International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

CERTIFICATE NO : ICLTSEMH /2025/C0125267

A Comprehensive Study on Detecting and Countering Malicious Activities in Online Social Networks

Sudipta Das

Research Scholar, Department of Computer Science and Engineering,
Kalinga University, Raipur, Chhattisgarh.

ABSTRACT

The use of the Internet for social purposes is on the rise among individuals of all ages nowadays. As a result, big amounts of data are being spread throughout social networks as a result of several duties being moved there, such as political messaging, ads, and so on. Nonetheless, this begs the question of how reliable the accounts that provide such data really are. In order to make money, malicious people frequently alter data. An example of how malevolent people may affect society as a whole is by creating false accounts and followers in an effort to boost their fame and gain more sponsors, followers, etc. The only way to address these problems is to improve the capacity to detect and remove imposter accounts and followers.

Keywords: *Malicious, Message, Comment, Links, Malware.*

I. INTRODUCTION

The advent of the internet in the mid-1990s made data sharing feasible in ways that had previously been inconceivable. Personal data exchange is still unaddressed. In the 2000s, a lot of individuals came to terms with the fact that social media makes it easier to disclose private information online. Social media platforms like Twitter, Facebook, LinkedIn, Instagram, and many more facilitate social networking, which in turn allows users to increase their interaction with other users. For professional and personal reasons alike, social networking is a lifesaver. By bringing individuals together, these social media sites facilitate conversation, the sharing of interests and information, and the establishment of new friendships. People can mostly communicate through social media. In terms of convenience, these platforms have always been useful. The aforementioned factors are largely responsible for the meteoric rise in both the quantity and popularity of social media sites. People may use social media to further their careers, amuse themselves, find new business possibilities, hone their social skills, and form relationships with others. Because of the large number of people who use social media sites online, the most popular ones are Facebook and Myspace, which have evolved into excellent platforms for enhancing business and security operations.

Because many individuals view social media as a means of personal connection, they fail to recognize the significance of safeguarding the personal information they post on these platforms. As more and more social media platforms provide unprecedented access to personal and company data,

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

more and more people are sharing personal information online. Competitors looking to harm others have found a lot of useful information saved in social networks. With access to a mountain of data, such individuals may wreck work. But now more than ever, dealers may only promote on social media. There are a lot of upsides to using the platforms, but there are also some downsides. There are a lot of reasons why these systems are vulnerable to hacking attempts. Someone who doesn't want to be there can create a website that mimics Facebook's design. On top of that, there are a lot of ways they entice users to input their credentials.

False news is "false information, spread deliberately intending to mislead and/or deceive". Disinformation material can spread through text, audio, visuals, or a combination of all three modalities; it is pervasive across several OSN platforms. The line between fact and fiction is blurry, but scholars have proposed definitions of disinformation that suggest it is "fabricated or deliberately manipulated" with the intent to mislead the audience. This kind of coordinated activity spreads among OSN users by presenting false information in a way that seems extremely legitimate. In addition, the manipulation tactics used by bad actors greatly increase the spread of misleading material, enabling it to swiftly reach a huge audience. Despite social media companies' best efforts, coordinated campaigns continue to find ways around their platforms and search engines. This allows bad actors to take advantage of loopholes in regulations and guidelines, such as verification processes and gate-keeping mechanisms, and spread misinformation.

Any danger that may be exploited to commit crimes over the Internet is known as a web threat. Online fraud and malware come in many forms, and while most of it uses the HTTP or HTTPS protocol, it can also use other components, such links in email or instant messaging, virus attachments, or servers that connect to the Web. They assist in the absorption of infected PCs into botnets and the theft of information for later sale, both of which enrich hackers. Threats on the web can cause a variety of problems, including as loss of money or personal information, theft of sensitive data or information, theft of network resources, harm to one's reputation or brand, and a decrease in trust in online banking and shopping. Apps developed and promoted by outside parties can greatly improve the quality of life for users of online social networks (OSN). Some examples of these improvements include more engaging methods of chatting with friends online and more varied entertainment options, such playing games or listening to music. Developers may take use of Facebook's application programming interface (API) to build apps that integrate with the Facebook user experience.

On Facebook, you can find over 500,000 applications, and every day, an average of 20 million apps are installed. In addition, a huge number of applications have attracted and continue to attract users. As an example, there is 26.5 million user data in the FarmVille and CityVille applications. Despite physical distance, millions of individuals are able to contact with one another using online social networking sites such as Facebook, Twitter, Myspace, etc. Thanks to this online social networking service, users are able to share not only text but also music, video, and web sites. This may be the

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

developer's goal and one of the many tremendous benefits of such sites. An integral part of this social networking website is the internet service providers. Some kind of interface links them to the user.

II. REVIEW OF LITERATURE

Caruccio, Loredana et al., (2023) The use of the Internet for social purposes is on the rise among individuals of all ages these days. As a result, a great deal of labor, including the distribution of ads and political messages, is taking place across social media platforms, leading to massive amounts of data being transmitted over these platforms. The veracity of the data and the accounts that generate it are, however, called into question by these developments. It is not uncommon for malicious people to modify data for financial advantage. As an example, bad actors frequently utilize false profiles and followers to boost their profile's popularity and gain more sponsors, followers, etc., which may have far-reaching detrimental consequences for society as a whole. Improving the capacity to detect false accounts and followers is crucial for addressing these concerns. In this study, we suggest a new feature engineering approach to enhance the capacity of current machine learning algorithms to distinguish between fake and real social media accounts. This approach takes advantage of automatically extracted data correlations that characterize meaningful patterns of malicious accounts. The suggested method is successful in automatically distinguishing between real and phony accounts, according to experimental findings generated by several machine learning models applied to datasets of Twitter and Instagram accounts. Because of its stringent privacy restrictions and the fact that it is the only social network site that makes data of its users' accounts publicly available, Twitter is primarily chosen.

Ben Sassi, Imen & Ben Yahia, Sadok. (2021) Some disruptive entities, such as cyber-extremists, bogus accounts, and bots, have become more active due to the proliferation of online social networks, which has led to an upsurge in undesired behaviors. Consequently, systems that might identify dangerous accounts and take action to reduce their impact were overwhelmed. This study provides a complete analysis and literature review on social network-based fraudulent account identification. We take a close look at the detection methods in order to find the domain's open challenges. We combed through 147 articles to extract the following information: the type of malicious accounts that were targeted, the features that were chosen for the detection task, the social media platform that provided the feature data, the domain where the detection of malicious accounts is needed, a comparison of detection methods, datasets that are available, and validation performance metrics. We also go into the upcoming difficulties with validation protocols, annotation approaches, and detection algorithms.

Thakur and Kumar (2021) provide a method for detecting phishing URLs that relies on ensemble learning. Decision trees and logistic regression are two examples of how they integrate several weak learners to build a more robust prediction model. By combining the best features of several classifiers, the ensemble technique increases the precision of detection. Feature engineering, which involves extracting domain-related characteristics and URL syntactical data for classification, is also emphasized in the study.

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

Gupta and Kumar (2020) investigate the potential of natural language processing (NLP) methods to identify unsuitable or hazardous text on social networking sites. Important techniques for identifying hate speech, cyberbullying, and disinformation are covered in detail, and they include sentiment analysis, topic modeling, and named entity recognition (NER). Using a combination of rule-based and machine learning techniques, the article suggests a solution to the problems caused by the informal and loud character of social media writing.

S., Adewole et al., (2017) In recent years, online social networks (OSNs) like Facebook, Twitter, and Tuenti have witnessed significant increase in profile registrations and social interactions. These networks enable individuals to disseminate many types of information, including news, photographs, videos, emotions, personal data, or research endeavors. The swift expansion of online social networks has precipitated a significant increase in nefarious activities such as spamming, the creation of counterfeit accounts, phishing, and malware dissemination. Nonetheless, creating an effective detection system capable of identifying fraudulent accounts and their dubious actions on social networks has proven to be rather difficult. Researchers have suggested many characteristics and techniques to identify rogue accounts. This study offers an exhaustive assessment of pertinent research concerning the identification of fraudulent accounts on social networking platforms. The study concentrates on four primary categories: identification of spam accounts, counterfeit accounts, compromised accounts, and phishing. A taxonomy of the many traits and methodologies employed in the literature to identify fraudulent accounts and their actions is provided to categorize the investigations. The review focused exclusively on social networking sites and omitted research related to email spam detection. The importance of suggested traits and methodologies, together with their constraints, is examined. Significant concerns and challenges necessitating extensive study endeavors are examined. In conclusion, the report delineates significant future research domains aimed at enhancing the development of scalable fraudulent account detection systems in online social networks (OSNs).

III. CONCEPT OF MALICIOUS DATA AND USERS IN OSN

Malicious data refers to information that, when inadvertently provided to a computer by an unsuspecting operator, prompts the machine to execute acts detrimental to the owner's interests. Malicious activities conducted by local network users that impede the effective sharing of network resources. Prevalent dangers include: Unauthorized Access, Data Destruction, Administrative Access, System Crash/Hardware Failure, and Viruses. Malware, an abbreviation for malicious software, refers to software designed to undermine computer functionality, exfiltrate data, circumvent access controls, or inflict damage on the host machine. Malware is an encompassing phrase that denotes many malevolent applications. This essay will delineate some commonplace categories of malware: adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

In the realm of OSN, malevolent actors are described as humans and software-based users who participate in illicit actions by generating, disseminating, and/or propagating misinformation. These entities demonstrate duplicitous actions, such as disseminating insulting content, appropriating information, engaging in dishonest or unethical conduct, and harassing other platform users.

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

Malicious individuals have utilized sophisticated tactics to circumvent the detection systems of social network communities and avert bans and other punitive measures outlined in the social network policies. Emotional emotions (e.g., anxiety), social identity, skepticism towards conventional media, prejudices and beliefs, and selective exposure have been recognized as potential factors enabling bad actors to maintain their facade as reputable information sources. Malicious actors cultivate trust with their victims and manipulate them into ingesting and disseminating misinformation using techniques that exploit gullibility.

Importance of Modeling Malicious Attacks in OSNs

Social network analysis has been beneficial in epidemiology for elucidating how patterns of human interaction or assistance impede the transmission of infectious illnesses within a community. A vulnerable host is in good health but can get sick easily. An infectious host has been affected and can infect additional hosts that are vulnerable. If recovering from an illness gives immunity, then hosts that recover is said to be eliminated since they won't be able to get sick again when they recover.

Agent-based models may occasionally be used to represent how social networks function. These models help us understand how communication norms, rumor propagation, and social structure all work together. You might also utilize social network analysis to spy on a lot of people at once. Malware spreading in OSNs is becoming a big security risk for anyone who utilize social networks. OSN virus spreads quicker than regular malware, which is much worse.

In addition to being a place where malware may spread, social networks have been criticized for invading their members' privacy. This means that people have been recruited or dismissed based on how they act on social media, and university applications have been evaluated based on how they act on social media. There are several cases of breaches of user privacy that have had bad effects. Hackers that want to do harm typically plan and strategize cyberattacks on social networks.

Analysts who look closely at these talks can tell system administrators what attackers can do and what they want to do. People commonly undertake this type of analysis by hand. Lincoln Laboratory has shown that it is possible to automatically find these kinds of harmful conversations on different OSNs using new machine learning technology.

IV. IDENTIFYING MALICIOUS USERS IN SOCIAL NETWORK

There are billions of individuals all over the globe that utilize social networks, making them an integral aspect of the modern internet. A lot of people use Facebook, and that app has access to a lot of data, including public records, news feeds, friend lists, and more. Detecting malevolent social network members via their unusual behavior within the program.

Login Authentication and Registration

The registration and login processes for social networks are essential for security purposes in each application. Login authentication has two elements: username and password. The login and password

must be robust, with the password incorporating special characters, letters, and numerals. A complicated password prevents unauthorized users from accessing login authentication information. It is a security measure provided to the user, designed to safeguard their profile. The registration procedure is necessary for utilizing social network services, since a valid email address is required for verification purposes. If any harmful or fraudulent user attempts to access the user ID, the original user will get notifications via email.

When enrolling for any social networking program, it is necessary to provide an authorized email address. It aids in safeguarding the user's profile and may also reveal an individual's hacking activities. When a harmful or fraudulent user attempts to compromise your social media profile, an alert message will be dispatched to your email indicating that someone is attempting to breach your account.

Message Characteristics

The communication patterns of certain social networks allow for the identification of malevolent users. Messages are organized into many types.

(a) Message Topic

Chat apps and text messaging are a common way for users of social media platforms to stay in touch with one another. Many messages containing many pieces of information may be sent by users. But we can also anticipate that many people will discuss about things that interest them, such movies, sports, and TV programs. An anomalous or fraudulent message occurs when the user abruptly alters their normal conversational pattern or when they speak with each other in a way that is unrelated to their normal discourse.

Without context, it's hard to tell whether a message that is completely irrelevant to the subject is unusual given their regular communication. Users of some social networking applications are able to publish messages that are directly related to the subjects discussed. A tagging technique that makes use of hash characters is one example. Facebook users are more likely to identify cricket with their tweets when they use the hashtag #Cricket. Malicious users may be located using these methods.

(b) Multimedia Messages

Text, graphics, music, and video are some of the many types of multimedia messaging. Thanks to the tools offered by social media sites, every user may strike up conversations with anyone else. One could infer malevolent intent from the many forms of offensive visual content. Assuming the other user supplied audio that may be seen as blackmail or any other kind of false user identification. A user may be deemed malevolent or phony based on the videos they utilize, whether they are spam films or not.

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

(c) Links in Messages

Social networks have applications that feature connections designed to hurt or mislead users. When a user clicks on the URL or links that prompt the theft of personal information. These links assist in assessing the malignancy of the communications. These URLs may be disseminated as messages or utilized as comments. If a user clicks on a link provided as a message on the social network, malware will be immediately downloaded, compromising the user's personal information to the criminal actor.

Comment Section

The comment area in social networks is significant, as users are inherently interested in the feedback on their postings. Numerous news websites, blogs, and social media platforms include a comments area for people to express feedback on their articles or published information. Social media programs offer several sorts of comment-able content, including videos, photographs, tagged images, news articles, status updates, and profile pictures. Every user of social media possesses the right to comment. There are two categories of comments: Gated comment sections will publish certain content on their website, after which the user will submit a remark pertaining to that topic. The non-gated comments area offers information and enables users to add comments and debate the content from various perspectives.

Toxic comments on social media may also hurt the original users. Toxic comments encompass derogatory language, inappropriate emojis, and GIFs, which can be utilized to identify unscrupulous or fraudulent users.

Friends List

In social networks, identifying potentially harmful users by perusing their friend lists. Users ought to use greater caution when consenting to requests from someone they do not know. Detecting malevolent individuals via their unusual behavior, including looking for profiles of various celebrities or girls. Requests are being sent exclusively to females.

Form a friendship group and make poisonous remarks on each member's profile. Making friends online may be fun at times, but it's not a smart idea to initiate contact with someone you don't know. If you want more likes, comments, and follows, don't create friends for that reason. Someone with ill intentions might exploit your personal information to do damage or even blackmail you. It is also possible for malicious people to utilize the information found on social media sites to build false profiles. Malicious users engage in these unusual behaviors.

V. MALICIOUS URLS IN SOCIAL MEDIA

Posts, comments, or messages might include malicious URLs, which direct users to hazardous websites. Users may unwittingly expose themselves to security risks when they click on these URLs, which are frequently disguised as real links. Such connections may lead to:

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

- **Phishing Attacks:** URLs that steal sensitive information by impersonating recognized websites (such as social media or banks).
- **Malware:** Connections that take visitors to malicious websites where they can download viruses or ransomware without their knowledge.
- **Fraudulent Websites:** URLs that take visitors to fraudulent websites that steal their personal and financial data or sell them counterfeit goods.

In addition to endangering individuals, bad URLs can compromise organizations and even the nation's security. Adding insult to injury, these URLs can also be utilized to disseminate false material on social media platforms.

Detection of Malicious URLs

The effective identification of malicious URLs is a complex issue. Conventional approaches encompass:

Signature-Based Detection

Signature-based detection approaches are the most direct. They evaluate URLs against a predetermined catalog of recognized harmful URLs or patterns. Signature-based systems are effective yet inadequate in identifying novel threats, such as zero-day attacks. A URL's domain or IP address may be reported if it corresponds to an entry in the threat database. Nonetheless, signature-based approaches are constrained in their capacity to identify emerging threats or assaults that employ dynamic and obfuscated URLs.

Heuristic-Based Detection

Heuristic approaches concentrate on examining the structure and attributes of the URL to detect possible dangers. These approaches analyze several characteristics, including:

- The presence of suspicious characters or encoding (e.g., excessive use of special characters, base64 encoding).
- The length of the URL (malicious URLs are often longer to accommodate hidden phishing or malware links).
- The use of URL shortening services (e.g., bit.ly, Tiny-URL) that can mask the true destination.
- Suspicious domain names (e.g., similar to popular domains, but with slight misspellings). While heuristic methods exhibit greater flexibility than signature-based approaches, they are susceptible to false positives and may overlook novel attack vectors.

Machine Learning-Based Detection

Machine learning (ML) models are progressively employed for the identification of harmful URLs. Machine learning algorithms can discern patterns that may not be immediately evident by training models on extensive datasets of tagged URLs. Several prevalent methodologies encompass:

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

- **Supervised Learning:** To determine if a URL is malicious or not, algorithms such as decision trees, support vector machines (SVM), and random forests can be employed. By studying characteristics like domain, length of URL, and usage of certain phrases, the model learns to identify trends.
- **Deep Learning:** Deep learning models in particular, such as RNNs and convolutional neural networks (CNNs), can learn complicated, nonlinear patterns from enormous datasets. These models have demonstrated enhanced performance, particularly when it comes to identifying hidden or previously undiscovered URLs.

Challenges in Malicious URL Detection

The key challenges in detecting malicious URLs include:

- **Evasion Techniques:** Attackers are always coming up with new ways to evade detection. It is challenging to detect malicious URLs because to techniques like domain generating algorithms (DGAs), URL obfuscation (using URL shorteners or encoding methods, etc.), and the usage of genuine but compromised websites.
- **Real-time Detection:** It is crucial that URL recognition systems function in real-time due to the great velocity of information exchanged on social media. It is quite challenging to process millions of connections efficiently while keeping accuracy high.
- **Scalability:** Scalable detection systems capable of handling millions of incoming requests simultaneously are necessary due to the enormous number of URLs published across social media sites.

VI. ARCHITECTURE OF A SYSTEM FOR COUNTERING MALICIOUS INFORMATION IN SOCIAL NETWORKS

The architecture includes three levels:

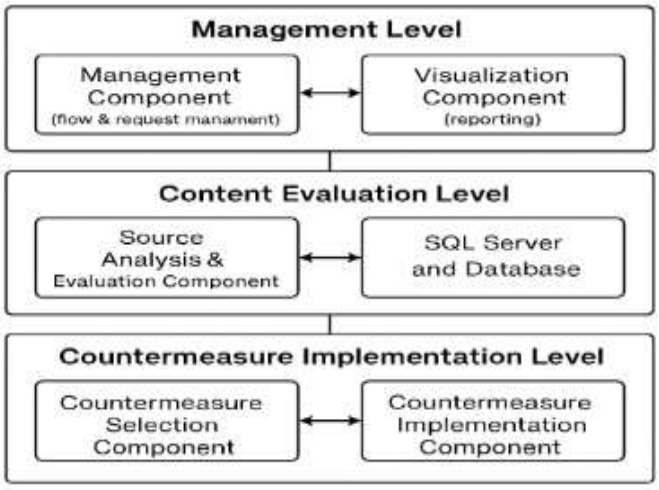

Figure 1: Architecture for Malicious User Detection and Countermeasure Implementation in Online Social Networks

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

1. **Management Level:** This level encompasses two primary components — the management component, which oversees data flow and request management across the system, and the visualization component, responsible for generating analytical reports and dashboards that provide actionable insights. This ensures effective monitoring, coordination, and decision-making for handling malicious activities.
2. **Content Evaluation Level:** This level focuses on the intelligent assessment of online content through the source analysis and evaluation component, coupled with an SQL server and database for structured data management. It supports algorithms for ranking, evaluating, and sorting information sources and effect objects, thereby facilitating the detection of potential threats based on data authenticity and behavior patterns.
3. **Countermeasure Implementation Level:** This level includes the countermeasure selection component and countermeasure implementation component, which work together to design and execute effective response strategies against malicious data or user activity. The selection process relies on a ranking mechanism and expert judgment algorithms to ensure that chosen countermeasures are both contextually appropriate and efficient.

Elements of the architecture are implemented as software prototypes:

- A software prototype for social network source analysis and evaluation, incorporating algorithms for source ranking, evaluation, and effect object sorting to identify and prioritize malicious entities.
- A software model for countermeasure selection, integrating algorithms that use expert judgment and ranking logic to determine optimal mitigation strategies.
- A software model of the Information Threat and Countermeasure Database (DBIT and C), which serves as a repository detailing counter-strategies against harmful social media content, potential targets for mitigation, and the agents capable of executing these countermeasures.

This multi-level architecture provides a holistic, adaptive, and data-driven framework to safeguard online social networks from evolving threats, promoting a safer and more reliable digital communication environment.

VII. CONCLUSION

Digital trust, privacy, and information authenticity are gravely threatened by the proliferation of malicious data and dishonest people in online social networks (OSNs). From spreading dangerous URLs and false information to manipulating user behavior through complex evasion techniques, the study shows that malicious behaviors are diverse. Protecting network integrity and developing robust detection systems require an understanding of user psychology and the notion of malicious data. To intelligently and systematically detect, analyze, and mitigate such risks, the three-tiered system architecture that is proposed—including management, content evaluation, and countermeasure implementation—is an effective framework. This design guarantees quick and flexible reactions to

IJAMSR

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

new cyber threats by combining sophisticated analytical models with expert judgment procedures and automated countermeasure execution. In order to build a social networking ecosystem that is safer and more dependable, it is necessary to work together to improve OSN security. This includes combining technology innovation with user awareness and policy enforcement.

REFERENCES

1. L. Caruccio, G. Cimino, S. Cirillo, D. Desiato, G. Polese, and G. Tortora, "Malicious account identification in social network platforms," *ACM Trans. Internet Technol.*, vol. 23, no. 4, pp. 1–12, 2023.
2. N. Deepika and N. Guruprasad, "Malicious content detection in social networks using hybrid machine learning model," *Indian J. Comput. Sci. Eng.*, vol. 14, no. 3, pp. 539–550, 2023.
3. X. Yang and Y. Zhang, "Classifying hate speech on social media using BERT-based transformers," *J. Mach. Learn. Res.*, vol. 23, no. 14, pp. 332–341, 2022.
4. U. Tanuja, B. Ramesh, H. L. Gururaj, and V. Janhavi, "Detecting malicious users in the social networks using machine learning approach," *Int. J. Soc. Comput. Cyber-Phys. Syst.*, vol. 2, no. 3, pp. 229–243, 2021.
5. M. Thakur and S. Kumar, "Phishing URL detection using ensemble learning techniques," *Comput. Intell. Cyber Secur.*, vol. 17, no. 4, pp. 12–26, 2021.
6. I. B. Sassi and S. B. Yahia, "Malicious accounts detection from online social networks: A systematic review of literature," *Int. J. Gen. Syst.*, vol. 50, no. 7, pp. 1–74, 2021.
7. V. Mangu, "Detecting and removing malicious social bots," *Sci. Technol. Dev.*, vol. 10, no. 7, pp. 602–608, 2021.
8. S. Kumar and M. Goyal, "A survey on social media spam detection techniques," *J. Comput. Sci. Technol.*, vol. 36, no. 2, pp. 254–272, 2021.
9. L. Wang and C. Zhao, "A hybrid deep learning model for malicious URL detection and its real-world application," *Int. J. Cyber Secur.*, vol. 19, no. 5, pp. 65–78, 2021.
10. A. Sharma and P. Joshi, "AI-powered content moderation: A review of automated techniques for identifying harmful social media posts," *J. Artif. Intell. Res.*, vol. 45, no. 1, pp. 97–112, 2021.
11. R. Gupta and A. Kumar, "Survey of methods for classifying online hate speech using machine learning algorithms," *Comput. Sci. Rev.*, vol. 33, no. 1, pp. 100–113, 2020.
12. S. Abbas and M. Martin, "Phishing detection and prevention: A review of techniques and tools," *J. Cyber Secur.*, vol. 15, no. 4, pp. 200–215, 2020.
13. S. Patel and R. Jain, "A hybrid approach to malicious URL detection based on URL structure and content analysis," *J. Comput. Secur.*, vol. 14, no. 6, pp. 399–412, 2020.
14. P. Nguyen and H. Cao, "Phishing URL detection using deep learning and big data technologies," *Int. J. Cyber Res.*, vol. 12, no. 3, pp. 130–145, 2020.
15. S. Park and K. Kim, "Real-time malicious URL detection based on supervised learning techniques," *Computers*, vol. 8, no. 3, p. 56, 2019.

International Conference on Latest Trends in Science, Engineering, Management and Humanities (ICLTSEMH -2025)
19th January, 2025, Noida, India.

16. S. Adewole, N. Anuar, A. Kamsin, K. Varathan, and S. A. R. S. Mahadi, "Malicious accounts: Dark of the social networks," *J. Netw. Comput. Appl.*, vol. 79, no. 1, pp. 41–67, 2017.
17. S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," *IEEE Comput.*, vol. 44, no. 9, pp. 23–28, 2011.