Exploring Privacy Vulnerabilities and Security Frameworks in Online Social Networks

Dr.S.Srinivasu

Associate Professor, Government Degree College(A), Khairatabad

Abstract

Online Social Networks (OSNs) have transformed the way people communicate, share information, and interact in the digital world. These platforms enable users to create profiles, build connections, and exchange various types of content such as text, images, and videos. With the rapid growth of OSNs, a vast amount of user data is generated, including personal, behavioural, and location-based information. While these features enhance user experience, they also introduce significant privacy and security challenges.

This paper presents a comprehensive study of data in OSNs, including user profile data, connections, interaction data, and behavioral patterns. It examines different types of online social networks and their functionalities. The study highlights major privacy issues faced by users, such as unauthorized data access, identity theft, information leakage, and third-party data misuse. It also discusses provider-related concerns, including data collection practices, lack of transparency, and risks associated with content recommendation algorithms.

Furthermore, the paper explores various threats in OSNs, including phishing attacks, malware, spam, cross-site scripting, and modern threats like de-anonymization and inference attacks. To address these challenges, several security mechanisms are analyzed, such as encryption techniques, privacy settings, access control methods, and user awareness strategies. Legal and regulatory frameworks related to data protection are also considered.

In conclusion, ensuring data confidentiality and user privacy in OSNs remains a critical challenge. Effective security measures, combined with user awareness and proper privacy management, are essential to create a safer and more secure online social networking environment.

1.1 DEFINITION OF OSNs

Digital platforms called Online Social Networks (OSNs) [01] make the people comfortable to share data and engage socially online. By connecting with others and building information-rich personal profiles, users establish communication networks. These platforms enable users to share experiences, ideas, and multimedia with their connections in a variety of content types, such as text, photographs, and videos. OSNs facilitate community formation and involvement with features including groups, comments, and messaging. Users may manage how visible their profiles are via privacy settings, and news feeds create material depending on user activity.

OSNs, which are accessible via mobile applications and online browsers alike, are becoming essential to contemporary communication since they allow for worldwide connectivity and provide forums for social, business, and personal exchanges. OSNs are dynamic, reflecting both user preferences and continuous technological improvements.

Online social networks are developing rapidly due to the quick iterations of information technology, and as a result, their networks are getting bigger and more intricate [02]. The algorithms needed to handle social networks and the associated issues they raise are likewise getting more and more numerous. Although the associated privacy protection algorithms—such as differential privacy protection, access control strategy, and encryption algorithms—have been researched and examined, the issue of privacy disclosure remains unresolved. To achieve the perception and protection of users' safe material, this article first properly filters and searches the pertinent data and content of online social networks using a deep convolution neural network algorithm.

Compared to 84% in 2018–19, 87% of adults reported using social networking sites or apps in the previous year in the United Kingdom. For age groups above 45, there was an increase in social networking use [03].

Two reasons are provided by the literature for looking into OSNs in CMC research in the era of digital networks. Firstly, OSN research aligns with the network structure of computer-mediated interactions and interaction, shifting the focus of CMC research "from individualist, atomistic, and essentialist explanations towards more relational, systemic, and contextual explanations of social phenomena." Such variations escape the pitfalls associated with trying to peer into the mysterious "black box" of emerging social technologies, and instead provide a more theoretically sound and practical understanding of different types of CMC and provide a suitable explanation. Second, OSNs go beyond some social technologies in that they rely on connectivity to function.

Over the past 20 years, the research of OSNs in communication field has increased in comparison to social network method. There are now primarily two research streams. First, some academics confuse social technologies, especially SNSs like Facebook, with OSNs and use these terms interchangeably [04]. Their findings suggest that when actors use social technologies, they engage in social interactions with their connections. The another line of inquiry focuses on the social networks that serve as the foundation for OSNs, as well as how they manifest in computer-mediated or non-mediated forms.

1.2 DATA IN OSNs

Data is a crucial element of Online Social Networks (OSNs), including many forms of information generated and shared by users on these platforms. The nature of data in OSNs is important for consumers, decision-makers, and scholars to understand [05]. The key points about data in OSNs are summed up as follows:

1.2.1 User Profile Data: In Online Social Networks (OSNs), user profile data refers to a range of information that users willingly contribute to establish and define their online identities. These profiles are

built around fundamental personal information like name, birthday, and gender. To facilitate communication, users frequently give contact details like phone numbers or email addresses.

1.2.2 Connections and Networks: In Online Social Networks (OSNs), the connections formed by friends and followers generate a dynamic social graph that displays information flow and impact patterns. Communities are shaped by the density and clustering of these networks, and trends and the quick spread of information within the network are facilitated by powerful users. The structure and characteristics of these relationships are frequently studied through social network analysis, which sheds light on user behavior and network dynamics.

1.2.3 Content and Interaction Data: Users create and exchange information through content and interaction data in Online Social Networks (OSNs), which shapes user engagement and the overall experience. While interactions take the form of likes, shares, and comments, users also offer a variety of material, including posts, images, videos, and comments.

1.2.4 Behavioral Data: When discussing Online Social Networks (OSNs), the term "behavioral data" refers to the data that documents user behavior, interactions, and engagement patterns on the platform. This contains information about how often users log in, how long they spend on the site, what kinds of material they see, like, or share, and what kinds of social connections they have. Understanding user preferences, trends, and the general dynamics of user involvement may be gained by analyzingbehavioral data.

1.2.5 Location Data: Users' physical whereabouts are revealed through location data in Online Social Networks (OSNs), which offer insights into their travels and activities offline. Users frequently tag certain locations in their posts, images, or check-ins, or they reveal their present position.

1.2.6 Preferences: Online Social Networks (OSNs) allow users to customize their experience based on their preferences, which include privacy settings, content interests, and notification preferences. Users may customize their involvement inside the OSN environment and have control over their online interactions thanks to these customizable choices, which also include connection preferences. A more user-centric and fulfilling OSN experience is facilitated by acknowledging and respecting these choices.

1.2.7 Temporal Data: Within Online Social Networks (OSNs), temporal data pertains to details on the order and time of user actions and content interactions. It contains information on when users check in to the site, publish material, and interact with postings. Understanding temporal patterns helps one understand posting trends, peak activity times, and changes in user behavior over time.

1.2.8 Login Credentials: The majority of OSNs demand or permit user login to use the service. The login credentials include this login information. This is also present on more established websites. As stated, not all OSNs incorporate data from the aforementioned categories. This primarily depends on an OSN's level of media richness, the functionality it provides for users, and its business model. Nearly information is exclusively accessible to OSN (i.e., its operators or software), whereas additional data is also accessible to portion of OSN users. Additionally, some information is provided to the OSN implicitly through actions

made within the OSN, and other information is provided expressly through the provision of this information.

1.3 TYPES OF OSNs

Multiple applications comes under the umbrella of OSN [06]. Some of them are mentioned below.

1.3.1 Dating: These days, several dating services include OSN components in their search to assist people in finding the love of their lives. Each user has a login name and password, as well as a profile to entice possible partners. Love interests are the most common type of connection, but friendship ties and group affiliations are also frequent. Instead of using connections already in place, accessing the OSN frequently relies on searches or recommendations. These systems are more efficient because of algorithmic matching, which takes preferences and geography into account. These OSNs' interactive features, such as their chat and message systems, give users a way to build relationships virtually by connecting with others. The secret to OSNs' dating success is their ability to employ technology to match people effectively while taking privacy, safety, and ethical issues into account to make the process pleasant and easy to use.

1.3.2 Business: These OSNs are designed to connect professionals with beneficial industry contacts. Finding profiles does not always involve registering. A user's capabilities and line of work are displayed in their profile, along with a way to get in touch with them. Typically, communications sent via the OSN are used for this. LinkedIn is an illustration of this category; it charges a monthly fee for its premium features.

1.3.3 Enforcing Real-Life Relationships: These OSNs focus on (re)connecting with old friends and acquaintances rather than making new ones. Examples include networks like MyLife and Plaxo that are family-focused, college- or ex-classmate-focused OSNs. [41]

1.3.4 Socializing Corresponds: In Online Social Networks (OSNs), socializing is a dynamic activity centered on making connections, exchanging a variety of information, and interacting digitally. By interacting with friends and acquaintances, users create social connections that serve as the foundation for a network of relationships. Everyone on the site may express themselves and add to the group discussion by sharing content, which includes text, photos, and videos. Messaging and commenting are examples of communication tools that facilitate private and public conversations, encouraging involvement in real-time and improving the social experience in general. Through socializing in OSNs, people may connect, exchange, and communicate in a digital arena that reflects and expands on real-world social interactions.

1.3.5 Content OSNs: Focused on content online social networks, or OSNs, are platforms where people trade, explore, and interact with many kinds of content. Instagram is a visualfocused OSN that encourages photo and short video sharing, which in turn fosters visual storytelling. YouTube is a video-focused social network that enables users to create, share, and engage with a wide variety of video content. Pinterest emphasizes visual discovery by letting users choose and investigate topics through picture sharing. With an emphasis on long-form content creation and consumption, Medium serves readers as well as authors. By demonstrating the various ways in which users engage with and contribute to information, these OSNs serve as a representation of the evolving nature of social interactions in the digital domain.

1.3.6 Content Recommendation: Sophisticated content recommendation algorithms are used by Online Social Networks (OSNs) to improve user engagement and experience. Algorithms are used by sites like Facebook to construct personalized News Feeds, suggesting multimedia material and posts based on user interactions and interests. Instagram curates content on its Explore page based on users' interaction history and interests.

1.3.7 Entertainment: Entertainment-focused Online Social Networks (OSNs) satisfy consumers' need for interesting and entertaining content. With its brief videos, TikTok has developed into a center for original and viral entertainment. Snapchat offers consumers an engaging and enjoyable experience with its interactive aspects and multimedia capabilities. Reddit provides a wide variety of amusing material via debates, memes, and specialized communities. Originally designed with gaming in mind, Discord has developed into a community-focused network where users can share movies, and memes, and take part in live streams.

1.3.8 Advice Sharing: Through question-and-answer formats and specialized communities, users may seek and exchange advice on Online Social Networks (OSNs) such as Quora and Reddit. The professional network on LinkedIn includes talks among groups with a specific sector that provide ideas.

Table 1.1 Comparative of various features for different types of OSN

Feature	Social Networks (General)	Media Sharing Networks	Professional Networks	Microblogging	Forum Communities
Primary Focus	Connecting with friends , family, and acquaintances	Sharing and consuming multimedia content	Building professional relationships and career development	Sharing short, frequent updates (microposts)	Sharing knowledge and discussions on specific topics
Content Type	Varied (text, photos, videos, links)	Photos, videos, live streams	Resumes, portfo-lios, job postings, industry news	Short text updates (tweets, posts)	Text-based discussions, threads, Q&A
User Interaction	Friendships, following, messaging, groups	Uploading, commenting, liking, sharing	Networking, endorsements, recommendations	Posting, following hashtags/topics, retweeting	Thread replies, up/down votes, member roles
Privacy	Varies, often customizable	Public or semi-private sharing op-tions	Focus on professional profiles, may have privacy settings	Public or semiprivate, character limits can impact privacy	Varying levels of anonymity, often moder-ated
Examples	Facebook, Twitter, Instagram	YouTube, Pinterest, TikTok	LinkedIn	Twitter, Mastodon	Reddit, Stack Overflow

The Stack Exchange Network, which includes websites such as Stack Overflow, promotes cooperative learning and problem-solving by enabling focused advice exchange in certain disciplines. These OSNs provide online communities where people may interact, exchange ideas, and look for advice on a wide range of subjects. Table 1.1 shows comparative for various features of different types of OSN.

1.4 USER RELATED PRIVACY ISSUES

The vast gathering and processing of personal data are at the center of user-related privacy concerns in Online Social Networks (OSNs). This is done on purpose (snooping, hacking), accidentally (users managing privacy settings incorrectly), or both, and the results could be disastrous [07]. Let us examine various privacy issues that include user-to-user disclosure.

OSNs' practice of data profiling, in which they collect information about user's interests and behaviors, gives rise to worries about possible abuse and illegal access. There are hazards associated with third-party app integration in OSNs since users could unintentionally give access to their personal information. Complicated privacy settings and default choices may expose information inadvertently, and user tracking for behavioral analytics raises concerns about monitoring and improper use of data. Addressing these privacy concerns and promoting a safe online social environment need to make sure that visibility controls are transparent, data practices are open and honest, and user education is strong.

Aspects like these concern customers' profiles, relationships with other users, messages, multimedia, tags, or group memberships. The information in OSNs is much more widely available than its owners may have thought and may even make it into the media. Even internet security specialists occasionally disclose information incorrectly.

In real life, humans can regulate the various social settings, but in online social networks, the boundaries between them frequently become hazy. Not all OSNs give users the ability to conceal information at this degree of specificity. Since users cannot choose to behave differently toward one user or set of users compared to another.

Various Users Posting Details about a person. The person has control over the information he wants to post to an OSN. Messages from the OSN frequently include details about several users. Information being released to the public beyond what was intended, which is a problem related to the disclosure border. It can happen when another user uploads information about you to the OSN that you don't want to be there or when information that you privately shared with another user is made public. This may even be a purposeful action.

1.5 PROVIDER RELATED PRIVACY ISSUES

Concerns about the practices and rules that platform providers themselves apply are included in the category of provider-related privacy problems in Online Social Networks (OSNs) [08]. Users are worried about the scope of data collection and retention, as well as the openness of these practices and the length of time that their data is kept on file. Concerns regarding the distribution and filtering of user material are raised by the opacity of algorithms employed for content curation and recommendation. Concerns over the unconsented disclosure of personal information to third parties for commercial gain are also raised by users. Government monitoring, policy modifications, and security lapses all add to the intricate web of OSN privacy concerns. To tackle these issues, open communication, easily navigable privacy settings, and

continuous endeavours to harmonize legal adherence with strong privacy safeguards are necessary. To create an atmosphere where OSNs are more privacy-conscious, user advocacy and education are essential.

1.6 PRIVACY SETTINGS AND MANAGEMENT

Online social networks (OSNs) provide users with important tools to regulate the display of their information and actions on the network, including privacy settings and administration [09].

In Online Social Networks (OSNs), profile privacy is a key feature that gives users control over who may view their data and activity. Users may choose who has access to their profiles using configurable visibility settings; choices include the public, a more limited group of friends, and customized lists. Users can protect sensitive data since this control covers personal information like names, contact details, and places of employment. Users may also control how visible each of their postings is, allowing them to strike a balance between sharing material with their network and preserving some privacy.

As an assessment tool, a privacy score derived from an Online Social Network (OSN) profile's visibility and sensitivity would indicate how well a user protects the privacy of their data. This score would take into account things like the submitted content's nature, the visibility settings selected, and the sensitivity of the shared data. A higher score would be indicative of a diligent attempt to restrict access to private data, choosing more stringent visibility settings, and following industry best practices. It would also take into account the user's proficiency in navigating third-party app permissions and integrating extra security measures. Users are given insightful feedback by such a privacy score, which promotes responsible and knowledgeable management of their online presence in the OSN environment.

Improving user privacy awareness in Online Social Networks (OSNs) requires putting methods into place that make clear the possible outcomes of their actions. During onboarding, interactive tutorials and guides can provide a visual representation of how various privacy settings affect the availability of personal information. Incorporate a privacy inspection function that leads users through their present configurations and warns them of possible threats, encouraging a proactive approach to managing their privacy. Real-time feedback from context-specific warnings and notifications can nudge users back before disclosing critical information. By using these strategies, OSNs may provide users with a better awareness of the ramifications of their choices, encouraging them to make responsible and knowledgeable decisions about how to manage their online privacy.

1.6.1 Encryption: Encryption is a key component in safeguarding Online Social Networks (OSNs) administration and privacy settings. End-to-end encryption ensures that user interactions private messages in particular remain confidential. Because only the sender and intended receiver can interpret the content, this lessens the chance of unauthorized access [10].

Moreover, overall security is improved when secure transmission protocols, such as HTTPS (SSL/TLS), are used when data is sent between users' devices and OSN servers. Sensitive data, such as login passwords and personal information, is shielded from possible surveillance or eavesdropping during data transfer using this encryption technique.

Data-at-rest encryption should be implemented by OSNs as well to fully solve privacy issues. This entails encrypting user data that is kept on the OSN servers to provide an extra degree of security against unwanted access to the data. This safeguard makes sure that encrypted data is unintelligible without the right decryption keys, even if the server is hacked.

Comprehensively, encryption secures communication channels, guards data during transmission, and strengthens stored information against possible intrusions, making it a strong defense for privacy settings and administration in open social networks. OSNs may greatly improve their platforms' overall security and privacy posture by using these encryption techniques, giving users more confidence that their sensitive data is protected.

2.6.2 Awareness, Law, and Regulations: Online Social Networks (OSNs) are impacted by several factors, including user awareness, legislation, and regulations designed to protect user privacy and promote responsible digital behaviour [11].

Within OSNs, user education and awareness initiatives are essential for encouraging appropriate online behaviour. Platforms can take steps to educate users about data-sharing consequences, privacy settings, and other hazards related to their behaviour. To address privacy problems inside OSNs, some nations and regions have passed legislation and regulations. These rules specify platform operators' obligations, user rights, and data protection regulations. Knowledgeable people are better able to make judgments about their security and privacy on these sites. For instance, The Digital Personal Data Protection (DPDP) Act, 2023 was enacted by the Indian Parliament at the beginning of August 2023. The new law was passed after more than five years of discussion and is the first cross sectoral law on personal data protection in India. In the United Kingdom, the General Data Protection Regulation (GDPR) is being enforced under the Data Protection Act of 2018. Everyone who works with personal data must abide by strict criteria known as "data protection principles."

To control user behaviour, OSN operators frequently create their own privacy rules, community guidelines, and terms of service. These guidelines specify content standards, permitted usage, and the repercussions for breaking platform guidelines. Maintaining a secure and civilized online community depends on making sure users understand and accept these regulations throughout the on boarding process.

1.7 PRIVACY ISSUES OF ONLINE SOCIAL NETWORKS

Previous studies on the privacy problems with online social networks served as the inspiration for this research. Information sharing in online social networks has been linked to potential hazards. Online social networks (OSNs) pose serious privacy concerns, including difficulties with data collecting, third-party access, and user monitoring. Concerns over the possible abuse of information for targeted advertising are raised by the comprehensive profiling of users' preferences and personal information. Giving third-party apps access within OSNs puts your privacy at risk since their standards for data security may differ. Intricate privacy configurations and default settings may lead to inadvertent disclosure of personal data,

and worries over monitoring and data misuse are reinforced by user tracking and behavioural analytics. The complex web of privacy concerns inside open social networks (OSNs) is further compounded by security lapses and location-based data sharing, underscoring the necessity of all-encompassing safeguards to protect user data and promote a safer online social milieu [08].

Multi-hop inference and Bayesian inference were applied in social networks to predict personal characteristics based on the friends and friends of friends of the persons who were the targets. Their findings demonstrate that eliminating linkages or user traits by themselves is insufficient to prevent inference attacks.

An external attacker can attempt to locate a target person in online social networks by using publicly accessible attributes of specific individuals. This type of attack is known as a navigation privacy attack. This method maximizes the usage of attributes like location, age, and propensity to associate social closeness while doing network searches. Research on Facebook and Google+ showed that most people could be found successfully by an attack if only a few peripheral details about the target were known, but in two instances, the attacks failed. Initially, the users can only disclose information that differs from their own to a small number of friends or other users.

Secondly, it is typically more difficult to find users in big cities on Facebook than other users. User interests can reveal information about users that is sensitive to privacy, as demonstrated. Consider the use of music preferences to infer sensitive personal information about Facebook users. This strategy simply considers a user's traits rather than their social connections or group memberships, the calculated user similarity, demonstrated how their model could be used to forecast information that was hidden and suggested that online social networks should openly hide the majority of user data by default.

The efficacy of three assault scenarios—friend-list recovery, profile recovery, and postrecovery attacks in terms of uncovering confidential information on Facebook was assessed. It was found that by using standard web requests, the suggested attacks could be successful in recovering sensitive data from a target user.

1.9 SOCIAL MEDIA'S CLASSIC AND MODERN THREATS

Due to social media's broad use, internet users now face security and privacy threats. These risks can be separated into traditional and contemporary hazards.

1.9.1 Classic Threats: Conventional risks have existed virtually from the inception of the Internet. Phishing, malware, spam, and cross-site scripting (XSS) attacks are some of these risks [12]. Even while OSNs have already helped researchers and industry address these risks, issues can still arise and spread faster than in the past. By tailoring the threat to match the personal characteristics of the target users, classic threats are used to obtain personal information provided by users over an OSN and attack both the target users and their friends.

Phishing Attacks: Online Social Networks (OSNs) are targets of phishing attacks, which take the shape of numerous misleading strategies intended to gain users' confidence and deceive them into disclosing sensitive information. Making fictitious login pages that closely resemble authentic OSN login screens is one such technique. People, who are frequently lured to these phony websites by phishing links, unwittingly divulge their login information, giving attackers access to their accounts without authorization.

Malware: The danger posed by malware in Online Social Networks (OSNs) is complex, taking advantage of the interconnectedness of these platforms to undermine user security. Phishing attacks frequently use misleading links to expose users to malware, which can result in the installation of dangerous software or the revealing of private data. Additional threats come from third-party plugins and infected software, which cause users to inadvertently download malware from unreliable sources. Malvertising, clickjacking, and likejacking take advantage of user interactions on open social networks (OSNs) to fool people into clicking on misleading adverts or hidden features that might infect them with malware.

Spam Attacks: Spam attacks on Online Social Networks (OSNs) can take many different forms, annoying users and perhaps putting their security at risk. One popular technique used by spammers to spread unwelcome information or obtain access to user networks is the establishment of fictitious identities and profiles. Users' feeds are cluttered with unsolicited messages, comments, and friend requests that contain phishing links or adverts, which degrades the quality of their OSN experience. To draw people, spammers may create and fabricate pages or events, which they then utilize as platforms to spread spam. Clickbait strategies and the presence of dangerous links in messages, postings, or comments entice readers to interact with potentially hazardous material.

Cross-Site Scripting: Cross-site scripting have substantial security concern to Online Social Networks (OSNs) since it enables attackers to introduce malicious scripts into various platform sections. Malicious actors may utilize vulnerabilities to introduce scripts into user profiles, postings, or comments. These scripts will begin to execute when other users read them. This might lead to several evil deeds, including data theft, session hijacking, and unauthorized access to user accounts. Clickjacking attacks, in which unseen things are superimposed over OSN content and users are tricked into interacting with the concealed pieces, can also be enabled by XSS.

1.9.2 Modern Threats: Usually, OSNs are where these threats are observed. Most contemporary attacks aim to obtain personal information about victims and those they know. For example, an attacker might be interested in learning about a user's present job. It is simple to view someone's Facebook privacy settings if they are set to public. However, only their friends might be able to see it if they have a specific privacy setting activated.

Clickjacking: Clickjacking poses a serious security issue in Online Social Networks (OSNs) because it employs devious methods to trick users into interacting with hidden features. Malicious actors overlay buttons or links, or other undetectable features, on top of ostensibly harmless OSN content. Users may click on these hidden components by accident and inadvertently initiate undesired actions if they are

unaware of them. One instance of this is when phony "Like" or "Share" buttons are deliberately placed above authentic OSN content, leading users to inadvertently share or support stuff they did not intend to.

De-Anonymization Attack : Attacks known as "de-anonymization" are directed at members of online social networks (OSNs) who have chosen to remain anonymous or go by a pseudonym. These attacks use a variety of techniques to connect purportedly anonymous accounts to actual identities. Cross-referencing information is a popular method in which attackers gather publically accessible data from various sources and compare it with information from OSN profiles. By using information like as usernames, connections, or hobbies, attackers can identify the real person behind the anonymous account.

Identity Clone Attacks: In Online Social Networks (OSNs), identity clone attacks refer to the process of creating false profiles to mimic authentic users, potentially resulting in deceit, disinformation, or fraudulent acts. The clone is almost indistinguishable from the original due to the painstaking replication of features from the target's legitimate profile, such as profile photographs and personal information. These assaults may be carried out for a variety of reasons, including disseminating false information, carrying out phishing schemes, or harming the reputation of the persona. Identity clones may target connections for phishing efforts or engage in scams by taking advantage of confidence inside the victim's network.

Inference Attacks: Online Social Networks (OSNs) are vulnerable to inference attacks that make use of seemingly innocuous data to infer private information about users. One popular method is friendship inference, in which adversaries exploit social media relationships to infer a user's affiliations or areas of interest. Behavioral inference is a different technique where hostile actors examine online behavior, including posting habits and content exchanges, to get information about a user's interests or personal life. Another issue is location inference, in which hackers infer a user's location from check-ins, geotagged posts, or patterns of online behavior. These methods draw attention to users' susceptibility to the disclosure of private information through seemingly innocuous data points.

Information Leakage: Information leakage in Online Social Networks (OSNs) is a major issue because of several factors. Users often inadvertently expose critical information because of inadequate privacy settings or default configurations, which emphasizes the need for user awareness and attention while adjusting privacy preferences. Integrating third-party applications with OSN accounts presents an additional risk as these apps may have varying data security standards that might disclose user information without consent.

Cyberstalking: Cyberstalking in Online Social Networks (OSNs) is a disturbing and unjustified online activity that is marked by continuous surveillance, threats, and harassment. Cyberstalkers use OSNs' capabilities to monitor their targets' online posts, conversations, and activities in great detail, giving the impression that people are always watching. Harassment is a typical method that causes mental pain and instills fear in the victim. It can take many different forms, from unwelcome messages to threats. Another tactic to control or mislead the target is to impersonate them or create false profiles.

Surveillance: Social media surveillance is a relatively new phenomena, in contrast to people's sociability and social roles in the political, economic, and civil arenas. Using their connections and profiles becomes a method of monitoring the diverse actions of their users in different social contexts. The term "social media surveillance" refers to technologybased monitoring that monitors users' online behavior. Ten percent of them got unseen users sending them explicit messages, and thirty-three percent of them experienced cyberbullying.

1.10 IDENTIFIED MODULES FOR OSN SECURITY

The term "identified modules" typically refers to specific components, sections, or units within a larger system, software application, or project that have been identified and designated for distinct purposes or functions. Identifying modules is a common practice in software engineering and system design to break down complex systems into manageable and organized parts [13]. These are described as follows:

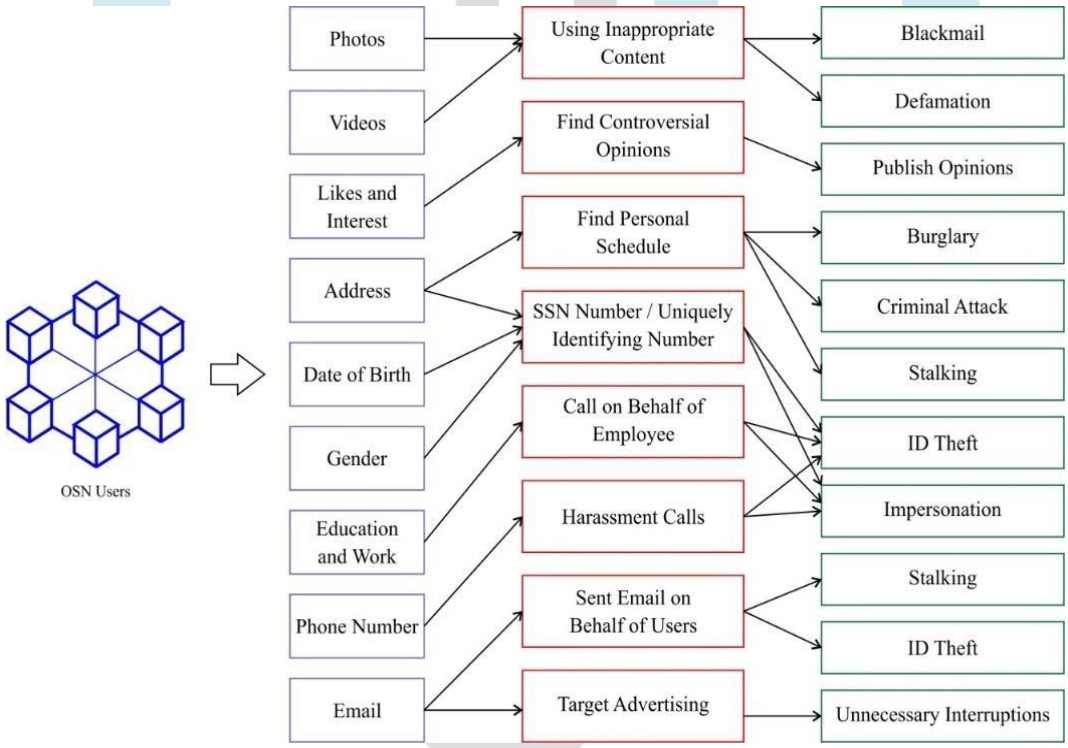

Figure 1.2 Information on OSN Users

The OSN User Information is displayed in Figure 1.2. Users' profile pictures and videos might be altered and used to defame and blackmail people. A person's likes and hobbies might disclose their beliefs and reveal a lot about them. An address can be used to locate someone, which might lead to a burglary or other criminal action. The combination of a person's address, date of birth, and gender may be used to establish their social security number (SSN), which can lead to identity theft or impersonation.

Businesses may utilize phone numbers and emails for targeted advertising, which results in spam and needless disruptions. As a result, ensuring accurate data and safeguarding sensitive and private information from unauthorized parties provide an open issue. The benefits and drawbacks of certain well-known social networks' characteristics are displayed in Table 2.2.

Table 1.2 Benefits and problems of Some Social Networks

Sr. No.	OSN	Benefits	Problems
1	Facebook	• The feature for setting groups • Business and Marketing • Entertainment	• Privacy Concerns • Addiction and Time Sink • Misinformation and Fake News
2	Twitter	• Real-time news and updates • Uncensored opinions and diverse perspectives • Connection and Community	• Misinformation and echo chambers • Toxicity and hate speech • Information overload and time sink
3	LinkedIn	• Professional Branding • Business development and networking • Learning and Knowledge	• Data Privacy Concerns • Time Commitment • Spam and Irrelevant Content
4	Google+	• Information Access • Innovation and Exploring • Accessibility and democratization do knowledge	• Privacy Concerns • Misinformation and fake news • Monopolization and Market Dominance
5	Snapchat	• Privacy Focused • In-the-moment connection • Limited Permanence	• Cyberbullying and Negativity • Misinformation and Privacy Concerns • Addiction Potential
6	Instagram	• Visual expression and creativity • Community and Connection • Personal Branding and Self-Expression	• Comparison and insecurity • Misinformation and fake news • Cyberbullying and Negativity
7	Pinterest	• Learning and skill development • Community and Connection • Cost-effective marketing and advertising	• Time sink and potential for addiction • Comparison and unrealistic expectations

Prominent development and research have taken place for security of OSNs; however various vulnerabilities are observed in case of user's identity and data, which shall keep OSNs on risk [14]. There are many different attacks on user's identity and data confidentiality therefore there is need to study mechanisms implemented for data confidentiality. After analysis of literature work and gap analysis, a novel mechanism for protecting user's identity and data confidentiality can be proposed.

Ralph and Alessandro [15] have analyzed pattern information revelation and highlighted potential attacks on privacy based on usage of privacy settings. The research shows that t very less percentage of users use the privacy preferences to prevent privacy attacks. Sean and Gautam proposed [16] graph-based greedy mechanism for attribute disclosure attacks, the user's sensitive information gets disclosed to adversary in attribute disclosure attacks. Researcher addressed the attacks on the data confidentiality however user identity attacks are unaddressed.

A proxy-based information protection mechanism is presented by Dwenet. al [17]. In this different commercial protection software and online security scanning services are integrated as security mechanism for OSNs. The proxy keeps user side protected from websites that can attack on user's information by blacklisting such websites. A cryptobased framework for securing OSNs is presented by Hoang et. al. [18]. In this research information confidentiality is maintain by digital signature. User sign digitally and encrypt the information at the client side before sharing it on the server, hence it protects the

data and maintains the data integrity. The promising work is done in the literature for user identity and data preservation based on anonymity algorithms [19-27] however these algorithms are based on structural and content attributes.

The symmetric encryption and hash function-based approach for user's content confidentiality is proposed by Charles et. al [28]. In this limitation of secrete key length is overcome by using the hash chain XOR algorithm and this makes algorithm suitable for various applications.

The virtual identity-based privacy preserving mechanism is presented by Elizabeth et. al [29]. In this, virtual identities are used to hide user's real identity. Every user has different virtual identities. For specific service usage, unique virtual identity will be selected as identity of the user. In the literature different mechanisms are discussed to protect user's identity i.e. token- based [30], crypto-based [31] and using blockchain [32]. However, protection of user's profile attributes and data confidentiality is still issue that to be addressed.

2.12 CONCLUDING REMARKS

It concludes with a thorough examination of the security and privacy practices of Facebook, Twitter, Instagram, and Snapchat. Through the exploration of various scholarly articles, papers, and studies, several key themes and findings have emerged.

Firstly, it is evident that data confidentiality is a critical concern in the realm of online social networks, given the vast amount of personal information shared and stored on these platforms. Researchers have highlighted the potential risks and vulnerabilities associated with the misuse or unauthorized access to user data, ranging from identity theft to privacy breaches.

Secondly, the literature has showcased a range of approaches and techniques employed to enhance data confidentiality on online social networks. These include encryption methods, access control mechanisms, anonymization techniques, and privacy-preserving algorithms. Each of these strategies aims to mitigate the risks associated with data exposure and unauthorized access while preserving the usability and functionality of the platforms. Furthermore, the literature has also emphasized the importance of user awareness and education in fostering a culture of privacy and data protection. Studies have shown that users often lack awareness of the implications of their online activities and may inadvertently compromise their own confidentiality. Therefore, there is a need for educational initiatives and user-friendly privacy controls to empower individuals to make informed decisions about their data sharing practices.

Overall, the literature survey has highlighted the multifaceted nature of the challenge of data confidentiality and profile visibility control in online social networks and the diverse range of strategies and solutions available to address it. In conclusion, ensuring data confidentiality in OSNs remains a complex issue. By addressing the research gaps identified in this survey, one can move towards a future where social media platforms are more respectful of user privacy and empower individuals to manage their online identities effectively.

References:

[01] Garton, Laura, Caroline Haythornthwaite, and Barry Wellman. "Studying online social networks." Journal of computer-mediated communication 3, no. 1 (1997):JCMC313.
[02] Chen, Wei, Carlos Castillo, and Laks VS Lakshmanan. Information and influence propagation in social networks. Springer Nature, 2022.
[03Stawarz, Katarzyna, Chris Preist, and David Coyle. "Use of smartphone apps, social media, and web-based resources to support mental health and well-being: onlinesurvey." JMIR mental health 6, no. 7 (2019): e12546.
[04] Camacho, David, Angel Panizo-LLedot, Gema Bello-Orgaz, Antonio GonzalezPardo, and Erik Cambria. "The four dimensions of social network analysis: An overview of research methods, applications, and software tools." Information Fusion 63 (2020): 88-120.
[05] Richthammer, Christian, Michael Netter, Moritz Riesner, Johannes Sänger, and GüntherPernul. "Taxonomy of social network data types." EURASIP Journal on Information Security 2014 (2014): 1-17.
[06] Chowdhury, Shihabur Rahman, Arup Raton Roy, Maheen Shaikh, and KhuzaimaDaudjee. "A taxonomy of decentralized online social networks." Peer-to-Peer Networking and Applications 8 (2015): 367-383
[41] Jain, A.K., Sahoo, S.R. &Kaubiyal, J. Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177 (2021). https://doi.org/10.1007/s40747-021-00409-7
[07] Hossain, Al Amin, and Weining Zhang. "Privacy and security concern of online social networks from user perspective." In 2015 International Conference on Information Systems Security and Privacy (ICISSP), pp. 246-253. IEEE, 2015.
[08] Ali, Shaukat, Naveed Islam, Azhar Rauf, IkramUd Din, Mohsen Guizani, and Joel JPC Rodrigues. "Privacy and security issues in online social networks." Future Internet 10, no. 12 (2018): 114.
[09] Netter, Michel, Moritz Riesner, Michael Weber, and GüntherPernul. "Privacy settings in online social networks--Preferences, perception, and reality." In 2013 46th
Hawaii International Conference on System Sciences, pp. 3219-3228. IEEE, 2013.
[10] Bhanot, Rajdeep, and Rahul Hans. "A review and comparative analysis of various encryption algorithms." International Journal of Security and Its Applications 9, no.4 (2015): 289-306.
[11] Pham, ThiHuyen, Thuy-Anh Phan, Phuong-Anh Trinh, Xuan Bach Mai, and QuynhChi Le. "Information security risks and sharing behavior on OSN: the impact of datacollection awareness." Journal of Information, Communication and Ethics in Society 22, no. 1 (2024): 82-102.
[12] Fire, Michael, Roy Goldschmidt, and Yuval Elovici. "Online social networks: threats and solutions." IEEE Communications Surveys & Tutorials 16, no. 4 (2014): 2019- 2036. [13] Benkaouz, Yahya, and Mohammed Erradi. "Towards a Decentralized OSN for a Privacy-preserving e-health System." Procedia Computer Science 63 (2015): 284- 291
[14] Hameed, Khizar, and Nafeesa Rahman. "Today's social network sites: An analysis of emerging security risks and their counter measures." In Communication Technologies (ComTech), 2017 International Conference on, pp. 143-148. IEEE, 2017.
[15] Gross Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71-80. ACM, 2005.
[16] Chester, Sean, and Gautam Srivastava. "Social network privacy for attribute disclosure attacks." In Advances in social networks analysis and mining (asonam). 2011 international conference on, pp. 445-449. IEEE, 2011.
[17] Tsai, Dwen-Ren, Allen Y. Chang, Sheng-Chich Chung, and You Sheng Li. "A proxybased real-time protection mechanism for social networking sites." In Security Technology (ICCST), 2010 IEEE International Carnahan Conference on, pp. 30-34.
IEEE, 2010.
[18] Do, Hoang Giang, Wee Keong Ng, and Zhendong Ma. "Privacy-Preserving Social Network for an Untrusted Server." In 2013 International Conference on Cloud and Green Computing. pp. 472-478. IEEE, 2013.

[19] K. Liu and E. Terzi, "Towards identity anonymization on graphs, "presented at the Proceedings of the 2008 ACM SIGMODinternational conference on Management of data, Vancouver, Canada, 2008.
[20] B. Zhou and J. Pei, "Preserving privacy in social networks against neighbourhood attacks, 2008, pp. 506-515.
[21] J. Cheng, et al., "K-isomorphism: privacy preserving network publication against structural attacks," presented at the Proceedings of the 2010 international conference on Management of data, Indianapolis, Indiana, USA, 2010.
[22] B. Zhou and J. Pei, "The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks," Knowledge and Information Systems, pp. 1-31, 2010.
[23] W. Wu, et al., "k-symmetry model for identity anonymization in social networks," presented at the Proceedings of the 13th International Conference on Extending Database Technology, Lausanne, Switzerland, 2010.
[24] L. Zou, et al., "K-automorphism: A general framework for privacy preserving network publication," Proceedings of the VLDB Endowment, vol. 2, pp. 946-957,2009.
[25] E. Zheleva and L. Getoor, "Preserving the privacy of sensitive relationships in graph data," presented at the Proceedings of the 1st ACM SIGKDD international conference on Privacy, security, and trust in KDD, San Jose, CA, USA, 2008.
[26] A. Campan and T. Truta, "A Clustering Approach for Data and Structural Anonymity in Social Networks," in In Privacy, Security, and Trust in KDD Workshop, 2008.
[27] Hay, et al., "Resisting structural re-identification in anonymized social networks," Proceedings of the VLDBEndowment, vol. 1, pp. 102-114, 2008.
[28] Clarke, Charles, EckhardPfluegel, and Dimitris Tsaptsinos. "Enhanced Virtual Private Social Networks: Implementing User Content Confidentiality." In Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, pp. 306-312. IEEE, 2013.
[29] Papadopoulou, Elizabeth, Sarah McBurney, Nick Taylor, M. Howard Williams, KajetanDolinar, and Martin Neubauer. "Using User Preferences to Enhance Privacy in Pervasive Systems." In Third International Conference on Systems (icons 2008), pp. 271-276. IEEE, 2008.
[30] Suguna, M., R. Anusia, S. Mercy Shalinie, and S. Deepti. "Secure identity management in mobile cloud computing." In Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017 International Conference on, pp. 42-45. IEEE, 2017.
[31] SdsAsghar, Muhammad Rizwan, Michael Backes, and MilivojSimeonovski. "PRIMA: Privacy-Preserving Identity and Access Management at Internet-Scale." In 2018 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE,
2018.
[32] Dunphy, Paul, and Fabien AP Petitcolas. "A first look at identity management schemes on the blockchain." arXiv preprint arXiv:1801.03294 (2018).