# A comprehensive study of fraudulent activities on social media networks

**K. Srinivas Rao[1], Dr. V. Harsha Shastri[2], Raman RK[3]**

[1,3]Assistant Professor in Computer Science, Dept of MCA, School of Informatics, Aurora University, Telangana, India

[2]Associate Professor in Computer Science, Dept of MCA, School of Informatics, Aurora University, Telangana, India

**Corresponding Author Email**: harshasastry@aurora.edu.in

**Abstract**— In the last few years social networks are gaining a vital importance and its popularity is tremendous. We can say that social media has become a part of the every one lives. Social media networks are widely used by people for various purposes like interactions, looking for opportunities in business and career, entertainment and so-on. But it has evidently shown that there are lot of frauds taking place through these online platforms. It has become a wide cyber threat in these social media sites. Especially the targets are those people who look for business opportunities, work from home job opportunities. The purpose of this article is primarily to explain the fraud type and the damage it might do to consumers.

**Keywords**: frauds, internet, social networks, threats, vulnerable

## I. INTRODUCTION

Due to the wide growth of internet these days, social media is gaining a lot of importance among the users. We use these social network services for connecting people who have similar interest, experience and actions. It has become a daily live for the people interacting on social media. The social media applications is spread among the community by interacting with friends, forming communities having personal interests, and generating and sharing information. The information is disseminated via many media formats such as articles, photos, videos, news, e-commerce, and even politics.

Many users are aware of using social media applications, but privacy and security is a major concern. Users are unaware of how to protect the personal information on these forums and websites. Social network frauds include situations where users are susceptible to online abuse, phishing, consumer fraud, hacking, and identity theft. It is possible to identify an individual using the data found on social media networks.

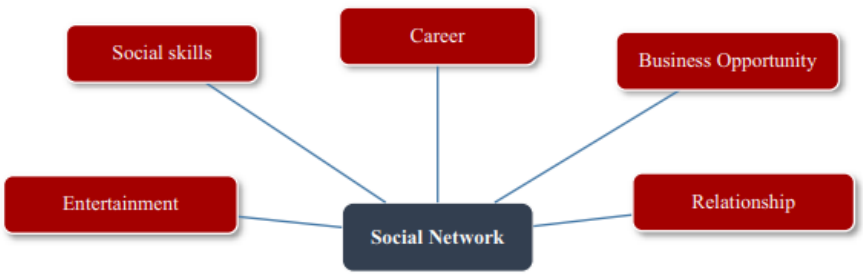


**Figure 1**: Types of Social network

The goal of fraud is to deceive people into parting with their money. As a result, consumers risk having their private information leaked or losing the money they had invested. Damage to a system's or an individual's credibility, financial resources, or faith in social media may come from these kinds of actions. When such a fraud occurs, users do not report this fraud due to loss of reputation or with the fear in mind as to what is going to happen with them. Some times by the nature of fraud it becomes hard to detect the fraud as well. The paper is divided into sections. The first part is dealt with statistics of social network fraud, types of fraud and prevention of fraud, later a case study is presented and conclusion for the work is shown.

## II. STATISTICS OF SOCIAL NETWORK FRAUD

The National Crime Records Bureau (NCRB) reports that 4,850 incidents of cybercrime totaled ₹66.66 crore in 2023, causing a tremendous loss in the country. Over the last three years, digital financial scams totaled an astounding 1.25 lakh crore, according to a new study from the Indian Cybercrime Coordination Centre (I4C). In 2023, victims of digital financial fraud were claimed to have lost a minimum of ₹10,319 crore, according to the National Cybercrime Reporting Portal (NCRP). The report on "cyber security and rising incidents of cyber/white collar crimes" by the Parliamentary standing committee on finance noted that the domestic fraud recorded by the SE (Supervising Entities) in FY'23 amounted to ₹2537.35 crore. The study states that 6.94 lakh complaints were received in 2023 alone.

This article discusses some of the issues encountered during investigations, along with potential solutions, for detecting and preventing online financial fraud.

As per information introduced on Wednesday, 3 January 2024, by the Indian Cybercrime Coordination Center (I4C), which works under the aegis of the Association Service of Home Issues, the most well-known neighborhood beginning tricks hailed by Indians in 2023 were KYC expiry extortion, sextortion, and QR code tricks.

On February 6, a response to a question from the Lok Sabha stated that 1.13 million instances of financial cyber theft would be discovered in 2023. Under the direction of the "Indian Cyber Crime Coordination Centre," the Ministry of Home Affairs established the "Citizen Financial Cyber Fraud Reporting and Management System" to facilitate the reporting of financial fraud. According to the response, "more than Rs 1,200 crore have been saved" since the system's inception in response to approximately 4,750,000 complaints.. It went on to say that 320,000 SIM cards and 49,000 IMEI numbers had been disabled by the government after police reported them.

Half of all instances of financial cyber fraud in 2018 occurred in only five states. With over 200,000 instances, Uttar Pradesh topped all 36 states and union territories. After Gujarat (120,000), Rajasthan (80,000), and Haryana (130,000), the next most complained about state was Maharashtra with 130,000. With 29 occurrences, Lakshadweep ranked last (Fig 2).

The total sum involved in these 1.13 million instances was 7,488.6 crore Indian rupees. The highest sum in Maharashtra was Rs 990.7 crore. Next came Telangana with 759.1 crore rupees. After that came Karnataka with 662.1 crore, Tamil Nadu with 661.2 crore, and Uttar Pradesh with 721.1 crore. Fig. 3 shows that the least sum involved was Lakshadweep, at Rs. 0.2 crore.

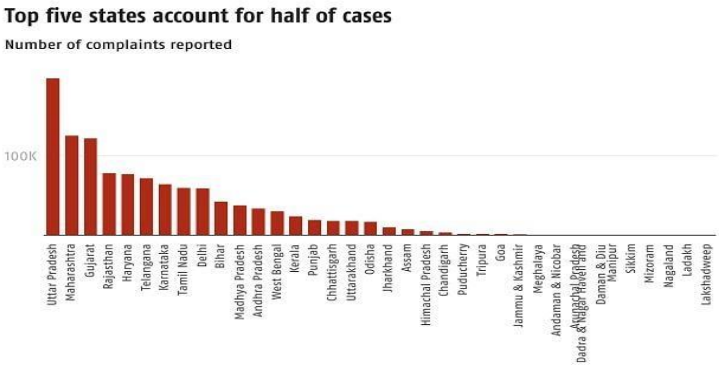


**Figure 2:** Top five states with half of the cases

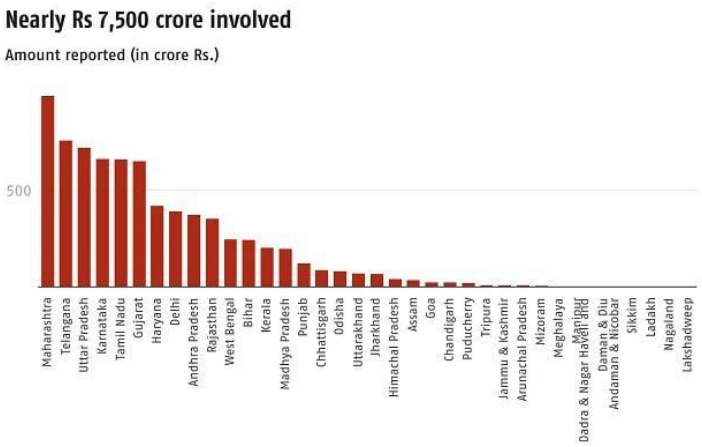


**Figure 3:** Amount loss across the states

About 300,000 complaints were still outstanding in 2023, with a total lien amounting to Rs 921.6 crore, as said in the answer. While 1,402,809 cyber security events were recorded in 2021, the number of occurrences reported in 2022 was 1,391,457 according to data from the Indian Computer Emergency Response Team (CERT-IN). In recent years, a tendency has emerged. In 2018, that figure came to 208,456.

Table 1 displays the statistics of the main types of fraud recorded as cyber crimes across states.

| **Sl. No.** | **State** | **No of** | **Amount** | **No of** | **Lien** |
|---|---|---|---|---|---|
| | | **Complaint** | **Reported** | **Complaints** | **Amount** |
| | | **Reported** | **(Rs in Lacs)** | **(Put on Hold)** | **(Rs in Lacs)** |
| 1 | Andaman & Nicobar | 526 | 311.97 | 161 | 26.46 |
| 2 | Andhra Pradesh | 33507 | 37419.77 | 9580 | 4664.14 |
| 3 | Arunachal Pradesh | 470 | 765.79 | 127 | 34.39 |
| 4 | Assam | 7621 | 3441.8 | 2163 | 451.61 |
| 5 | Bihar | 42029 | 24327.79 | 11533 | 2779.41 |
| 6 | Chandigarh | 3601 | 2258.61 | 1058 | 296.67 |
| 7 | Chhattisgarh | 18147 | 8777.15 | 5056 | 898.41 |
| 8 | Dadra & Nagar Haveli and Daman & Diu | 412 | 326.21 | 105 | 40.88 |
| 9 | Delhi | 58748 | 39157.86 | 13674 | 3425.03 |
| 10 | Goa | 1788 | 2318.25 | 450 | 153.22 |
| 11 | Gujarat | 121701 | 65053.35 | 49220 | 15690.9 |
| 12 | Haryana | 76736 | 41924.75 | 21178 | 4653.4 |
| 13 | Himachal Pradesh | 5268 | 4115.25 | 1502 | 370.78 |
| 14 | Jammu & Kashmir | 1046 | 786.56 | 253 | 62.55 |

| | | | | | |
|---|---|---|---|---|---|
| 15 | Jharkhand | 10040 | 6788.98 | 2822 | 556.38 |
| 16 | Karnataka | 64301 | 66210.02 | 18989 | 7315.52 |
| 17 | Kerala | 23757 | 20179.86 | 8559 | 3647.83 |
| 18 | Ladakh | 162 | 190.29 | 41 | 10.03 |
| 19 | Lakshadweep | 29 | 19.58 | 6 | 0.51 |
| 20 | Madhya Pradesh | 37435 | 19625.03 | 9336 | 1462.33 |
| 21 | Maharashtra | 125153 | 99069.22 | 32050 | 10308.47 |
| 22 | Manipur | 339 | 333.03 | 108 | 66.94 |
| 23 | Meghalaya | 654 | 424.2 | 252 | 46.71 |
| 24 | Mizoram | 239 | 484.12 | 75 | 35.44 |
| 25 | Nagaland | 224 | 148.94 | 73 | 18.09 |
| 26 | Odisha | 16869 | 7967.11 | 5187 | 1049.34 |
| 27 | Puducherry | 1953 | 2020.34 | 568 | 143.38 |
| 28 | Punjab | 19252 | 12178.42 | 4923 | 1332.66 |
| 29 | Rajasthan | 77769 | 35392.09 | 20899 | 3934.82 |
| 30 | Sikkim | 292 | 197.92 | 65 | 18.01 |
| 31 | Tamil Nadu | 59549 | 66123.21 | 17941 | 6980.72 |
| 32 | Telangana | 71426 | 75905.62 | 26148 | 13137.94 |
| 33 | Tripura | 1913 | 900.35 | 488 | 84.82 |
| 34 | Uttarakhand | 17958 | 6879.67 | 4813 | 708.94 |
| 35 | Uttar Pradesh | 197547 | 72107.46 | 44089 | 5906.86 |
| 36 | West Bengal | 29804 | 24733.33 | 6307 | 1845.97 |

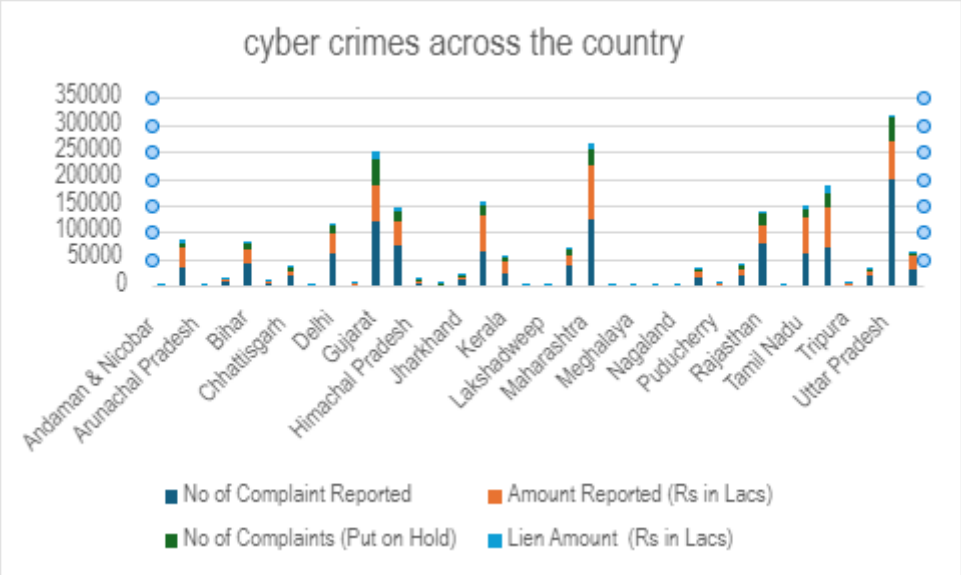


**Figure 4** : Showing the cyber crimes across the country

## II.I. TYPES OF FRAUDS

Nowadays, it's impossible to go about our day without using some type of social media. In order to stay in touch with friends and family, express ourselves, and find new and fascinating material, we are constantly on our favorite social networking platforms. Scammers have taken up residence there. The best defense against social media frauds is knowledge.

### II.I.I. PHISHING THROUGH DIRECT MESSAGES

This kind of fraud isn't limited to email. Indeed, one may discover it on social media. When con artists pose as friends or respected businesses in an attempt to trick their targets into divulging sensitive information, they are engaging in social media phishing. The victims are tricked into clicking on a link by messages that make them feel like they need to click on anything quickly. After you click the link, you'll be sent to a phony login screen. Scammers may steal your credentials and access your accounts after you submit them.

### II.I.II. QUIZZES OR PERSONALITY TESTS

Many social media platforms provide quizzes and personality tests as a seemingly innocent way to kill time or learn more about oneself. In order to access your profile information, the social networking site will request it whenever you open a personality test or quiz. Con artists will even use security question trickery to get you to divulge sensitive information.

### II.I.III. FAKE GIVEAWAYS AND CONTESTS

Giving out free stuff and holding competitions on social media are two ways that firms have taken advantage of people's passion of winning free stuff. A lot of individuals fall for the "giveaway or contest" scam when they see an unscrupulous business offering great rewards in return for their personal details.

### II.I.IV. IMPERSONATION OF FAMILY AND FRIENDS

Communicating with loved ones is a top priority for many people who use social media. Con artists have made advantage of this to further their own objectives, forging profiles in order to pose as somebody you know and trust. With these phoney accounts, they may pose as loved ones, say they're having a medical emergency, and beg you for money.

### II.I.V. GET-RICH-QUICK INVESTMENT SCHEMES

Misleading investment plans that promise high returns with little effort are a common way to deceive people. For that reason, fraudsters often target them. Scammers might make it seem like a real investment opportunity by using altered photos and phoney testimonials to entice you with the promise of great profits on little to no commitment.

### II.I.VI. JOB OFFER SCAMS

Nowadays, a lot of people who used to work in offices are looking for remote employment instead, thus work-from-home arrangements are all the rage. Unfortunately, con artists are taking advantage of those looking for employment by advertising legitimate-sounding work-from-home possibilities. The con artist will ask for sensitive information or money before they begin working for the victim after they accept the deal.

### II.I.VII. FREE APP DOWNLOADS

A lot of the time, these applications will ask for your personal details. Malware may be downloaded onto your smartphone by apps that seem legitimate. Do your homework, be wary of unofficial app stores, and only use the one provided by your phone company when installing new applications..

### II.I.VIII. AI FRAUD

A proliferation of frauds powered by artificial intelligence has emerged alongside new kinds of fraud and cybersecurity risks brought about by technological advancements. Attackers automate and personalize their assaults with the use of AI, making them more sophisticated. Generative AI, a kind of AI, may also be used to generate very lifelike imitation pictures, texts,

videos, and audios by training complex models on previously collected behavioral data. A large portion of the AI technology used by fraudsters is devoted to targeted social engineering assaults, which greatly complicates efforts to prevent fraud.

### II.I.IX. DEPOSIT CHEQUE FRAUD

This tired con became all the rage again, shocking as it may seem. As a result, there are new obstacles for banks to overcome, such as the need for more sophisticated processing tools to combat issues like identity fraud and phony accounts. When a bank swiftly enables the withdrawal of portion of the deposited monies even if the check has insufficient amounts, it is considered deposit cheque fraud.

### II.I.X. FRAUD AS A SERVICE (FAAS)

A widely used fraud service where con artists provide their clients tips on how to commit fraud more efficiently and covertly. Many cybercrimes, including ransomware, financial fraud, identity theft, and illegal access to sensitive systems, use FaaS. Because of recent wars and diseases that have triggered worldwide economic downturns, individuals are more prone to engaging in insider fraud and other forms of collusion.

### II.I.XI. PHONE SCAMS

The use of disguised or faked numbers, or the practice of leaving a missed call to pique the victim's interest and prompt a return contact, are two of the most deceptive aspects of phone scams. False "call centres" situated on many countries make this fraud really worldwide. The intended victims are either people or companies (e.g., "CEO Fraud," "call from Microsoft," "technical support," and "bank for account verification" scams). Its appeal stems from the fact that callers may remain anonymous and that there is a great opportunity for quick gains. With the help of the Dark Web, it is very well-organized. The Wangiri scam exemplifies the widespread popularity and rapid global expansion of phone scams, which have their roots in Japan.

Table 2 details the opinions on the scam category, the ways in which individual scams vary and relate to one another in online social networks, and the negative consequences of these scams.

| Class of fraud | Type of fraud | Purpose | Intention and potential harm |
|---|---|---|---|
| Social engineering frauds | Phishing | The hacker poses as a reliable entity in order to deceive victims into divulging sensitive information or money by creating or sending fraudulent links for communication. | Disclosure of private information, advertising efforts, pornography. |
| | Pretexting | The aggressor manipulates the victim into submissively carrying out the aggressor's directives in order to accomplish a predetermined goal. | Reputation loss, personal data loss. |
| | Baiting | By offering free gifts, the attacker hopes to trick the victim into falling into a social manipulation trap. | Personal data loss |
| Human-targeted fraud (child/ adults) | Cyberbullying | Intentionally and repetitively online provocation or harassment. | Suffering from emotional abuse, tarnished reputation, emotional distress, despair, nervousness, and panic attacks. |
| | Cyberstalking | Attackers steal personal information like phone no., address, location, profile photo, and misuse it. | Concerns about safety, privacy, emotional abuse, damage to one's |

| | | | |
|---|---|---|---|
| | | | reputation, worry, despair, insomnia, dread, and panic attacks |
| | Dating fraud | It occurs when an individual establishes a false persona and initiates contact with a target in order to get sensitive information. | Money loss, safety loss, emotional harassment, loss of reputation. |
| False identity | Fake accounts or sybil | A hacker creates a phony account to further their own interests. | Economic loss, personal information loss |
| Misinformation | Spamming | Spammers bombard OSN users with an overwhelming amount of unwanted communications. | Loss of reputation, spread of malicious content. |
| E-commerce fraud (consumer frauds) | Online shopping fraud | The practice of con artists using phoney websites or adverts to pose as legitimate internet vendors. The perpetrator bought something online and then demanded a refund, claiming the purchase was invalid or unacceptable. | Economic loss |

## II.II. SOLUTIONS FOR VARIOUS FRAUDS

People need to be protected from various types of fraudulent activities. And here we provide some of the measures

### II.II.I. USE STRONG, UNIQUE PASSWORDS

Your email account, like all of your other online accounts, requires a unique password. It is risky since many people use the same password for all of their accounts. A fraudster might easily get your password from your social media postings if it contains any personal data, such as a pet's name or your mother's maiden name.

### II.II.II. DON’T POST PERSONAL DETAILS

A fraudster's chances of obtaining your personal information are higher if you provide details such as your pet's name, address, nickname, or even when you're on vacation.

### II.II.III. STEER CLEAR OF STRANGERS

Be wary of anybody contacting you over social media and requesting sensitive information. Verify their authenticity and the validity of the information you're supplying at all times.

### II.II.IV. DELETE OLD SOCIAL MEDIA PROFILES

Eliminating accounts you no longer use is a good way to keep tabs on your digital footprint. If a profile is from a decade ago, there can be personal details that a fraudster can utilize that you either don't know about or have forgotten about.

### II.II.V. INSTALL ANTI-VIRUS SOFTWARE

You can safeguard your laptop and other personal gadgets against viruses with the aid of many free services..

### II.II.VI. TAKE CARE ON PUBLIC WI-FI

Scammers may sometimes get access to legitimate Wi-Fi networks by masquerading as them. Stay away from mobile banking and other applications that collect sensitive information if you're going to be connected while on the road.

### II.II.VII. REPORT THE CRIME TO ACTION FRAUD

You may officially report any instances of ID fraud here and get a criminal reference number..

### II.II.VIII. GUARD YOUR ONLINE INFORMATION

We must ensure that computer security software is regularly updated and instruct staff to refrain from inputting sensitive information (such as login credentials and financial details) onto public computers, since these machines may include software that records such details when logged in. When we want to log into an account or exchange data with a website—for example, when we bank or shop online—we need to make sure that the URL starts with HTTPS.

### II.II.IX. MONITOR YOUR ACCOUNTS

If you want to stay on top of your finances, monitor your balances and activity, and uncover fraudulent transactions fast, it's a good idea to use online banking or a mobile banking app every day.

### II.II.X. THINK TWICE ABOUT SHARING YOUR INFORMATION

Avoid giving up personal information over the phone or in an email. Make sure the source is trustworthy and confirmed before you divulge any private information. Scammers might attempt to get information about your company by sending you fake mails that seem to be from reputable sources. One of the biggest problems with online fraud is phishing, which takes place mostly via phone calls, text messages, and email..

### II.II.XI. AUTHENTICATION MECHANISM

Several OSN use authentication techniques like CAPTCHA, multi-factor authentication, and photos-of-friend identification to guarantee that only actual users, and not social bots, are login or enrolling in a social network. For example, two-factor authentication is used by top social networks such as Facebook and Twitter. This approach makes use of a mobile-device-received verification code and a login password. This lessens the likelihood of an account being hacked and stops an intruder from taking over a real account and publishing harmful stuff.

### II.II.XII. REPORT USERS

The ability to report abuse or policy violations by any member on a social network helps keep children and teens safe from harassment online. For example, users may use the report links to urge the person who posted something offensive to remove it from Facebook if it doesn't violate Facebook's conditions but still offends their sensibilities. In accordance with Facebook's community standards, complaints are examined and deleted when received.

### II.II.XIII. PHISHING DETECTION

Websites, social media, emails, and blogs are just a few examples of the regular online apps that are vulnerable to phishing attacks. Consequently, a number of anti-phishing methods have been created to identify phishing attempts. As a result, several academics have proposed anti-phishing protocols that use methods to detect and block malicious websites and URLs. Social networking sites are prime targets for phishing attempts, and researchers have come up with unique ways to combat this growing threat. In order to detect phishing attempts on Twitter in real-time, Aggarwal et al. suggested the PhishAri method. Whether the tweet was phishing or not, it used Twitter attributes like the account's age and follower count to determine the legitimacy of the message.

### II.II.XIV. BE AWARE OF LINKS AND THIRD-PARTY APPLICATIONS

If an unauthorized user shares a malicious link, they may get access to another user's account and potentially steal important information. These days, a lot of people use abbreviated URLs on different social networking sites. It is possible for harmful malware or script to disguise these compressed URLs. These scripts attempt to collect sensitive user information, which might compromise their privacy. Also, many prominent social networks have third-party applications connected with them, which means hackers might exploit security holes in such apps. Games that are playable on social media platforms, for instance, employ third-party applications that need users' public data in order to access their services. Outside parties or third-party initiatives may get this collected data. Users should exercise caution while adding third-party apps to their profiles in order to circumvent this danger.

## III. PROBLEM STATEMENT

A case study on Pre texting fraud attack where the victim was subjected to a whats app message asking to do work from home and would be paid for the work done. The message included the job details and the company offering the job. At first the victim got lured by the offer and decided to work with them. A week time was given to the victim to complete the job. After completion, the victim was asked to submit documents related to him so that offer letter be given to him. Slowly the victim was asked to pay money for the charges incurred as per their policy and was promised to pay the whole amount that the victim paid. Finally victim shed 2.5 lac amount. And came to know that it was a fraud. Later on logging the complaint with police, the case is under investigation. We need to set the objectives for determining the solution for the problem

1. To have a study analysis on all the types of frauds through social media
2. To detect the messages to be fraudulent based on the keywords in message by using Machine learning techniques and natural language processing
3. To develop a solution to determine the location from where the message originated so that fraud person is known which will help the authorities locate for the fraud person

## IV. CONCLUSION

The research article provided a detailed study on the types of fraud and solution are provided to prevent fraud activities. Also the paper highlighted the fraud activities taking place over the country say India and how much loss took place due to these activities. We can see the effects of OSN fraud in our day-to-day life from the latest fraud figures. As a result of using various OSN platforms, users are falling prey to fraud. We went on to detail the different The issue of OSN fraud persists after much studies. In the years to come, we could see a proliferation of new types of deception. We must continuously enhance our methods for detecting, preventing, and controlling OSN fraud.

We will be developing the solution to detect the fraudulent activities such as pretexting or phishing attacks using machine learning to prevent the activities to take place. The use of machine learning algorithms is crucial in the fight against fraud.

## REFERENCES

1. Kayes I, Iamnitchi A (2017) Privacy and security in online social networks: a survey. Online Soc Netw Media 3:1–21
2. Rathore S, Sharma PK, Loia V, Jeong Y-S, Park JH (2017) Social network security: Issues, challenges, threats, and solutions. Inf Sci 421:43–69
3. Jain AK, Sahoo SR, Kaubiyal J (2021) Online social networks security and privacy: comprehensive review and analysis. Complex Intell Syst 7(5):2157–2177
4. Guo Z, Cho J-H, Chen R, Sengupta S, Hong M, Mitra T (2020) Online social deception and its countermeasures: a survey. IEEE Access 9:1770–1806
5. Number of Social Media Users 2025 | Statista.” Statista, www.statista.com, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/. Accessed 28 May 2022

6. New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021 | Federal Trade Commission. Federal Trade Commission, www.ftc.gov, 22 Feb. 2022, https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-rec eived-28-million-fraud-reports-consumers-2021-0
7. Digital financial frauds in India: a call for improved investigation strategies https://thehindu.com/sci-tech/technology/digital-financial-frauds-in-india-a-call-for-improved-investigation-strategies/article67988607.ece#:~:text=A%20recent%20report%20by%20the,over%20the%20last%20three%20years&text=Cybercrime%20poses%20a%20burgeoning%20threat,millions%20of%20individuals%20and%20organisations
8. Around 1.1 million financial fraud cases registered in 2023, shows data https://www.business-standard.com/india-news/around-1-1-million-financial-fraud-cases-registered-in-2023-shows-data-124020601528_1.html
9. Cases of Cyber Frauds Posted On: 06 FEB 2024 5:45PM by PIB Delhi, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158
10. Social Media - Stay Safe Online [Online]. https://staysafeon line.org/stay-safe-online/securing-key-accounts-devices/socialmedia/. Accessed 7 Jan 2019