisation techniques that can be used to analyse network packet data for threat detection. Time series plots, scatter plots, heatmaps, and network graphs are some of the visualisation techniques that can be used to identify patterns and anomalies in network traffic for social networks. The lightweight nature of this approach enables efficient processing and analysis of large and complex datasets. In conclusion, analysing and visualizing network packet data is a crucial technique for identifying potential security threats, and a lightweight approach can enable efficient processing and analysis of large and complex network traffic of social networks. By using the techniques and tools presented in this paper, network administrators and researchers can gain valuable insights into network behaviour and identify potential security threats.

Keywords: Analysis, Network, Network traffic, Social network, Threat hunting, Visualisation.

INTRODUCTION

The exponential growth of the internet has resulted in a massive increase in the volume of network traffic in social networks. Artificial intelligence in social networks unveils unseen vulnerabilities, exposing hidden dangers. With this increase in network traffic, there is an ever-growing need to analyse and understand network behaviour [1]. Network traffic visualisation has become a

* **Corresponding author Prashant Upadhyay:** Department of Computer Science & Engineering, School of Engineering & Technology, Sharda University, Greater Noida, U.P., India; E-mail: prashanttheac@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

crucial approach for achieving this goal. It allows network administrators and security professionals to identify network anomalies, monitor network performance, and detect potential security threats [2]. Visualisation techniques provide a way to represent complex network traffic data in a visual format, making it easier to understand and analyse [3]. Network traffic visualisation is a multidisciplinary field that combines computer networking, data analysis, and visualisation techniques [4]. Over the years, several approaches and techniques have been developed to visualise network traffic, including commercial approaches and open-source approaches. In this paper, we present an approach for visualizing and analysing network packet data for threat detection. We describe the key components of network packet data and explain how they can be visualised. We also discuss several network packet visualisation techniques and how they can be used to gain insights into network behaviour [5]. Our approach is designed to be lightweight and efficient, making it easy to deploy and use for network analysis. Our approach is based on offline analysis of network packet captures. We first extract key information from the packet headers, such as source and destination IP addresses, protocol type, and port numbers. We then analyse this information to identify patterns and anomalies in the network traffic. To visualise the network packet data, we use a range of visualisation techniques, including time series plots, scatter plots, heatmaps, and network graphs [6].

Combining offline network packet analysis with visualisation can greatly benefit network specialists in their analysis of network traffic data. Visualisation provides a powerful way to understand and interpret complex data sets, allowing network specialists to quickly identify patterns and anomalies in network traffic that may indicate potential security threats [7]. Visualisation can also help to reveal trends and patterns that may not be immediately apparent from raw network data. Moreover, visualisation can help network specialists to communicate their findings more effectively to non-technical stakeholders [8]. By presenting data in an easily digestible format, visualisation can help convey the severity of a security threat and the potential impact it may have on an organization. In conclusion, visualizing and analysing network packet data are powerful approaches for detecting potential security threats in network traffic. Our lightweight approach provides a flexible and efficient platform for network administrators and security professionals to gain valuable insights into network behaviour and identify potential security threats. By using the techniques and approaches presented in this paper, network specialists can improve network security and prevent cyberattacks on social networks.

LITERATURE SURVEY

Network traffic visualisation is an important task in network monitoring and management, and there have been many papers published on the topic of creating tools for visualizing network traffic. In this section, we highlight the different approaches used in those papers alongside their strong points and limitations in Table **1**.

PROPOSED METHODOLOGY

The approach presented involves the development of a lightweight framework that aims to simplify the analysis workload of network analysts and expedite the analysis process by offering clear and concise representations. The network traffic visualisation tool architecture consists of four main components that work together to capture, analyse, and visualise network traffic data. The network interface captures the data from social networking websites like Facebook, the packet sniffer analyses it, the network traffic visualisation tool generates visualisations, and the visualisation interface displays them to the user. This architecture provides a powerful and flexible framework for monitoring and managing network performance, security, and compliance. An overview of the entire process, from the collection of the network data to the construction of the visual representations, is shown in Fig. (**1**).

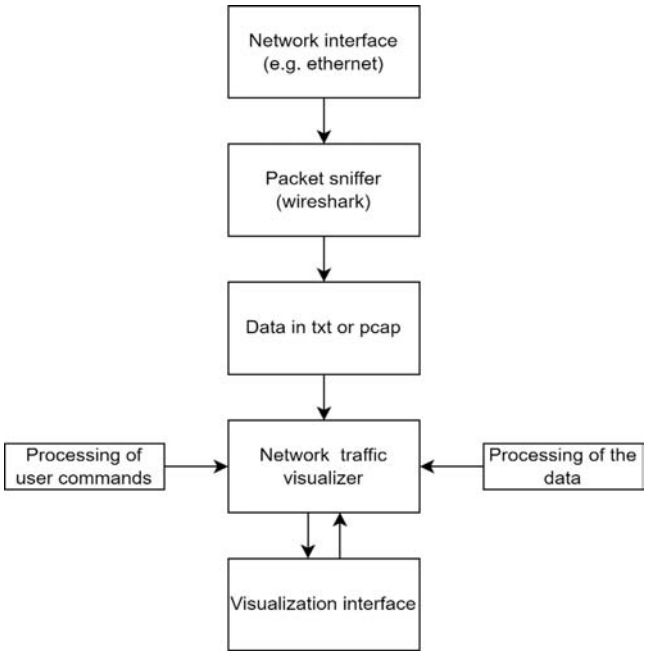

Fig. (1). Overall process of visualisation.

CHAPTER 16

AI's Psychological Impact on Users in Social Networks

Pawan Kumar[1,*], Rupa Rani[1], Deepika Yadav[2] and **Mandeep Singh[3]**

[1] *Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad. U.P., India*

[2] *Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, Delhi, India*

[3] *School of Computer Science Engineering, Bennett University, Greater Noida, U.P., India*

Abstract: Artificial intelligence (AI) is widely spreading daily in our daily communication, with some positive and negative impacts. The inclusion of AI in social media has several advantages and disadvantages and has a psychological impact on users' lives. The research study aims to investigate the harmful psychological impacts of AI on users using social media, which are discussed theoretically for enhancing and improving our social lives through social interactions of users, as well as sharing their personal life experiences or events. However, despite positive impacts, there are some negative concerns also. The research study focuses briefly on all the psychological impacts of AI on society, users, and social networks and defines all the challenges and applications of using AI in social media. AI algorithms deliver personalized content of data based on user recommendation and enhance connection and user access time on social media, but excessive access to social media has significantly high impacts on the mental health of users and results in more stress on the mind and pressure to compare themselves to others, thus increasing sadness and isolation.

Keywords: Artificial intelligence, Algorithm influence, Mental health, Psychological impact, Social networks.

INTRODUCTION

Communication is an activity through which one can read the psychology of human beings and can help to build strong human relationships and also make perceptions of others. Through strong social communication, we can achieve cooperative outcomes. Social media communication is different from old communication media such as TV, newspapers, and radio signal broadcasting.

[*] **Corresponding author Pawan Kumar:** Department of Computer Science & Engineering, Ajay Kumar Garg Engineering College, Ghaziabad. U.P., India; E-mails: drpawancse@gmail.com, rupachoudhary2010@gmail.com

Rupa Rani, Prashant Upadhyay, Rohit Sahu, Satya Prakash Yadav & Hardeo Kumar Thakur (Eds.)

The latest social media communication technology based on a dialogic transmission approach is in which many sources of information are available to many receivers; on the other hand, in old traditional communication technology, only a single source of information is available to many users, and it works on a monologic transmission approach. For instance, a single newspaper is distributed to many users or subscribers in the same way a radio station broadcasts the same signal or programs to an entire city.

Nowadays, social media has become a very interactive technology for virtual human communications, and it provides the facility for resource sharing and creation (such as new ideas, thoughts, images, and some other form of expression) to all virtual communities and social networks. There are several online platforms available through which users can create and exchange their content, participate in social networking, and easily access user-generated data content, like video, audio, text posts, digital photos, etc. Social media also plays a very vital role in developing a strong online social or digital network by connecting different profile users. Users access social media platforms through mobile devices and various web-based applications, and all these platforms permit individual users or communities to exchange, create, share, discuss, and access user-generated content. Social media is also very helpful for the promotion of movies, people, ideas, companies, products, *etc*. There are several online social media platforms available in which more than 100 million users are registered. Some popular online social media platforms are Twitter, ShareChat, Facebook, Instagram, Linkedin, QZone, *etc*., and some popular platforms that are used as social media services are YouTube, Telegram, WhatsApp, Snapchat, *etc* [1, 2].

Social media has now become an integral part of our daily life routine, and billions of people are sharing their thoughts or views in the form of text, video, or images on various social media platforms such as Facebook, *etc*. AI algorithms help to analyze this data and user behavior and deliver appropriate personalized content to each specific user. By analyzing the engagement of users by posting their pages or content, AI easily identifies content patterns and makes appropriate recommendations for new suitable content as per the interest of those users. This complete process is known as content curation, and it keeps the users more engaged on social platforms and makes them spend more time on the platform [3].

AI plays a vital role in identifying and removing harmful or abusive content that has a very significant effect on social network platforms. Presently, social network platforms are facing scrutiny due to their inability to police content, which leads to the spreading of hate speech, useless misinformation, and other dangerous content. With the help of AI algorithms, social media platforms easily, quickly, and efficiently identify the problem and then remove the content that is

harmful; thus AI tools help reduce the harm. Overall, AI plays a very significant role in social media networks by helping them provide personalized content and also ensure a saferand more positive online experience for users.

The book chapter aims to recognize the critical role of the potential psychological impacts of AI on users in social networks and how it affects user lives. The chapter broadly focuses on identifying the harmful impacts of AI and how to eliminate and ensure that everyone in society can benefit from AI technologies to the greatest possible extent. The proposed approach summarizes how the inclusion of AI in the field of social networks has made a new revolution. It deeply focuses on how AI psychology impacts a user's life. The inclusion of AI in social networks helps users make social decisions easily, like the generation of captions, the creation of images and videos, the generation of new ideas, and content planning for new strategies, customer support, *etc*. The book chapter also highlights all the positive and negative impacts of AI on users, along with the applications and challenges of using AI in social networks. The chapter also concludes all the challenges and applications of using AI in psychology.

The chapter is comprised of five sections. The first section of the book chapter discusses the introduction. The second section of the book chapter consists of the background of the chapter. This section includes the impact of AI on users and social networks and describes all the features and drawbacks of AI along with its positive and negative impact on inclusion on social networks. The third section of the book chapter describes the AI's psychological impact on users in social networks. The fourth section of the book chapter concludes future work, and the final section contains references.

BACKGROUND

As we know, AI plays a very vital role in the field of social networks, and it highly affects the lives of users. The integration of AI with social media enhances the experience of users by moderating organic data and content advertising. It also shows where the interest of users lies. AI also helps the social network to enhance its reach in terms of users, and now more people are connected to social networks and share their thoughts. Meanwhile, AI is used as a powerful tool for marketing products that help in enhancing businesses. It also helps in new content generation and the monitoring of social media and ad management. The inclusion of AI in social networks has brought a new revolution in the lives of users. It also highly affects society and the behavior of users. This section contains how AI affects society and the behavior of users and also focuses on all the positive and negative impacts of AI on users in the field of social networks [5, 6].

CHAPTER 17

Confronting the Dark Side of AI and Its Impact on Social Networks

Pawan Kumar[1,*] and **Amit Upadhyay**[2]

[1] *Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India*

[2] *Department of Computer Science and Engineering, Sharda University, Greater Noida, U.P., India*

Abstract: In a world where virtual interactions and digital connections rule the roost, the deep and often frightening social landscapes are being profoundly altered by the hidden complexity of artificial intelligence (AI). Explore "Uncovering the Dark Side of AI in Social Networks" to take a trip through the pages and discover the hidden stories of the digital world. The book provides a thorough knowledge of the intricate interactions between artificial intelligence (AI), social networks, and human behavior by fusing theoretical analysis with real-world case studies. Additionally, it provides doable advice on how individuals, governments, and tech corporations may encourage a more useful and ethical use of AI in the context of social networks. The book attempts to create a meaningful dialogue and increase public awareness of the possible risks related to artificial intelligence in social networks. By exposing the negative aspects of AI, it hopes to inspire people, decision-makers, and tech innovators to assess present procedures critically and take proactive steps to resolve the problems found. The authors intend to foster a more ethical and responsible approach to the development and deployment of AI algorithms within social networks.

Keywords: Challenges, Dark side of AI, Digital connection, Development and deployment of AI algorithms, Machine learning, Social networks.

SUMMARIZATION

Chapter 1 defined AI and its introduction. Social networks have a huge impact on our lives, transforming communication, information exchange, and social interaction. While they provide unquestionable benefits such as creating connections, community, and different opportunities, they also create issues such as misinformation, cyberbullying, violation of privacy, and mental health [1]. Moving forward, it is critical to solve these concerns through collaboration among

* **Corresponding author Pawan Kumar:** Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, U.P., India; E-mail: drpawancse@gmail.com

technology companies, governments, and individuals, ensuring that social networks are used ethically and responsibly, increasing good impact while avoiding potential drawbacks. Artificial intelligence (AI) has unquestionably become a vital force in the social network landscape, substantially altering user experience in a variety of ways. AI has revolutionized the way users engage with and consume information on various platforms, from personalized content streams to automated content creation. Its success in advertising and marketing has resulted in enormous benefits for both organizations and users since it provides tailored campaigns and relevant content. Furthermore, AI-powered chatbots and customer service solutions have improved user interaction and problem resolution, offering support 24 hours a day, seven days a week, and optimizing operational efficiency.

But even with all of the benefits, AI's presence on social networks also means that any possible drawbacks must be carefully considered. Problems such as discrimination and algorithmic bias have the potential to exacerbate already-existing disparities and unfairly disfavor particular user groups. Because of the ethical and legal issues raised by the broad collection and use of user data, concerns about data security and privacy are also quite important. AI-powered automation also carries the possibility of job displacement, which might affect those in customer service, content moderation, and other social media-related professions. Finally, to guarantee moral decision-making and reduce the possibility of unforeseen consequences, greater accountability and openness are required due to the opaque nature of many AI algorithms.

As we all know, there are two sides to the use of AI in social networks. Although its indisputable advantages have revolutionized platform efficiency and user experience, its possible risks and difficulties necessitate cautious thought and appropriate application. To maximize AI's enormous potential while reducing its drawbacks, technology companies, legislators, and users must work together going ahead. We cannot guarantee a future in which artificial intelligence (AI) improves everyone's social media experience by promoting inclusion, safety, and user empowerment unless we concentrate on responsible development, ethical use, and transparency.

Chapter 2 discussed social network vulnerabilities, including misinformation, manipulation, *etc*. Even though social networks have many advantages, using them securely necessitates being aware of the inherent security dangers [2]. These include susceptible third-party apps, phishing and malware assaults, and fake accounts, which generate misinformation. You may greatly lower these risks and completely utilize social networks without compromising by being cautious when clicking links, keeping your passwords secure, and properly adjusting privacy

settings. Recall that everyone must practice online safety, so having a happy and safe social media experience depends on being careful about what you publish and keeping up with new dangers.

There is a serious and developing threat to cybersecurity [2] from the use of AI to exploit weaknesses. Artificial intelligence (AI)-powered assaults can overcome conventional defenses and seriously harm systems and networks by automating vulnerability finding, developing complex attacks, and focusing on particular vulnerabilities. This concern is heightened by the potential for weaponized AI, which might lead to autonomous systems that could launch destructive assaults without the need for human participation.

However, it is important to keep in mind that artificial intelligence has two sides. Even while there are threats, AI offers a ton of opportunities to improve cybersecurity. AI is being used to fortify defenses and enhance security posture in a variety of ways, from automatic patching and threat intelligence to anomaly detection [3] and malware analysis. The future of cybersecurity will depend on striking a balance between attack and defense. Organizations need to constantly invest in their defenses, keep aware of emerging threats, and be alert and proactive. This involves setting up a layered security strategy, utilizing AI to identify vulnerabilities and mitigate attacks, and encouraging a cybersecurity-aware culture within the company.

Chapter 3 introduced the combating of digital deception in IoT-enabled social networks with the help of federated learning, security concerns, FL-based intrusion detection systems, and aggregated algorithms. Artificial intelligence (AI) has undergone rapid innovation [4] and a revolution in social networks. From its modest beginnings in the early 2000s with crude algorithms for basic content recommendation and friend recommendations, artificial intelligence (AI) has grown into a powerful force influencing almost every facet of the social media scene. A new era of tailored experiences arrived with the emergence of AI in the 2010s. With the help of painstaking user data analysis, machine learning algorithms were able to precisely target ads and suggest content at a level that was previously unthinkable. This led to a sharp change in the advertising environment as well as higher user engagement, allowing marketers to more effectively target their demographic. These days, AI has far more impact than just curating material. Complex tasks like anomaly detection, sentiment analysis, and picture recognition [5] are handled by sophisticated models like deep learning. This enables social media companies to create content on their own, filter offensive content, and even create chatbots and virtual assistants that can communicate with users in ways that are more and more like those of humans. Platforms can even build better online

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

Rupa Rani

Rupa Rani is an assistant professor in CSE at Ajay Kumar Garg Engineering College, Ghaziabad, and a postdoctoral researcher at National Kaohsiung University of Science and Technology, Taiwan. She holds a Ph.D. in CSE from Banasthali Vidyapith and has over 10 years of teaching experience. With more than 20 publications in WoS, SCOPUS, and SCIE-indexed journals and conferences, she also serves as a session chair, TPC member, and reviewer. Her research focuses on data science, AI, machine learning, and cyber security.

Prashant Upadhyay

Prashant Upadhyay is an assistant professor in CSE at Sharda University, India, specializing in computer vision, NLP, and AI-driven healthcare. With a Ph.D. from Gautam Buddha University and more than 7 years of experience, he has published in top journals (SCIE/Scopus) and conferences. He has authored a Wiley book on Python, edited 11 books (CRC Press, IGI Global), and holds 3 patents with 8 more published. His research focuses on deep learning for Alzheimer's classification, neuroimaging, and IoT security. An active TPC member and reviewer, he bridges AI, biomedical engineering, and intelligent systems for industry and academia.

Rohit Sahu

Rohit Sahu is an assistant professor in mechanical engineering at G.L. Bajaj Institute of Technology, Greater Noida. He holds a B.Tech (AKTU), M.Tech (BIET Jhansi), and is pursuing a Ph.D. (DTU Delhi). His research focuses on composite materials, unconventional machining, and manufacturing optimization. With more than 25 publications in national/international journals, he serves as an editorial board member for Scopus-indexed journals and guest editor for SCI/Scopus journals. He is also involved in Springer, IOP, and AIP conference proceedings. Additionally, he received an honorary doctorate from a Ukrainian healthcare university.

Satya Prakash Yadav

Satya Prakash Yadav (SMIEEE) is an associate professor in CSE at MMMUT Gorakhpur, India, with a Ph.D. from AKTU and postdoctoral experience from Brazil. He has more than 17 years of experience in academia, he has supervised 6 Ph.D. students and published 4 books (C/C++, Blockchain, AI) and multiple patents. His research focuses on image processing, feature extraction, and AI. He has industry exposure in SAP, railway systems, and metro network design. An NSIT Delhi alumnus, he has numerous WoS-indexed publications and serves as Editor-in-Chief for several journals, including Computer Systems Science and Engineering (Tech Science Press) and Measurement: Sensors (Elsevier).

Hardeo Kumar Thakur

Hardeo Kumar Thakur (SMIEEE) is an associate professor at Bennett University, Greater Noida, with 17+ years of teaching and research experience. He holds a Ph.D. in computer engineering from the University of Delhi, with specialization in data mining. With 28 journal papers, 25 conference papers, and 2 books, his research focuses on dynamic graph mining, ML, and big data analytics. He has supervised 3 Ph.D. and 2 M.Tech students and serves as a guest editor and reviewer for reputed journals. Earlier, he worked as a teaching cum research fellow at NSIT, Delhi.