Study of Awareness about Peer to Peer Security in Social Networks

[1*] Aruna Devi K, [2] Shalini N, [3] Steffi Sabu, [4] Yeshodha S

[1*] Associate Professor, [2,3,4] PG Students, Department of Computer Science (PG), Kristu Jayanti College (Autonomous), Bengaluru

[1] *arunadevi@kristujayanti.com*, [2] *21mcaa30@kristujayanti.com*, [3] *21mcaa32@kristujayanti.com*,

[4] *21mcaa35@kristujayanti.com*

Abstract

In the present world, utilising Social media usage has grown at a phenomenal rate. The social network platforms such as Instagram, Facebook, WhatsApp, Twitter and many more provide services and facilitate peer-to-peer communication through chat, audio/video conferencing, and data sharing in a variety of formats. Using these platforms for their communication has become easier to communicate and adapt whereas the scams behind these underlying networks is unknown. As a potential case of zero trust, peer-to-peer technologies assert that they will support end-to-end communication while demanding access control, negligibility, and adaptability against suppression and enormous data breaches caused by abused trust.. This paper gives the survey of about how the security, confidentiality in social networks are prone to be in the first level. Second, how clueless people are of this demanding use of applications and analysis of the survey and the (P2P) technologies and its framework. Finally it gives a comprehensive examination of the frameworks, applications, and architectures for P2P-based online social networks.

Keywords: *Social Networks, Privacy, Social Media, Security, Transaction Security, Peer to Peer Security.*

1. Introduction

The growth of user's using social networks will rapidly increase by 2022. It increased suddenly high over the past 2 years. During covid 19 the user's used social networks to connect with people. The users came to know more about the social networks and started to become addicted towards it. Later on user's started to spend more time in usage of different social networks. Social networks started making more money from different social networks such as Facebook, Instagram and so on. Applications must be able to access private data in order for users to be able to use them. This data is public. In many cases, there is no component to monitor how the application manipulates the user's data. It introduces the security problems of social networks. The security problems are of different kinds such as privacy leak, threats, spreading rumors, hacking accounts, misuse of information, virus attacks and so on. A social networking service used to establish and develop social relationships between people. It provides a means for interacting with users online with individuals with comparable interests for social purposes and can publish blog entries. It also provides opportunities for people with disabilities to communicate their ideas and opinions in a virtual environment.

Peer-to-peer networks are a type of dispersed network in which audiences act simultaneously as clients and servers, supplying and consuming resources to and from one another in an unstructured, self-organizing fashion. P2P networks are characterized by their high degree of decentralization, tone-association, nature of wallets, different executive disciplines, low barrier to deployment, organic growth, and adaptation to faults and attacksP2P systems, like structured overlay networks, face numerous security difficulties in their unaltered state that render the network unstable. Additionally, data access is typically unrestricted on the P2P open landscape, which jeopardizes the stoner's data sequester. [4]. While social operations require a

suite of advanced- position services to lower the outflow while the operation is being developed, the majority of P2P strategies can help only offer veritably specified and low- position APIs.

2. SOCIAL NETWORKING CATEGORIES

2.1 Definition

In the traditional way, A more technical definition refers to it as a directed graph structure, while a social network is made up of actual people interacting in the real world. But in today's usage, the word "social network" frequently refers to a blend of the physical and digital worlds using online services. Social media communication is defined as" utilizing social media sites with a strong online presence to stay in touch with musketeers, family, or peers" in the environment of computer- intermediated communication. The social networking categories based on the scope, data, network and system is depicted as shown in Fig 1.

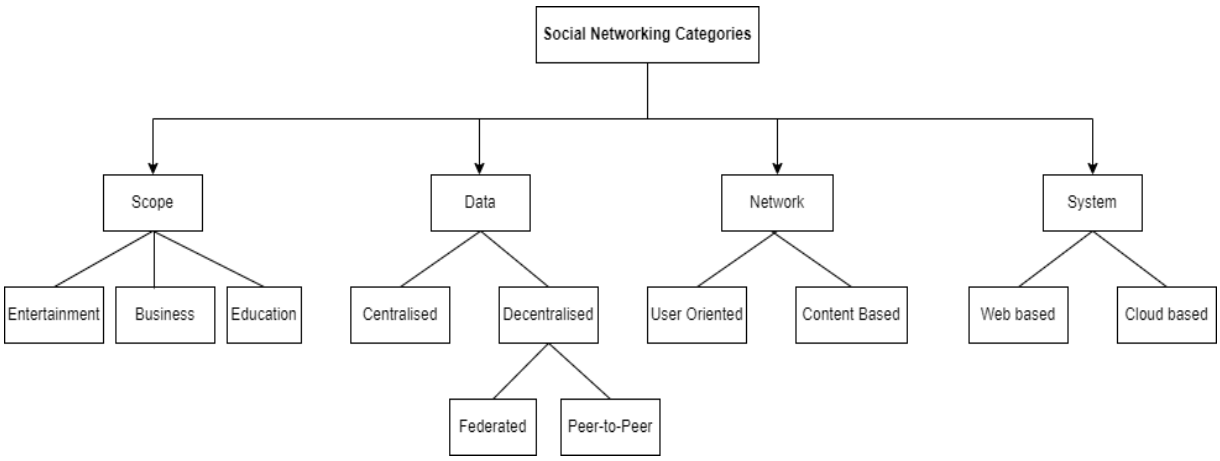

Fig 1. Social Networking Categories

2.2 Model Categories

The Scope Model

This model describes the core details of the application related to entertainment, business and education [5].

- Entertainment: This focuses on the fun and entertainment part of the applications, posting and sharing contents like pictures and videos etc. Eg: Facebook, instagram,Snapchat and whatsapp.
- Business: This focuses on the marketing and hiring strategies of the business model. Eg: LinkedIn and Naukri.
- Education: This focuses on the learning management, activities and monitoring purpose. Eg: Byju’s, LMS ,Coursera, Udemy etc.

The Data Model

This model gives a clear view of data being used. The model for programming paradigms is another name for it. It categorizes according to how data management is carried out, either uniformly or autonomously.

- Integrated client servers or client-servers that are not connected together manage all data in a centralized model with one administration domain.
- Decentralized model data administration needs to be decentralised, federated, or peer-to-peer because it is spread over several administrative domains.
- The peer-to-peer (P2P) paradigm is performed primarily, allowing users to connect with their reliable friends and share content with them. Developers use either preexisting P2P technologies or create their own P2P protocols..

The Network Model

The Network Model: The entity around which relationships within the system are built is the main focus of this approach. As a result, networks are frequently user- or content-oriented.

- User-oriented (profile-based) The focus is on the interpersonal connections that users have and how they distribute content within a community. Social networking sites like Facebook, MySpace, and LinkedIn are examples of security networks.
- Content-focused (content based) Instead of emphasising social connections, the system focuses on shared user interests. YouTube is just one example in this category.

The System Model

This viewpoint changes to the way that the application servers host and disseminate content. Thus, there are two categories as follows

- Web-based system The websites are hosted on application servers that belong to the service provider. The service provider directly manages the duties of assuring load balancing, managing failover, and sending requests to the appropriate application server. In these situations, the majority of the services provided to users are highly convenient.
- A cloud-based approach A utility computing infrastructure, such as Amazon Elastic Compute Cloud (Amazon EC2), hosts application servers, freeing the service provider to focus solely on the application. However, this adds extra expenses for the service provider, which occasionally trickles down to the customers directly or indirectly.

3. SECURITY ISSUES IN SOCIAL NETWORK

Social media has been compromised in terms of security, posing a serious risk to users' personal, intellectual, and professional assets. The purpose of this section is to describe the threats to security that social media users face. These security risks include those connected to privacy settings, identity theft, social engineering, anonymity, and information disclosure. Even said, some of these dangers may be avoided by merely educating consumers about the dangers that could exist [6].

3.1 Spam

Spam is unsolicited or unwelcome email or social media communication’s delivered to user’s accounts. Even while some have attempted to utilise them as an advertising approach, such messages are often malevolent. Spam has been used since the inception of communication networks on the Internet, and it has

developed along with those networks' technological advancements, not to improve them but rather as a means of avoiding the well-intended contact of legitimate account holders. Various media have been used to spread social spam. Text-based, image- or picture-based, and URL-based are a few of them. The text is typically excluded from URL-based social spam, leaving the user with only the link to see, numbing the victim's consciousness.

Images or advertising used in image-based social spam have the power to attract members of social networks to click them. This often directs the user to other internet computers where Trojans are downloaded into the system. Phishing is a motive behind the text-based social spam that is distributed. Utilizing the message filtering features offered by the SNS where the user has an account is the security precaution to be adopted in this scenario.

3.2 Malware

Malware is a result of harmful software. Malware is made up of Trojan horses, worms, and viruses. Koobface and Twitter Worm are examples of typical malware. A worm called Koobface propagated through social media sites like Facebook. Users may propagate this kind of worm by sending messages—which may take the shape of videos—to their pals. When a friend receives a message like this with a video link attached, the user may be prompted to download or update the Flash Player after clicking the link. If the user agrees to download the Flash Player, their computer may be infected with worms that can harm the computer system.

Another threat that frequently targets Twitter users is the Twitter Worm. One of these worms, called Profile Spy, enables attackers to tweet links for third-party applications called Profile Spy, which, when users click to download them, prompts a form to collect personal information from them. Using this information, the worm then tweets malicious messages to the user's followers on Twitter. Another worm that is well-known on Twitter provides phoney invitation links that lead people to malicious attachments containing email addresses from infected machines. It spreads by copying itself onto portable devices and folders.

3.3 SQL Injections

Developers of web applications have experienced SQL injection attacks on their databases. Attackers exploit the technical method of SQL injection to access databases. The majority of the responsibility for mitigating this attack resides on the social network's developers in order to protect user profiles. Insecure social network apps' underlying databases are sensitive to fraudulent SQL queries from hackers.

3.4 De-Anonymization Attack

In social media platforms, anonymization enables individuals to disguise information that could identify them. These details could contain things like their names, photos, addresses, and other private information.The reason of this anonymity is to protect customers from 0.33% events who violate their privacy together with advertising, programme developers and facts mining researchers Nevertheless, certain studies have demonstrated that it is easy to deanonymize users of online social networks.

According to Wondracek et al, Anonymity can be removed from an online user and even the social network membership group they are a part of by using public records like marriage and birth information. Additionally, the study demonstrated that there is a chance to de-anonymize a user using a mixture of data about a person that may be gathered from various online communities. De-anonymization attacks are now another method that attackers on social networks employ to get around users' privacy settings [7].

3.5 Stalking and Corporate Espionage

Information leakage cost such organizations great loss either on financial terms or reputation ground. Social media sites continue to be used as a base for encouraging workers to provide confidential corporate information without their knowledge. Some of this information was shared on social media without the owner's knowledge or consent for uses that were not intended. For instance, Scott McClellan, vice president of cloud services at Hewlett-Packard, made a mistake on his LinkedIn page when he revealed the specifics of HP's cloud-based computing system. Nonetheless, the news media learned of the total secrecy before he could remove it from his LinkedIn page, which prompted Microsoft and Amazon to study further about HP's strategy in this regard.

4. SURVEY ANALYSIS ON SOCIAL MEDIA AND SECURITY

Aljohani et. al. conducted an inclusive survey to discover the level of social networking site expose the personal information [1]. They evaluated at the information they reveal, their understanding of how SNSs protect their information, and their awareness of potential risks associated with oversharing. He and Wu conducted a survey to examine the security element of mobile social media, spot current trends, and offer advice for scholars and practitioners in this quickly developing sector. [2]. Imrul Kayes, Adriana Iamnitchi provided an overview of the privacy and security issues that emerged so far in OSNs. A Taxonomy of security and confidentiality attacks in OSNs was developed, along with existing mitigation techniques. A review of the remaining difficulties was also done. [3]. A questionnaire was constructed and distributed to analyse the awareness on the topic. The received responses are summarized as follows:

4.1 USAGE OF SOCIAL NETWORKS

- In the current generation most of the young people, the youths between the age group of 18-25, the students are the ones using social media the most. As their developmental needs are well matched with what social media has to offer—forming friendships, determining their identities, establishing social status by being "in the know," and being at least somewhat aware of the scams taking place through it—this shows that this age group uses social media at the highest rate. 48.5% of the survey participants utilize social media for 2-4 hours daily. Under 18 respondents can be seen that they are unaware of the scams, violence and threats occurring through social media platforms.

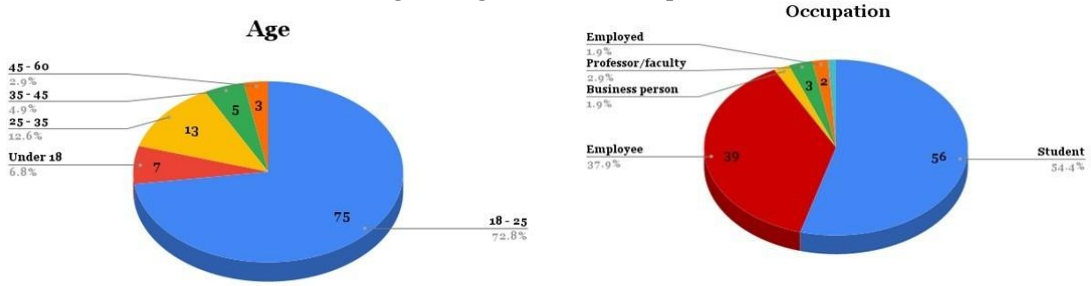

Fig 2. Responders Age and Occupation

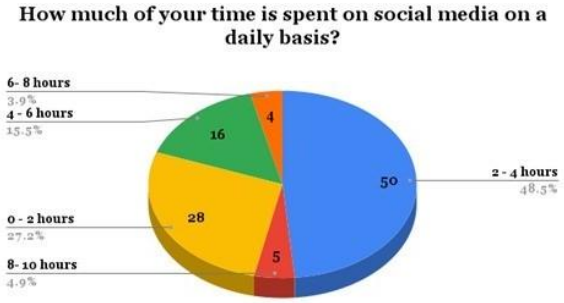

Fig 3. Responders Time Usage Analysis

- Moreover, the frequently used social platform is Instagram (trending app), it's because the application is made in such a way that people could interact with each other effectively and the entertainment is up to the mark like reels, posting ofpictures, promotions and many more which has affected the users psychologically. There are security measures available in these platforms like two factor authentication, private account, blocking and restriction also reporting any accounts according to the problem.

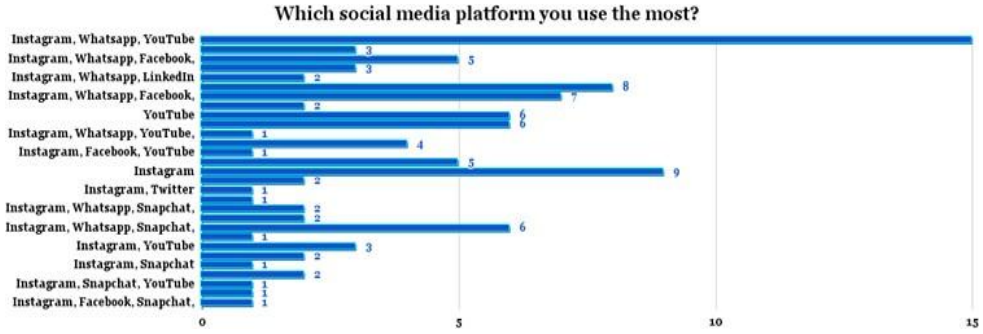

Fig 4. Most Used Platform listed by Responders

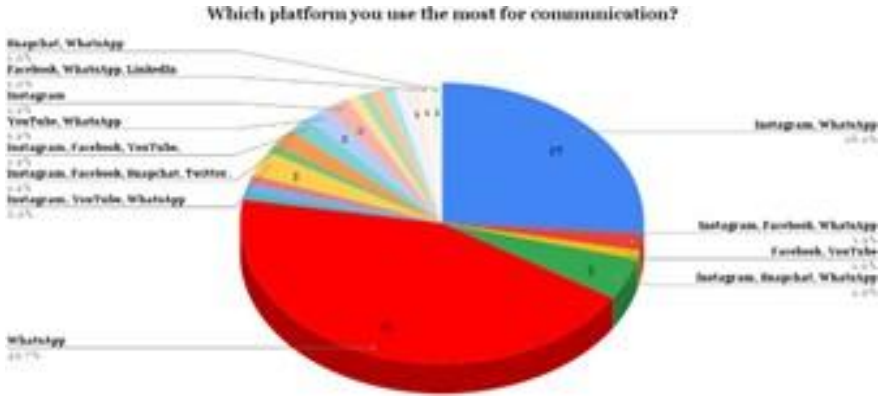

Fig 5. Most Used Platform for Communication

4.2 PRIVACY CONCERN AND SECURITY

Everyone is concerned about their personal data in relation to privacy and confidentiality. Confidentiality is something which can be authorized only by the particular user, Integrity is all about if any data is modified or any data are taken by unauthorized people, Availability is the requirement when needed while using the social media platform for their security purpose. Social media have invaded privacy in this generation, as of

the answer, it may be understood that it involves monitoring the activities of users online forum.

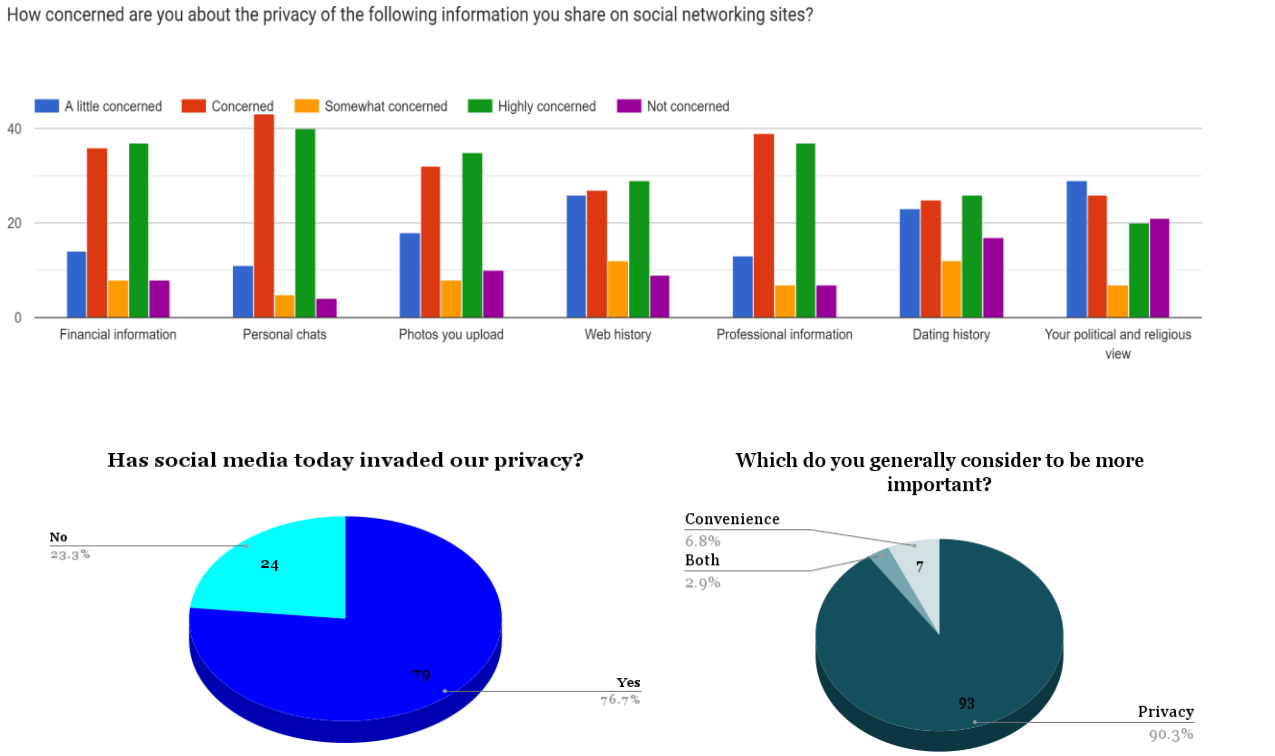

Fig 6. Privacy Concerns of the Responders

- People don't read any terms and conditions prior to installing any applications, let it bethe updates, new versions of any applications, this ignorant factor puts people in trouble sometimes. It is a must to read terms and conditions before installing any applications. Without the knowledge of users, it takes the data, and we give access to our data from our devices. WhatsApp has end to end encryption too, where one person messages can't be read by any third party, but till what state is this fact true, all the users believe in end-to-end encryption of messages, All the messages will be stored in cloud by the WhatsApp database which is in use. It is safer to use it when we have proper security features.

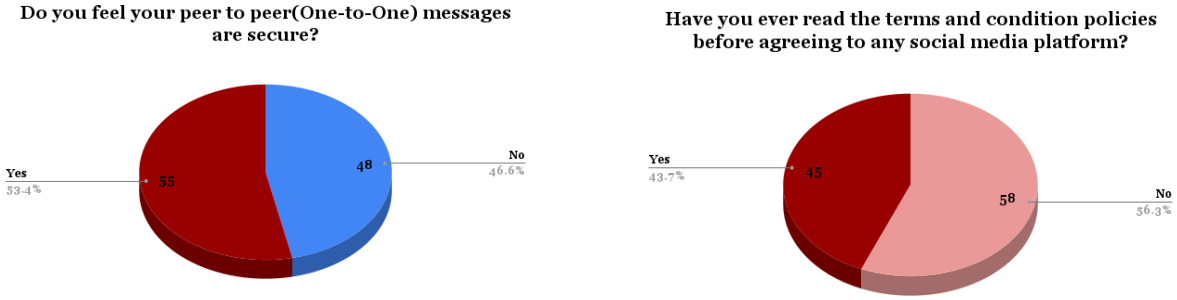

Fig 7. Security Concerns of the Responders

4.3 IMPACT ON WELL BEING

The heavy social media usage is linked to higher likelihood of sadness, anxiety, loneliness, and self-harm and even bad thoughts which may lead to a negative path. Social media can promote negative experiences

or spread negative messages and thoughts. Due to long time usage of social media before sleep, it reduces the hour of sleep which causes stress and may affect the mental health. A survey was conducted if social media has an adverse effect on the well-being of a person and the results were collected. Based on the survey 80.6% that is 83 people have selected the option yes that it has an adverse effect on well-being and 19.4% thatis 20 people have chosen the option as no which according to them social media does not cause or have an adverse effect on a person's health or life.

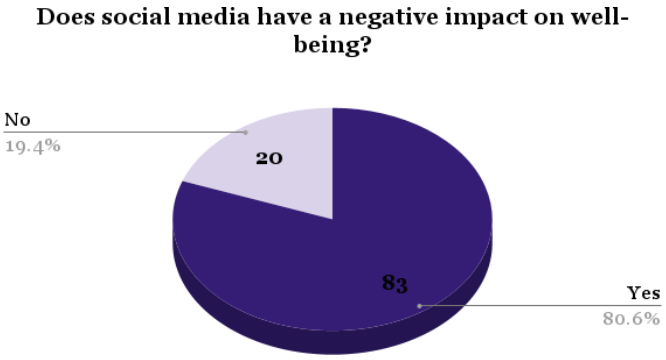

Fig 8. Wellbeing Concerns of the Responders

4.4 VIOLENCE, THREATS & SCAMS

However, like using social media grows, there are growing concerns about how it can be used for exploitative purposes. Using social media to spread misinformation and promote intolerance is a major concern for many governments and regulators. However, there are also concerns about how social media platforms can be used to spread e-commerce fraud andother unfair trade practices through social media posts and misleading advertisements.Likejacking is more sneaky than it is harmful because it deceives the user into like something without their knowledge.

Social media competitions are well-liked and generate a lot of activity, but they can also have a trap door in the form of phoney gifts designed to deceive users into giving up their private information. Any scam's goal is to make money. If con artists aren't making money, they'll need to move on to a new scheme or piece of technology. Affiliate programs are frequently the source of funding for social media scams. Affiliate schemes are incentive programs in which businesses pay an affiliate to bring traffic or new subscribers to their website. Every year, millions of individuals are victims of identity theft. A lack of awareness, greater confidence in social media, and a lack of data standards for data acquired on social media all play a role. The rise of social advertising also plays a role, as consumers give up massive quantities of personal information - frequently without even realising it. From the survey conducted, 41% of respondents agree that social networking sites are dangerous to privacy and 94% of them are aware of scams, also 79% of respondents agree that social media can contribute to violence.

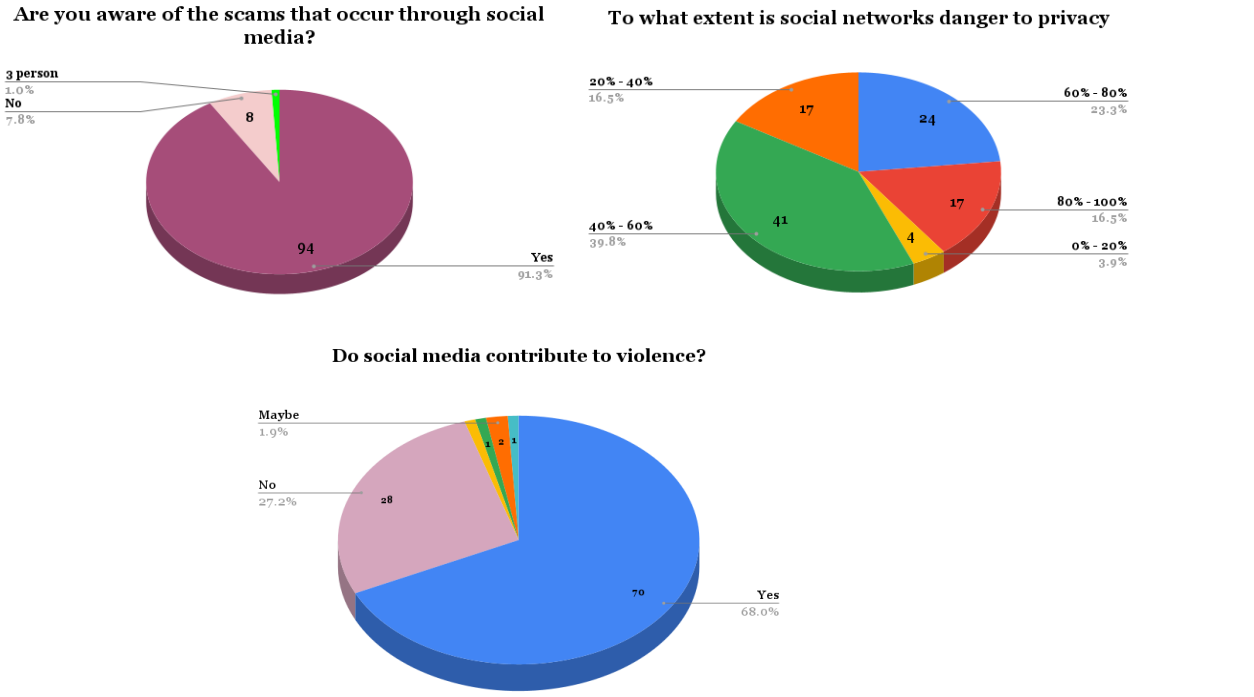

Fig 9.Violence, Threats and Scams Awareness

4.4 TRANSACTION SECURITY ON SOCIAL PLATFORMS

Transaction security is the most important and fundamental form of security checking that is required to secure the payment through online using social platforms. Phishing schemes endanger the security of social media information. Giving buyers and seller's privacy during transactions and defending the client-server network against malfunctions and outside threats are also concerns of transaction security. Social media is frequently flooded with reports of data breaches and dangers to consumers' security during safe online transactions. To studythe knowledge or to what extent people use social media transactions, a survey was conducted. 45 that is 43.7% individuals agree that 60% to 80% of transactions are safe through social media and 24.3% that is 25 individuals go on with 40% to 60% transactions are safe. The remaining 10.7% that is 11 opted that 80% to 100% of the transactions are safe through social media and 10.7% that is 11 people go on 20% to 40% of transactions done are secure through social media. 7.8% that is 8 people have an opinion that 20% of transactions done are secured though the social media platform.

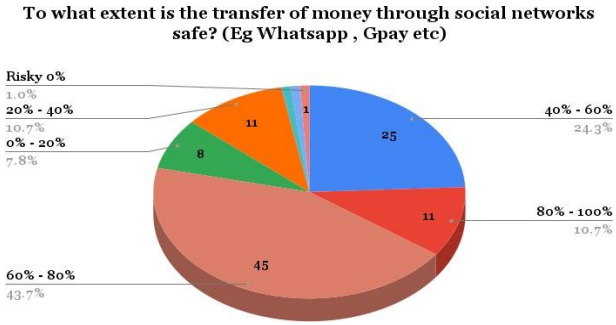

Fig 10. Responders View on Transaction Security

5. CONCLUSION

In this Research we have shown the emergence of social media due to the pandemic and the study on Social networks and Social network security. Social networks are used amongpeople from different areas and fields. Nowadays peer to peer networks are really convenient and important for everyone all over the world. We have discussed social networking categories in detail and even the security issues occurring in the day to day life for a social network user. The survey has taken how the social media network has caused the impact on each individual. We have concentrated on the study on security of a P2P Social network.

References

[1] Aljohani, M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users privacy settings & information disclosure. In Johnstone, M. (Ed.). (2016). The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia. (pp.67-75).

[2] He, Wu. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. Information Management & Computer Security. 21. 10.1108/IMCS-12-2012-0068.

[3] Imrul Kayes, Adriana Iamnitchi, (2017) Privacy and security in online social networks: A survey, Online Social Networks and Media, Vol. 3–4, Pages 1- 21,ISSN 2468-6964, https://doi.org/10.1016/j.osnem.2017.09.001

[4] Masinde, N., Graffi, K. Peer-to-Peer-Based Social Networks: A Comprehensive Survey. SN COMPUT. SCI. 1, 299 (2020). https://doi.org/10.1007/s42979-020-00315-8

[5] Masinde, Newton & Khitman, Liat & Dlikman, Iakov & Graffi, Kalman. (2020). Systematic Evaluation of LibreSocial—A Peer-to-Peer Framework for Online Social Networks. Future Internet. 12. 140. 10.3390/fi12090140.

[6] Obiniyi, Afolayan & Olaide, Oyelade & Obiniyi, P. (2014). Social Network and Security Issues: Mitigating Threat through Reliable Security Model. International Journal of Computer Applications. 103. 1-7. 10.5120/18099-9163.

[7] Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010, May). A practical attack to de-anonymize social network users. In 2010 ieee symposium on security and privacy (pp. 223-238). IEEE.