Privacy Concerns in Online Social Networks: A Users' Perspective

Ahmad Ali[1], Ahmad Kamran Malik[2],
Mansoor Ahmed[3], Basit Raza[4]
Department of Computer Science
COMSATS University Islamabad, Pakistan

Muhammad Ilyas[5]
Department of Computer Science & IT
University of Sargodha
Sargodha, Pakistan

***Abstract*—Social networking has elevated the human life to the heights of interaction, response and content sharing. It has been offering state of the art facilities to its users for a long time. Though, over the period of time, the systems have become quite matured yet alongside the benefits, multiple concerns of the user with regard to the privacy and information security also exist. Multidimensional threat spectrum to the Internet has also been posed to social networking tools. A lot of work is being done to understand privacy concerns in social networks. In this scenario, a survey of privacy concerns in online social networks is conducted. Risks, privacy issues, and threats have been highlighted that occurred in recent years, analyzing the targets of attackers, their methods of attack and measures taken to counter/manage these threats are the focus. A social network depends on the user, social network site/application and communication medium provider i.e. the Internet facility. Existing research contains domain specific research work regarding privacy issues in social networks; however, a comprehensive research work related to overall infrastructure of online social networks is missing. Development of a taxonomy of threats and categorization of frauds relevant to social networks is an important contribution of this survey. After completing a comprehensive research survey on privacy concerns in online social networks, a set of privacy guidelines is provided and open research challenges are highlighted.**

Keywords*—*Online social networks; information security; privacy; social networking; attribute disclosure

I. Introduction

Researchers related to different research areas have analyzed the on-line social network (OSN) in different ways. User privacy problem has been considered as one of surveillance, institutional privacy, social or an individuals' privacy issue. Researchers made their understanding independently, however, OSN privacy research would benefit from a more holistic approach. Privacy and an individual's social network are viewed in a multifaceted relation. For example, at sometime we do not want to publish our information on the web, however, we want it to be accessible to a small number of close friends, and not to outsiders or unknown. At some other occasions, we are eager to share information with the public, but not to our friends. Social network analysis techniques describe the impact of different depth and strength of ties in an individual's social network and the importance of these ties in the flow of information across the network. Social engineering is a well-known practice in the information security domain in which confidential information is retrieved by manipulating legitimate users. This practice may be implemented on an online social network, like Facebook, very simply by sending friend request. Shockingly, it has high success rate, the friend request was accepted by 75,000 out of 250,000 unknown users, when sent using a programmed script on Facebook [1]. Teenagers as compared to professionals are very much influenced by social networking sites. Sometimes they represent some sort of addiction to social networking. They behave carelessly and share private data without realizing its effects on privacy [2]. Users conversations, like/dislike some time may help in deducing some results related to personal data. Studies have also been conducted to compare the behavior and response methods of male and female [3]. Majority of Facebook users are eager to publicize themselves [4] and their profile information is available to a stranger and their network of friends. Is there any proper way to make decision positively for joining an OSN [5]. The Internet and social media content sharing made tremendous developments, however, at the cast of one's privacy. Manufacturers of smart devices like LCD/LED TVs categorically warned users not to share anything private before their smart devices [6]. User awareness about handling Smart Devices, especially privacy sensitivity instead of information security measures [7], is actually core need of the time. Samsung Smart TV is one of the Smart devices whose privacy policy statement declares clearly about voice recording and transmitting it to a third party [8]. Mainly a user or group of users, Internet service providers, Communication medium and the Social Networking Application makes a Social Networking infrastructure. Details related to OSN such as its definition, methods, facilities, history, rise and fall of different OSNs are covered in [9]. Details about Social Networks and Network Structures are also explored. Different types of frauds, hacking / cracking activities, spyware, malware, and malvertising etc. have been in practice for capturing private data of user/(s) [10], [11], [12]. With the advent of new approaches in Web technologies, from Web 1.0 to Web 4.0, the Internet of Things, connectivity of heterogeneous devices and sharing of data among them may cause new dimensions of Privacy Risks along with Safety and Security aspects[13], [12]. Social Networking is actually a need of time, where its usage again needs a responsible behavior. It is the user, who is solely responsible for her data/privacy, a user himself has to take strong measures for the protection of privacy [14]. Data analysts have worked for data collection, categorization and establishing links among different users as well as a group of users, based on not only user profiles but also comments, uploads and like or dislike measures. This study categorically highlights concerns and important measures for users privacy [15], [16]. This survey is divided into different sections starting from privacy understandings till providing some practical guidelines to be taken care while remaining on online social networks. Section II covers common concepts of OSN and its privacy, interaction vs surveillance, and parameters for user privacy. In Section III the need of limiting social network activities for privacy preservation is highlighted. Section IV provides taxonomy of OSN threats and its details in which threats and vulnerabilities in OSN are categorized in different classes and furthermore discussed in an information sharing approach. In Section V, a comprehensive discussion on issues after compromised privacy is carried out. Disaster after a compromised and how compromised privacy support in terrorism are also covered in Discussion part. Also privacy guidelines for secure OSNs are provided. Finally, Section VI concludes the paper.

II. Understanding OSNs

Pros and Cons of OSNs have been deliberated for a long time. Cyber Connectivity and Cyber Security, User Privacy and Anonymity, Cyber Bullying and Cyber Threats, Surveillance and Connectivity, Cyber terrorism and Cyber Warfare, are the areas of extraordinary interest in these days. Multidimensional attention has been given in terms of Information Sharing and User privacy in Online Social Networks. Research on OSNs can be expressed and categorized in the following subcategories.

- Need for OSNs
- OSNs Models
- Information Extraction on OSNs.
- Privacy Leaks and Privacy Measures in OSNs
- Anonymous behavior of users
- User / Human Behaviors in OSNs
- Privacy Issues in OSNs
- Cyber Threats in OSNs
- Cyber Crime / Terrorism and Attacks using OSNs
- Miscellaneous trends and trend building approaches in different of OSNs

A lot of research work has been carried in this regards. A detailed literature review is carried out as under.

A. *Need for OSNs*

It is related to the use of Social media and how people are dependent on Social media. We can not avoid Social media but can use reasonably. The importance, utility, and dependency of social media is explained in [17].

B. *OSNs Models*

OSN models for information security and their usefulness comparison is described here. The concept of Total Utility, Social Welfare along with cost functions are introduced in information sharing and privacy in social networks [18]. Multiple social networking applications are very much in practice in different communities. Multiple social networking sites and applications are having heterogeneous architectures and functionalities. A need for a generalized architecture for different social networking sites / apps is suggested [10], [19]. A comparison of different defense systems and models is provided and an approach is proposed for identity theft attacks in social network sites. Because of the insecure Internet [20], users are always vulnerable to the misuse of identity and problems of remote authentication. A secure authentication and validation of authentication are crucial for remote transactions [21], [22], [23]. A social network model None of Your Business (NOYB) [24] is used to implement improved privacy settings which helps users to implement more security settings. Privacy-preserving techniques in different OSNs and their comparison is carried out in [25]. Authors introduced a new concept of end-to-end encryption, hidden social graphs and discarding incompatible devices in [26]. Privacy preservation in decentralized online social networks has been highlighted in [27]. In [28], a machine-learning based approach is presented for privacy-aware information-sharing in mobile social networks. Authors presented and evaluated a privacy-preserving information sharing system (SPISM) in an automated fashion to share different types of contextual information and for specific levels of detail. It is a system that may be used to further automate other systems in instant messaging like applications. Authors explored privacy issues in online social networks and proposed a k-degree anonymity to secure information on social networks using Data Collection, Reduce Node Degree, add Node Degree and add Noise Node. The study [29], critically highlighted the privacy leakage in data sharing using social networking sites. It describes that sharing photos and tagging a photo increases the chances of data leakage exponentially. A new technique i.e. rule-based photo sharing for securing data for social networking sites is suggested. Separating privacy settings for photos and profiles by introducing independent privacy settings for each attribute is covered in [30]. Another dimension of symmetry about the architecture of social networks is highlighted in [31]. An approach using architectural symmetry and functional harmony can eliminate diverse nature of social networks. Privacy risks in OSNs are introduced because of un-symmetric configurations across the OSNs. For highlighting the issue of privacy leakage, an inference attack for leakage of data privacy is introduced. A new approach known as PbD (Privacy by Design) principles is introduced for OSNs in distributed computing environments [32], instead of any framework or technique, it pointed out the lack of proper PIA (Privacy Impact Assessment) [33]. Authentication and access control always remained the core area of research in every computing system development [34], [35]. Involvement of the third party for certification of OSN applications is suggested in [36], [37]. The openness of OSN users and application capability for information classification is to be taken care of. There are multiple classes of adversaries for example inside attackers and external attackers or intruders, who use user social space and social interaction to get into user's information. Two types of OSN architectures i.e. Client-Server architecture and P2P architecture are in practice. The important aspect of user identity anonymity, user personal space privacy and user communication privacy are the top priority[38]. Protecting online social graphs, defense against Social Link Forging Attacks and defense against Node Identity Forging Attacks are suggested in [5] . Another data security approach for OSN content sharing especially photo sharing is described in [22]. It provides a concept of policy-based photo sharing along with its demonstration.

C. Information Extraction on OSNs

The general attitude of OSN actors looks very strange sometimes [39]. There should be a clear understanding to handle a friendship request. A scripting technique was used to send automated requests for friendship to Facebook users. Out of 250,000 requests, author was successful in making 75,000 friends [1]. Tools exist for mining information from structured data[40], but in OSN data is not fully structured or unstructured. The authors exlore Semantic Web techniques for the collection of useful cyber security-related information from Social Networks. Analysis and storage of triples of RDF/OWL have been explored. OSNs are very much in practice in smartphones [41]. Mobile social networks (MSN) are providing real-time connectivity and content sharing. These MSNs provides datasets, and tools/techniques are available to find communities and groups in Mobile Social Networks [42] and other Online social networks [43]. A study carried out to analyze Facebook data using Netvizz application [44], [45]. The NetVizz application is covered in detail and the use of this application for data extraction and further use in different analyzing tools i.e. empirical analysis is discussed. Importance and utility of User Data Graphs and Social Nets are also highlighted. Extraction of Cyber security data from Linked Open Data (LOD) is also very much in practice. Semantics-based data extraction using RDF is suggested and an architecture is defined in [41]. Similarly, botnets are being used for data extraction from social networks [46], [47]. Neighborhood attack is another important concern of user privacy[48].

D. Privacy Leaks and Privacy Measures in OSNs

Data leakage of social network users is also a great threat. It is covered in [49], [50], [51], [52], [53]. These papers provide different methods for collecting identities, cloning and their use for criminal acts. Identity theft attack causes leakage of user privacy. Email ID is the only unique identifier which can cause disclosure of other information also. Three approaches for defending against Identity Theft attack are covered in [20]. Location disclosure is one of the most important privacy issues. Smart Phones provide state of the art Internet connectivity along with location information based on GPS and Internet-based location information. These Smart phones also provide updated social network applications with real-time connectivity and information sharing. Mobil share architecture is introduced to address location sharing problems in mOSNs [54], [55]. Improvements are suggested in location information gathering. Authors suggested that trusted and untrusted information providers should be classified and proposed the use of k-anonymity technique for information disclosure. Users depend on OSNs for interaction among their groups [36], [56], [57]. Basic four things that invite spammers are (i) controlling entity of the entire OSN (ii) well-defined interactions (iii) user Identity (iv) multiple interfaces of OSN providing different views [44]. Spams are spread on OSNs for collecting user activities and data, and a cause for privacy leakage [58]. Conventional coping and technological coping are suggested to protect against Identity Theft in [59]. A comparative study for consideration of conventional coping and technological coping is also provided.

E. Anonymous Behavior of Users

Users of Facebook and other SN applications, stay un-friended on the Internet. Positive, as well as negative concepts exists while remaining un-friended. Users may un-friend a few to reduce their friend's list [60], [61]. Staying hidden vs staying un-friended [62] is again another important research direction in social sciences. OSN users have different intentions to stay hidden or stay un-friended. A user staying hidden may be more dangerous than staying un-friended because of users shared content space, and in some cases, it may be otherwise. An exploratory study [63], [61] is carried out to determine users' emotional and cognitive response for un-friending someone on OSN. This is very much clear and an eye-opener for privacy researchers, where an individual's privacy is at great stake [60], [64].

F. User / Human Behaviors in OSNs

Human behavior and the way how a user responds to OSNs activities depends on specific class. Here, these classes are Age and Gender-based.

1) Age Factor: Social network users belong to different age brackets. But the majority of users belong to teenagers. In [24], authors made a mathematical analysis of teens activities and their concerns about privacy while remaining online. How their parents and guardians affect teens awareness about privacy? Since young adults are very much active on OSNs, therefore, neuroticism, extraversion, and online self-presentation among young adults occur. Comprehensive research has been carried out to analyze and understand these situations in [65].

2) Gender Factor: An interesting study provided in [3], authors explored dissimilarities in the behavior of men and women to handle the threats on social media. The main focus was the how and up-to what extent man and woman retaliate to threats, dislikes, rejections, etc. How users decide to join a Social Network? In [5], Data Mining, Group Analysis, Sensitive Attribute Inference development approaches for OSN are explored and a new Link Data Analysis approach is suggested.

G. Privacy Issues in OSNs

User authentication is the basic need for user data security. To handle identity theft and cyber-crime, [66] describes suitable authentication systems and parameters for a good authentication system. Use of biometric devices is also suggested. However, the issues of Biometric device utility and availability must be taken care. These biometric and other wearable sensors may not be available everywhere. Basic components of user authentication are User Identity and Password Credentials. Protecting login credentials is the responsibility of a user. But what are the measures to protect user identities? In [59], the coping perspective, threats related to user identities are covered. How to avoid misuse of user identity [67], parameters and methods required for safe use of identity in terms of financial loss, criminal activity, colluding attacks and identity cloning are described [68]. An analysis is carried for security challenges and vulnerabilities in software architectures of social networks. Mostly script based / programming attacks are emphasized in [69]. Smart Phones are now fully powered to connect OSNs. Privacy threats categorically related to mobile social networks are covered in [69]. Threats and vulnerabilities in mobile social network applications and gadgets already installed in mobile devices may cause more privacy issues. Various security and privacy challenges in mobile social networks are discussed in [70]. A gesture assisted authentication proposed three research areas covering Gesture assisted secure information sharing, effective resistance to Sybil attacks (especially mobile based) and private information management based on the social context. An article about privacy in the use of Smart TV [6] uncovered a story about spying approaches and practices used in different models of smart TVs. Samsung Privacy Policy [8] - Samsung rejects the allegations of spying but accepts about data collection for voice commands and their proper recognition. This feature can be disabled also. Humanly, it is very difficult to confirm or authenticates legitimate social media account, a lot of research is required in this domain [71], [72].

H. Cyber Threats in OSNs

Cyber space is too vulnerable for its users as claimed in [73]. Threats arose in social networking sites are categorized based on their portfolios and solutions are also suggested [11]. Different aspects of threats in cyberspace in terms of software, hardware, and network and also outstretched [13]. Smart devices are the basic entities for smart cities. Smart devices are connected to each other using the Internet as a communication infrastructure. Different threats like leakage of user privacy parameters in smart devices and a need for meaningful debate for cyber-security challenges in smart cities is also highlighted. In cyber threats in social networking websites [14], user gathering comparison on different social networks is carried out along with user behavior & awareness level that affects controlling of user privacy. Highlighted security threats raised with the advent of new technologies especially in social networking, and few suggestions are made for user privacy. User awareness and narcissism techniques introduced for detection of Insiders Threats, Outliers, Text, Context, video, and other uploads analysis provide very useful inferences and deductions. In [15], a detailed study is presented for the importance of the privacy factor in OSNs. A survey for privacy in SNs is carried out and calculated the privacy quotient of users by using the naive approach [16]. A privacy Armor model is proposed to ensure privacy in the unstructured data by generating an alert for leakage of the specific / private term. Interaction and contact vs surveillance are the two bright faces of SNs. In [16], it is highlighted that social connectivity and surveillance are two important aspects of Social Networking Sites. A detailed study is carried out for concepts and common understandings of privacy.

I. Cyber Crime / Terrorism and Attacks using OSN

With the development and advancement of OSNs, data collection, analysis, collection and coalition of information is not a very big deal. Cyber Terrorism, nowadays, depends on online available information. In [74], authors provide different aspects of threats and terrorism using the Internet, also differences between Cyber terrorists and hackers. Cyberspace opens for all types of Internet and unfortunately used by miscreants. A detailed study highlights all the aspects of threats and terrorism using Cyberspace. The motives, targets and methods of attackers, levels of attacks, and activities, influences, and paybacks in cyberspace are highlighted in [59]. Different types of social networks are highlighted and based on these types, dynamic aspects of national security and threats suspected to national security by using SNs are described in [58]. Authors critically pointed Government organizations to take part and make policies on use and misuse of OSNs to counter miscreants. Identity misuse and representation of multiple identities by a single user is really a danger. Vulnerabilities, exploits in data communication and networks, its effects for data leakage and countermeasures are given in [75], [76]. The Sybil attack openness and dynamic nature of SNs, are more vulnerable, and these vulnerabilities are exploited by different attackers. One of the attacks launched on social networks is the Sybil attack. Its behavior and scheme of operations and mathematical analysis have is provided. Use of Sybil seeds and edges of graph are explored in [77]. Privacy setting can be enforced to allow communication /interaction/sharing among friends only. However, there are threats in which mutual friend based attack is launched as highlighted in [78]. Attribute disclosure is one of the Social Network attacks. An approach for security within social networks against attribute disclosure attacks is suggested in [79]. For privacy patterns, a measure for an attribute disclosure attack is provided when one succeeds in getting particular nodes identity. A detailed list of reported cyber-crimes using social networks data are given in [80]

J. Miscellaneous Trends and Trend Building Approaches in Different OSNs

Semantic Web is emerging and helping people to cope with interoperability issues. In [81], authors highlighted the importance of Semantic Web for interoperability, and how the large collection of vocabularies developed for Semantic Web affect user privacy and interoperability. The user may belong to only a single Social Network or may have its presentation on few or all available social networks. An activity comparison of users on three SNs is carried out and privacy issues in terms of data analysis, network analysis, account association leakage, network connection leakage, etc are discussed in [82]. Furthermore, removal of identities from public search engines, disabling of reverse lookup functions, and provision to create users own attribute lists/groups is explained.

III. Understanding the Privacy

User Privacy is concerned with the information of a user that he or she is not willing to share with all others knowingly or unknowingly. Privacy can be defined in multiple dimensions. The easiest to understand definition found is the right of the individual to decide what information about himself should be communicated to others and under what circumstances [82]. Different perspectives of user privacy in OSN is explained in [83] with very comprehensive detail. Another important aspect of privacy and security is taking the assessment and monitoring user privacy and security in social networks [84]. Privacy may be explored in terms of the following.

A. The Surveillance Perspective

Revolutions because of web-based social media are much popular and are under discussion similar to Facebook and Twitter revolutions in politics and democracy. International moves for Internet Freedom and Right of Information also have greater impacts on OSN. Insecure Internet, identity theft, misuse of identity, mining identity-based information and exploration content space of a user generates surveillance concerns [63].

B. The Social Privacy Perspective

Analysis of an individual's shopping interests boosts economic revolutions and analysis of traveling and living information may strengthen the exploration of interests of society. However, along with all these benefits, individuals likes and dislikes, status and personal preferences may cause problems of social respect and security as well [49].

C. Parameters of Privacy

User ID, Password, DOB, Address, and Location, etc. are the basics of user privacy. Data mining and other network extraction, analysis, and drawing techniques help users to infer required information.

D. Limits for Sociality

A mechanism for suitable limits in Social Networking / Connectivity is missing. When a social network user posts something to his profile and then every one of his / her network can access the post, there is no way for a user to limit/hide posts for individuals. It is the established fact that people on OSN are not only social users. Directly or indirectly, knowingly or unknowingly, all are spying on each other [17]. The responsible social actor is the need of time. Some basic rules must be defined and practiced for social actors [85]. An expression generated on OSN for celebrating an event may cause a danger for the recipient. Similarly congratulating someone on any occasion may cause some serious family problems.

E. Privacy Issues in Social Networking

Sites for social networking like Facebook, Twitter & Google Plus have gained more popularity in recent years. Larger user-base and a large amount of information attracted the attackers and a potential channel is provided to be exploited. Most of the users try to prevent from such exploitations, however, attackers are more capable to overcome provided security measures by using diverse techniques. Users may not be aware of such threats or vulnerabilities that may include privacy issues, social networks spam, identity theft, malware, and physical threats. Very dangerous & deadliest attacks found in recent history are discussed in [86], [87].

IV. Taxonomy of OSN Threats

In this section, we propose the taxonomy of all possible threats shown in the Fig. 1. Four basic dimensions have been introduced to take care of threats to OSN as well as smart cities as explained in [13] and [14], similarly [59], [17], [20], [88], [89], [90]. Different types of threats have been found in the literature. These dimensions have further been divided into the following categories for clear understanding.

A. Infrastructure

OSN Infrastructure consists of a website/service hosted on a server, user application or website, central database and a communication channel i.e. Internet service [33], [26], [91]. Infrastructure threats can be further categorized into server-based threats, database threats and ISP/Internet-based threats. These threats are described as follows.

1) Server: Threats can damage servers partially or completely. Access Control, Viruses, Spam, Hacking, DOS, DDOS and Flooding (Unicor, etc.) are important dimensions. Location disclosure is also a great threat for OSN users. Weak access control allows unauthorized access to a server and can cause social privacy issues. Viruses can disrupt the infrastructure of a social network. The viruses can damage OSNs in several ways either by causing system failures or unwanted data leakage. These include Malware and Spyware etc. Spams are unsolicited messages that can disrupt the server and can cause data leakages. Hacking is a well-known server threat. An attacker who can get the server access can unfold all the data in OSN. DOS, DDOS, Flooding (Unicorn, etc) are functionality based attacks that eventually lead to denial of services along with data unavailability and leakage.

Users' location is a key privacy measure. Location of a user in social network discloses many things to a data analyst. This information causes severe threats for a user after disclosing the location.

2) Database: Database Theft and SQL Injection are very common threats to databases. Leakage/theft of data reveals complete social network data and cause misuse of the whole database. SQL Injection is a hacking technique to access the database without any legitimate authentication. A successful SQL Injection may cause leakage of the whole database.

3) Internet / Internet Service Providers: Insecure authentication, communication interception are known vulnerabilities in the usage of online application. Doxing, Evil Twin, Phishing & Pharming, Browser Sniffing, Network Sniffing, Baiting, Sybil attack, Hactivism, XSS and CSRF are some examples of such vulnerabilities. Companies providing Internet services to social network users have access to users' data traveling through their channels. Mechanisms exist to protect data during transportation. If data in communication is not encrypted, it is visible to everyone on the network. Doxing is the phenomenon in which an unknown person can publish victims information without his/her consent. No one of us is hereby ethically allowed others personal / privacy information on the Internet. Wireless network attacks exist in which a Wi-Fi access point can illegally represents itself as a legitimate one. Phishing refers to the attack in which an adversary attempts to reveal to the user's sensitive information by masquerading as a trustworthy entity. Pharming explains a cyber-attack intended to divert or redirect Internet traffic to another site.

Browser Sniffing is an act of detecting a browser of the victim whereas Network Sniffing / Packet Sniffing is a technique to analyze network packets for solving network problems. These techniques can be used for capturing user data. In a Sybil attack, an insecure hijacked computer claims multiple identities. Baiting are the threats which are carried out using the greedy attitude of the user. The user is tempted/seduced for some charm. Hacktivism is the subversive use of computers and computer networks to promote a political agenda. Cross-site scripting and cross-site [1] request forgery are such Internet-based attacks in which scripts are executed remotely on user/victims' machines.

B. Social Network Website / App

In this category, threats related to Social Network Website / App are covered. These threats mostly cover the issues related to the technical aspects of computer / Smartphone communication architecture [58]. Phishing, Vishing (Voice Phishing), Smishing, Application Vulnerabilities, Social Data Generation, Data Mining, SocioNet Graphs lie in this category. Similar to Phishing in infrastructure, at the website or application level, it leaks user data to others. In Vishing(Voice Phishing), audio calls using voice changers are used to get private info using Internet / social media application. Smishing is another type of Phishing, in which SMS services are used and users are fooled for financial or some other benefits. Like other computer software, most of the social network applications are vulnerable to exploitations. Social media applications for computers and/or Smart Phones also have some hidden vulnerabilities that are used for privacy leakage as described by Samsung Smart TV case [6], [8]. In Social Data Generation, users records of identities, usages, friends' lists, likes, and comments are centrally stored. These collections of social media items at a central place provide too much knowledge about users' personal information. By using some data extraction methods provided by every social application, Social data is generated for information extraction purposes.

Data Mining tools and techniques provide a wide range of pattern finding methods on social databases. SocioNet Graphs, another automatic method to draw social graphs to find links among network actors can reveal user privacy[92]. User privacy settings/measures, published contents can be extracted from social media accounts [93] which itself is the worst threat. Similar, Top-K strong pattern finding approaches are described in [94].

C. User(S)

This dimension of threats is related to the user, her behavior and usage of OSN [48]. It is very important for a user, "How an individual takes care of his/her data and is responding to the different situations". Identity Theft, Profile access control, Cyber Stalking / Cyber Bullying, Installed Applications, Surveillance Perspective, Social Privacy Perspective, Mutual-friend, Anonymity Risks, Script Generated Requests are common examples of threats which falls in this category. User identity is sole property to get legitimate access to his/her social space. Identity theft is the stealing of someone identity and to pretend as someone else. Profile Access Control is crucial whereas Web technologies provide seamless, open sharing of data on social networks using the concept of Open Web and Cloud Computing. Online harassment of users is known as Cyber Stalking or Cyber Bullying. This is only possible if mostly private data of victim is available to others. All the applications a user installs on Computer / Smart Phone are not confirmed for vulnerability proof. Applications may have vulnerabilities that may be exploited and used as Trojan horses. Every member in a social network cannot be guaranteed as a friend, he may be acting a surveillance actor [95]. For an individual, social activities of a user are shared on the social network, and to the people in a user's network. His likes and locations open users' privacy to the social network. Mutual-friend based or Friend of a friend scam is very much popular regarding social network privacy [78]. Attribute disclosure causes leakage of privacy information [79]. Location, Address, Educational Institutes, Friends, Likes, and Comments are some of the attributes that identify a user. Their disclosure also causes privacy issues in social networks and leads to threats/attacks. Anonymous data access and profile exploration cause data privacy leakage issues in social networks [96]. The script generated anonymous requests to join a network cause severe threat, and the majority of users accept requests without confirming the source.

D. Miscellaneous

Surveillance Perspective, Cyber Espionage/Cyber Spying, Information War, Cyber Terror, Cyber Crimes, and the social privacy - overall perspective is general cyber threats that affect user privacy [5], [73], [82].

Monitoring others and having eyes on others is made very much easy while using a social network and social surveillance. After establishing a social network, Cyber Espionage starts. Research explains that knowingly or unknowingly, every actor spies on the others. The social network is providing a comprehensive data bank for information warfare, which is available for use either positively or negatively. Cyber terror is based on the appearance of an adversary on the Internet, especially via the social network. The social network, not only affects a single one, but it may harm the whole network of an individual [74], [66]. Cyber Terror and other Cyber-crimes are examples of social network data usage. In larger perspective, social privacy also includes complete information of an area, explaining user's trends, market search, and the community likes and dislikes.

V. Discussion

Use and misuse, both exist simultaneously everywhere. Social Media is providing a platform for finding market flow, making users opinions, setting a trend and political move. With the development and advancement of data mining applications, data analysis, pattern finding, network link establishment, inference development and making an individual's family tree is not a difficult task. Most e-banking, telemarketing, credit card systems and telecommunication services need only a few parameters for user authentication. A person, with malicious-intentions, may follow the individual for some time on the social media, collect data, make references, and infer useful parameters and then finally launch an attack. Criminals need data to plan for their activities. The more data and analysis power they have, the probability of success in their activities increases exponentially. It is obvious, that social media is providing a huge data-bank for this purpose. Identity Theft, ATM Skimming, Spear Phishing are few examples in this regards. An overview of these frauds is given in Table I.

A. Disasters after a Compromised Privacy

The majority of Cyber Frauds are based on privacy leaks. Cyber Frauds are mostly initialized because of privacy leaks.

Well-known International Cyber Frauds list is being maintained by the FBI. These frauds can be categorized in different domains and at different levels.

1) Direct finance / Cash involvement: Financial benefits are the core objectives of criminals. They try their best for financial benefits and utilize different approaches. For example, (a) Advance Fee Schemes, in which the greedy victim gives some money and expects something of greater value in return in terms of financial benefits such as approval of the loan, service contract, business investment, or a gift whereas receives much little or even nothing in return. (b) Bankruptcy Fraud is a white-collar crime that commonly takes place where an individual intentionally submits false or incomplete forms. (c) Corporate Fraud can be defined as any fraud committed against a commercial activity. Fraud affecting that target commercial activity can be from general frauds to sector specific frauds. (d) Funeral Fraud or Prepaid Funeral Scams, where service regulations like prepaid funeral service vary from state to state and provide a chance for deceiving operators to overprice and list themselves as beneficiaries. (e) Insider Trading, the trading of financial commodities by insiders with material where non-public information pertaining to a significance is shared and hence often market-moving developments occur which benefit themselves or others financially. These developments can include undecided mergers and procurements, expected earnings releases, and product line progresses. (f) Market Manipulation Fraud generally referred to as a pump and dump which creates artificial demand pressure for a targeted commodity i.e. security or share in a stock exchange, in general, a low-trading volume issuer (over-the-counter) in the securities market mostly administered and controlled by the fraud committers. (g) Credit Card Fraud is a famous wide-ranging term for fraud and theft committed used by a payment card, such as a credit card or debit card, as a deceitful source of funds in a financial transaction. The reason may be to buy something or to get unlawful funds from an account. The unlawful use of a bank card, or matching number, to deceitfully obtain assets or money is also known as credit card fraud. (h) Financial Institution Frauds, another class of criminal schemes which targets traditional as well as modern retail banks, credit card unions, and other similar federally-insured financial institutions. Such type of schemes involve the compromised customers' accounts or personal identifying information; where stolen account identities belong to any of the financial institution or customers are considered victims. Mortgage fraud is a sub-category of such frauds. For example a lie, based on the social engineering or social information leakage, that influences a bank's decision about whether to approve or disapprove a loan, accept or reject a reduced payoff amount, or agree to a certain defined repayment terms. (i) Nigerian Letter Frauds comprise the threats of impersonation with a type of an advance fee scheme in which a letter is forwarded via courier or e-mailed, from Nigeria and offers the opportunity to the recipient to share some amount out of a heavy amount that the author i.e. a self-proclaimed official of their government, trying to transfer somewhere out of the country illegally. It is also known as Nigerian 419 fraud. (j) Investment and Business Frauds highlight the activities of stakeholders in a dishonest or an illegal manner designed to be beneficial for the establishment or the executing person and manage the escort by insiders. (k) Letter of Credit (L/C) Frauds is such types which are often attempted against financial institutions like banks by providing incorrect information in the documentation to prove that required goods have been shipped whereas in reality no goods or at least inferior goods were shipped. (l) Ransom-ware is a type of malware that infects computers, networks, and servers using encryption to make files unreadable. Afterwards, cyber attackers demand a ransom to return the files.

2) Online activities: Online activities where proper information and social network security is not accounted for, may cause severe disasters [97] (a) Identity theft is another type of authentication fraud occurs when someone assumes others' identity to perform a fraud or a criminal act. (b) Timeshare Scams where criminals hire marketing agents for their benefits and sometimes pays a little as a reward. (c) Another extremely sophisticated kind of malware is GameOver Zeus. This malware is engineered categorically to steal banking and other credentials from the computers. It is broadcasted through e-mails as well as phishing methods. (d) Work-at-Home Scams, just like Timeshare schemes, criminals initially try to gain the trust of job seekers/victims by offering very seductive plans varying from ad posting to email checking, etc.

3) Bank notes / Bonds: (a) Prime Bank Note Fraud. The need of such frauds is commonly to embolden the victim to transfer money to a bank outside his/her country where it is eventually received into an off-shore account in the control of the main artist. Furthermore, this money is used for the perpetrator's personal benefits/expenses or is laundered in an effort to make it disappear. (b) Redemption / Strawman / Bond Fraud. Criminals use such financial documents that appear to be legitimate but are not in reality. (c) Securities and Commodities Fraud is a wide range of illegal activities, all of which involve the deception of investors or the manipulation of financial markets. (d) Social Security Card Fraud is similar to identity theft frauds where criminals use Social Security Card information to launch any exploit. (e) Staged Auto Accident Fraud is fraudulently claiming much more re-reimbursement of a car accident expenses which never met or of low intensity / less expensive. (f) Stock Options Backdating is manipulating stock statistics with respect to the current market situation.

4) Market manipulation: Artificial Share Value Raising, Ponzi and Pyramid Schemes are used for market manipulation. Using telemarketing approaches some other approaches include: (a) Anti-Aging Product Fraud, (b) Foreclosure Fraud, (c) Health Care Fraud, (d) Internet Pharmacy Fraud, (e) Mass Marketing Fraud, (f) Online Auction Fraud, (g) Online Auto Auction Fraud, (h) Telemarketing Fraud.

5) Social engineering: Victimizing users using their social information falls in this category. A broadened list of Social Engineering Scams consists of the following approaches: (a) Scareware, (b) Grandparent Scam, (c) Lottery Scams, (d) Natural Disaster Fraud, (e) Online Dating Scams, (f) Reverse Mortgage Scams, (g) Senior Citizen Fraud, (h) Smishing, (i) Spear Phishing, (j) Sports Memorabilia Fraud, (k) Surrogacy Scam, (l) Swatting, (m) Telephone Denial of Service Fraud, (n) House Stealing, (o) Jury Duty Scam, (p) Online Rental Housing Scheme, (q) Adoption Scams.

6) Online social networks supporting cyber terrorism: The number of terrorist activities is getting higher in which the Internet is the battlefield [8]. In Cyber Terrorism, following few techniques used as war tools are of high impact [10]. Cyber Terror - A computer-based violence or destruction to target. Innocent victims for a Political or social change. Cyber Stalking People harassment using social media. Social media-based attempts are key elements in collecting information about victims and bullying them by using social data [98]. Cyber Bullying Children harassment using social media. Social media-based attempts are key elements in bullying anyone by using anonymous social IDs. Similarly, Ransomware is also the other dimension of cybersecurity issues [76].

B. Privacy Guidelines

After a comprehensive study of OSN threats, considering measures taken in social networking sites, and using lessons learnt from existing privacy attacks, this survey presents privacy guidelines that each user must consider.

The prime objective of OSNs is content sharing, however, before sharing something it is necessary to have a look at content and only public data should be published for the public. A large number of scams based on social engineering data has been reported and offer very enticing and seductive plans for attraction. It is again very important to verify the authenticity of offers offered on OSNs or Online application.

Surveillance and contact are two contradictory phenomena, users must remain vigilant for privacy parameters. Internet / Application service providers only have an interest in their business and financial benefits. Always keep in mind the reasons and effects of recent privacy leaks. Privacy risks has a very low impact on the service providers as compared to the user. Live with limited financial information shared on social media and never share Credit Card / Debit Card information on Social Media. Hackers need Social information for their financial benefits. In addition, de-activate stolen Financial Cards and get renewed ones immediately.

Leakage of sibling's information and other blood relatives may cause severe disaster so avoid disclosing such information. Blood relatives' information is manipulated by criminals for financial benefits. Posting of vacation and traveling plan on social media is not advised and visiting suspicious pages and links is strongly discouraged. Never respond to any request/offers until/unless the source is confirmed. After all, a user has sole responsibility for his/her data privacy so take care of data as well as privacy and remain alert and vigilant about strangers.

C. Open Research Problems

Here we provide the OSN privacy issues/threats that are still an open challenge for researchers.

- Malware - Malware is small software applications used to collect user information/data. Antivirus programs can detect malware using their signatures; however, in the case of Malvertising, a systematic solution is not available, user's attentive response is very much necessary.
- XSS: Cross Site Scripting vulnerability has been in practice for a long time by the attackers. Encryption was introduced to protect web data, however, in the case of Key Compromises and "Man in The Middle Attack" encryption becomes useless.
- SQL Injection: SQL injection is a technique [99] used to collect data in database connected application. This type of vulnerability can further be made multifarious using DOS, DDO, and DNS hijacking attacks. Encryption facilitates in protecting from SQL Injection, however, in case of encryption key compromise, no solution is yet available.
- Symmetric Key Compromises: Asymmetric key encryption mechanism (PKI infrastructure) has been introduced. Digital signatures are very much in practice to implement Information Security practices. In the case of Digital Signatures Theft or Public Key loss, renewal of these is suggested, however, during the period of compromise, no mechanism still found.
- Two Factors Authentication: Two-factor authentication is in practice in order to manage and maintain security and provides mechanism against Identity Loss. Risks increases if the second source of authentication is already compromised. Further measures are required to handle such types of vulnerabilities.
- Solutions Required for Multidimensional Threats: FoaF Scams, Interaction vs Surveillance, Independent Group of Friends, and Security Keys (Text Files) in the case of password loss are still very important, critical and useful dimensions for research.

D. Known Solutions and Problem Areas

Along with maturity in security parameters, some useful developments also appeared in social network applications. The antivirus industry has been quite a mature database to handle issues of viruses, malware, Spywares and Spams having already detected signatures. Different Malware and their detection approaches are described in [100].

Cross-site scripting and Cross-site request forgery attacks are web-based attacks. Careful and vigilant browsing help in the prevention of such attacks and encrypted data communication also provides a security layer. Another problem of key compromises in symmetric encryption keys has been solved using Asymmetric encryption keys (Public Key Infrastructure).

Users' social data remains public in most of the cases which cause identity theft. Multi-factor and multi-channel authentication was introduced to provide protection against identity theft [101].

E. Solutions Still Awaited

Though different solutions have been developed to provide security and privacy measures in social network applications, however, following grey areas and their solutions are still awaited. Advertising is very common in social networking applications which is being used for malicious intentions.

Malvertising is an approach in which hackers publish links in social network applications for different products where a victim gets compromised after clicking the given link. Two distinct keys, Private and Public, are used in Public Key Infrastructure. it becomes the worst scenario when a Private key is compromised and the victim is totally unaware of it unless some criminal activity is detected. Friend of a Friend Scams (FoaF Scams) and Independent Group of Friends are popular vulnerabilities in social networks.

How a user can detect surveillance and differentiate it form interaction. In the case of password loss, Security Keys (Text Files) have been introduced by different web application providers. what if security keys themselves got lost.

VI. Conclusions

In this paper, security and privacy issues related to social network and social engineering are discussed. Latest risks and vulnerabilities are highlighted. A taxonomy is developed by organizing threats into different categories. From a user point of view, few considerations like lessons learned are provided as privacy guidelines to take care of user privacy. Social Networking is open to all as it has been materialized long ago because it is Social. Users must respond responsibly and use social media only for public matters (reduce and control private information/data sharing).

Availability, customization, and enforcement of a set of well-defined privacy and security policies for social media are very crucial. Using a strong password, changing passwords frequently, information disclosure threats and measures, using antivirus, and certified software can secure social networks and limit the possibility of attacks and vulnerabilities. Anything once shared on social media is away from user control. As compared to the privacy risks affecting a user, no one else is at stake.

References

[1] K. Jump, "A new kind of fame," *The Columbian Missourian*, 2005.

[2] Y. Feng and W. Xie, "Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," *Computers in Human Behavior*, vol. 33, pp. 153–162, 2014.

[3] G. M. Chen and Z. Abedin, "Exploring differences in how men and women respond to threats to positive face on social media," *Computers in Human Behavior*, vol. 38, pp. 118–126, 2014.

[4] S. Zhang, R. C.-W. Kwok, P. B. Lowry, and Z. Liu, "Does more accessibility lead to more disclosure? exploring the influence of information accessibility on self-disclosure in online social networks," *Information Technology & People*, 2019.

[5] E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in *Proceedings of the 18th international conference on World wide web*. ACM, 2009, pp. 531–540.

[6] Online, "The daily beast(http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html)," 2015. [Online]. Available: http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html

[7] A. Bibi, Z. Hussain, F. Khan, and A. Maqsood, "Quantitative evaluation of security and privacy perceptions in online social networks: A case study," in *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*. IEEE, 2017, pp. 425–433.

[8] Online, "Samsung privacy policy (http://www.samsung.com/sg/info/privacy/smarttv.html?cid=afl-hq-mul-0813-11000170)," 2015. [Online]. Available: http://www.samsung.com/sg/info/privacy/smarttv.html?CID=AFL-hq-mul-0813-11000170

[9] D. Boyd and N. Ellison, "Social network sites: definition, history, and scholarship," *IEEE Engineering Management Review*, vol. 3, no. 38, pp. 16–31, 2010.

[10] L. J. Elliott and V. Polyakova, "Beyond facebook: The generalization of social networking site measures," *Computers in Human Behavior*, vol. 33, pp. 163–170, 2014.

[11] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: threats and solutions," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019–2036, 2014.

[12] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[13] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of advanced research*, vol. 5, no. 4, pp. 491–497, 2014.

[14] W. Gharibi and M. Shaabi, "Cyber threats in social networking websites," *arXiv preprint arXiv:1202.2420*, 2012.

[15] A. Srivastava and G. Geethakumari, "Measuring privacy leaks in online social networks," in *Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on*. IEEE, 2013, pp. 2095–2100.

[16] S. Gürses and C. Diaz, "Two tales of privacy in online social networks," *IEEE Security & Privacy*, vol. 11, no. 3, pp. 29–37, 2013.

[17] H. Zhang, M. De Choudhury, and J. Grudin, "Creepy but inevitable?: the evolution of social networking," in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, 2014, pp. 368–378.

[18] J. Kleinberg and K. Ligett, "Information-sharing and privacy in social networks," *arXiv preprint arXiv:1003.0469*, 2010.

[19] E. Muller and R. Peres, "The effect of social networks structure on innovation performance: A review and directions for research," *International Journal of Research in Marketing*, vol. 36, no. 1, pp. 3–19, 2019.

[20] B.-Z. He, C.-M. Chen, Y.-P. Su, and H.-M. Sun, "A defence scheme against identity theft attack based on multiple social networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2345–2352, 2014.

[21] E. Mik, "Mistaken identity, identity theft and problems of remote authentication in e-commerce," *Computer Law & Security Review*, vol. 28, no. 4, pp. 396–402, 2012.

[22] M. Ilyas, A. Ali, and J. Kueng, "Websea: A secure framework for multi-site knowledge representation in software engineering," in *International Conference on Bio-Inspired Models of Network, Information, and Computing Systems*. Springer, 2010, pp. 682–686.

[23] A. Ali, M. Ahmed, M. Ilyas, and J. Küng, "Mitis-an insider threats mitigation framework for information systems," in *International Conference on Future Data and Security Engineering*. Springer, 2017, pp. 407–415.

[24] S. Guha, K. Tang, and P. Francis, "Noyb: Privacy in online social networks," in *Proceedings of the first workshop on Online social networks*. ACM, 2008, pp. 49–54.

[25] M. Chewae, S. Hayikader, M. H. Hasan, and J. Ibrahim, "How much privacy we still have on social network?" *International Journal of Scientific and Research Publications*, vol. 5, no. 1, pp. 2250–315, 2015.

[26] L. Schwittmann, M. Wander, C. Boelmann, and T. Weis, "Privacy preservation in decentralized online social networks," *IEEE Internet Computing*, vol. 18, no. 2, pp. 16–23, 2014.

[27] X. Zheng, Z. Cai, G. Luo, L. Tian, and X. Bai, "Privacy-preserved community discovery in online social networks," *Future Generation Computer Systems*, vol. 93, pp. 1002–1009, 2019.

[28] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, M. Gazaki, and J.-P. Hubaux, "A machine-learning based approach to privacy-aware information-sharing in mobile social networks," *Pervasive and Mobile Computing*, vol. 25, pp. 125–142, 2016.

[29] M. A. S. I. Raj and M. N. Radhika, "Securing sensitive information in social network data anonymization," 2014.

[30] S. D. Bachpalle and M. Desai, "Data security approach for online social network," in *Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on*. IEEE, 2014, pp. 262–267.

[31] C. Tang, Y. Wang, H. Xiong, T. Yang, J. Hu, Q. Shen, and Z. Chen, "Need for symmetry: Addressing privacy risks in online social networks," in *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*. IEEE, 2011, pp. 534–541.

[32] T. Bauereiß, A. P. Gritti, A. Popescu, and F. Raimondi, "Cosmedis: a distributed social media platform with formally verified confidentiality guarantees," in *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 2017, pp. 729–748.

[33] M. B. Islam and R. Iannella, "Privacy by design: Does it matter for social networks?" in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 2011, pp. 207–220.

[34] C. Belbergui, N. Elkamoun, and R. Hilal, "Modeling access control policy of a social network," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, 2016.

[35] B. Chaimaa, E. Najib, and R. Hilal, "An access control model for a social network: Case of facebook," *International Journal of Computer Science and Information Security*, vol. 14, no. 11, p. 91, 2016.

[36] M. Shehab, A. Squicciarini, G.-J. Ahn, and I. Kokkinou, "Access control for online social networks third party applications," *computers & security*, vol. 31, no. 8, pp. 897–911, 2012.

[37] S. I. Tamrin, S. I. Tamrin, A. A. Norman, A. A. Norman, S. Hamid, and S. Hamid, "Information systems security practices in social software applications: a systematic literature review," *Aslib Journal of Information Management*, vol. 69, no. 2, pp. 131–157, 2017.

[38] K. J. Pegg, A. W. O'Donnell, G. Lala, and B. L. Barber, "The role of online social identity in the relationship between alcohol-related content on social networking sites and adolescent alcohol use," *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 1, pp. 50–55, 2018.

[39] B. C. Singh, B. Carminati, and E. Ferrari, "Learning privacy habits of pds owners," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 151–161.

[40] E. Bertino and E. Ferrari, "Big data security and privacy," in *A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years*. Springer, 2018, pp. 425–439.

[41] A. Joshi, R. Lal, T. Finin, and A. Joshi, "Extracting cybersecurity related linked data from text," in *Semantic Computing (ICSC), 2013 IEEE Seventh International Conference on*. IEEE, 2013, pp. 252–259.

[42] K. Xu and X. Zhang, "Mining community in mobile social network," *Procedia Engineering*, vol. 29, pp. 3080–3084, 2012.

[43] Z. Zhao, C. Li, X. Zhang, F. Chiclana, and E. H. Viedma, "An incremental method to detect communities in dynamic evolving social networks," *Knowledge-Based Systems*, vol. 163, pp. 404–415, 2019.

[44] B. Rieder, "Studying facebook via data extraction: the netvizz application," in *Proceedings of the 5th annual ACM web science conference*. ACM, 2013, pp. 346–355.

[45] K. Knautz and K. S. Baran, "Facets of facebook," 2016.

[46] J. Zhang, R. Zhang, Y. Zhang, and G. Yan, "The rise of social botnets: Attacks and countermeasures," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[47] K.-C. Yang, O. Varol, C. A. Davis, E. Ferrara, A. Flammini, and F. Menczer, "Arming the public with artificial intelligence to counter social bots," *Human Behavior and Emerging Technologies*, vol. 1, no. 1, pp. 48–61, 2019.

[48] A. K. Diwakar, N. K. Singh, and D. S. Tomar, "End user privacy preservation in social networks against neighborhood attack," in *Asia Security and Privacy (ISEASP), 2017 ISEA*. IEEE, 2017, pp. 1–9.

[49] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in *Proceedings of the 18th international conference on World wide web*. ACM, 2009, pp. 551–560.

[50] S. L. Buglass, J. F. Binder, L. R. Betts, and J. D. Underwood, "Looking for trouble: A multilevel analysis of disagreeable contacts in online social networks," *Computers in Human Behavior*, vol. 70, pp. 234–243, 2017.

[51] D. R. Cornelius, "Online identity theft victimization: An assessment of victims and non-victims level of cyber security knowledge," Ph.D. dissertation, Colorado Technical University, 2016.

[52] B. Hughes, B. DAVID, I. MOHAMMOD, M.-M. ELI, and S. JOSÉ, "Cyber benefits and risks: Quantitatively understanding and forecasting the balance," *Frederick S. Pardee Center for International Futures*, 2015.

[53] R. K. Minniti, "Identifying business risk factors of identity theft," Ph.D. dissertation, Walden University, 2016.

[54] R. Ajami, N. Al Qirim, and N. Ramadan, "Privacy issues in mobile social networks," *Procedia Computer Science*, vol. 10, pp. 672–679, 2012.

[55] A. Ometov, A. Levina, P. Borisenko, R. Mostovoy, A. Orsino, and S. Andreev, "Mobile social networking under side-channel attacks: Practical security challenges," *IEEE Access*, vol. 5, pp. 2591–2601, 2017.

[56] S. Sindhu and A. Bhuvaneswari, "A survey on multi-party privacy conflicts in online social networks," 2016.

[57] F. Sabatini and F. Sarracino, "Online social networks and trust," *Social Indicators Research*, vol. 142, no. 1, pp. 229–260, 2019.

[58] S. M. Abdulhamid, S. Ahmad, V. O. Waziri, and F. N. Jibril, "Privacy and national security issues in social networks: The challenges," *arXiv preprint arXiv:1402.3301*, 2014.

[59] F. Lai, D. Li, and C.-T. Hsieh, "Fighting identity theft: The coping perspective," *Decision Support Systems*, vol. 52, no. 2, pp. 353–363, 2012.

[60] J. L. Bevan, J. Pfyl, and B. Barclay, "Negative emotional and cognitive responses to being unfriended on facebook: An exploratory study," *Computers in Human Behavior*, vol. 28, no. 4, pp. 1458–1464, 2012.

[61] C. Sibona and S. Walczak, "Unfriending on facebook: Friend request and online/offline behavior analysis," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*. IEEE, 2011, pp. 1–10.

[62] J. L. Bevan, P.-C. Ang, and J. B. Fearns, "Being unfriended on facebook: An application of expectancy violation theory," *Computers in Human Behavior*, vol. 33, pp. 171–178, 2014.

[63] J. Peña and N. Brody, "Intentions to hide and unfriend facebook connections based on perceptions of sender attractiveness and status updates," *Computers in Human Behavior*, vol. 31, pp. 143–150, 2014.

[64] V. Katic, "Ranking external content on online social networks," Apr. 23 2019, uS Patent App. 10/268,763.

[65] M. Michikyan, K. Subrahmanyam, and J. Dennis, "Can you tell who i am? neuroticism, extraversion, and online self-presentation among young adults," *Computers in Human Behavior*, vol. 33, pp. 179–183, 2014.

[66] C. Edwards, "Ending identity theft and cyber crime," *Biometric Technology Today*, vol. 2014, no. 2, pp. 9–11, 2014.

[67] S. M. Furnell, "Online identity: Giving it all away?" *Information Security Technical Report*, vol. 15, no. 2, pp. 42–46, 2010.

[68] G. A. Kamhoua, N. Pissinou, S. Iyengar, J. Beltran, C. Kamhoua, B. L. Hernandez, L. Njilla, and A. P. Makki, "Preventing colluding identity clone attacks in online social networks," in *Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 187–192.

[69] R. Ajami, N. Ramadan, N. Mohamed, and J. Al-Jaroodi, "Security challenges and approaches in online social networks: A survey," *IJCSNS*, vol. 11, no. 8, p. 1, 2011.

[70] X. Liang, K. Zhang, X. Shen, and X. Lin, "Security and privacy in mobile social networks: challenges and solutions," *IEEE Wireless Communications*, vol. 21, no. 1, pp. 33–41, 2014.

[71] C. Sandy, P. Rusconi, and S. Li, "Can humans detect the authenticity of social media accounts?" 2017.

[72] N. Alomar, M. Alsaleh, and A. Alarifi, "Social authentication applications, attacks, defense strategies and future research directions: a systematic review," *IEEE Communications Surveys & Tutorials*, 2017.

[73] B. Vidyalakshmi, R. K. Wong, and C.-H. Chi, "Privacy scoring of social network users as a service," in *Services Computing (SCC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 218–225.

[74] I. Lachow, "Cyber terrorism: Menace or myth," *Cyberpower and national security*, pp. 434–467, 2009.

[75] J. R. Douceur, "The sybil attack," in *International Workshop on Peer-to-Peer Systems*. Springer, 2002, pp. 251–260.

[76] D. Koll, M. Schwarzmaier, J. Li, X.-Y. Li, and X. Fu, "Thank you for being a friend: An attacker view on online-social-network-based sybil defenses," in *Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 157–162.

[77] H. Zhang, C. Xu, and J. Zhang, "Exploiting trust and distrust information to combat sybil attack in online social networks," in *IFIP International Conference on Trust Management*. Springer, 2014, pp. 77–92.

[78] L. Jin, J. B. Joshi, and M. Anwar, "Mutual-friend based attacks in social network systems," *Computers & security*, vol. 37, pp. 15–30, 2013.

[79] S. Chester and G. Srivastava, "Social network privacy for attribute disclosure attacks," in *Advances in social networks analysis and mining (asonam), 2011 international conference on*. IEEE, 2011, pp. 445–449.

[80] Online, 2015. [Online]. Available: http://www.fbi.gov/scams-safety/frauds-from-a-to-z

[81] V. K. Kumar, "Semantic web approach towards interoperability and privacy issues in social networks," *arXiv preprint arXiv:1410.1995*, 2014.

[82] P. Wang, W. He, and J. Zhao, "A tale of three social networks: User activity comparisons across facebook, twitter, and foursquare," *IEEE Internet Computing*, vol. 18, no. 2, pp. 10–15, 2014.

[83] G. Weimann, "Cyberterrorism: The sum of all fears?" *Studies in Conflict & Terrorism*, vol. 28, no. 2, pp. 129–149, 2005.

[84] M. Sahinoglu, A. D. Akkaya, and D. Ang, "Can we assess and monitor privacy and security risk for social networks?" *Procedia-Social and Behavioral Sciences*, vol. 57, pp. 163–169, 2012.

[85] B. Kepez and P. Yolum, "Learning privacy rules cooperatively in online social networks," in *Proceedings of the 1st International Workshop on AI for Privacy and Security*. ACM, 2016, p. 3.

[86] C. Timm and R. Perez, *Seven deadliest social network attacks*. Syngress, 2010.

[87] S. Kumar, K. Saravanakumar, and K. Deepa, "On privacy and security in social media–a comprehensive study," *Procedia Computer Science*, vol. 78, pp. 114–119, 2016.

[88] K. J. Reza, M. Z. Islam, and V. Estivill-Castro, "3lp: Three layers of protection for individual privacy in facebook," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2017, pp. 108–123.

[89] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," *IEEE Network*, vol. 24, no. 4, 2010.

[90] P. Heymann, G. Koutrika, and H. Garcia-Molina, "Fighting spam on social web sites: A survey of approaches and future challenges," *IEEE Internet Computing*, vol. 11, no. 6, 2007.

[91] G. Misra, J. Such, and L. Gill, "A privacy assessment of social media aggregators," 2017.

[92] E. Angel, E. Bampis, A. Kononov, D. Paparas, E. Pountourakis, and V. Zissimopoulos, "Clustering on k-edge-colored graphs," *Discrete Applied Mathematics*, vol. 211, pp. 15–22, 2016.

[93] T. Khazaei, L. Xiao, R. E. Mercer, and A. Khan, "Detecting privacy preferences from online social footprints: a literature review," *IConference 2016 Proceedings*, 2016.

[94] B. Bakariya, K. Chaturvedi, K. P. Singh, and G. Thakur, "Efficient approach for mining top-k strong patterns in social network service," in *Eco-friendly Computing and Communication Systems (ICECCS), 2016 Fifth International Conference on*. IEEE, 2016, pp. 104–108.

[95] L. Gashi and K. Knautz, "Unfriending and becoming unfriended on facebook," *Facets of Facebook: Use and Users*, p. 1, 2016.

[96] T. Saad and F. Khan, "Nudging pakistani users towards privacy on social networks," in *SAI Computing Conference (SAI), 2016*. IEEE, 2016, pp. 1147–1154.

[97] J. Kim and M. Hastak, "Social network analysis: Characteristics of online social networks after a disaster," *International Journal of Information Management*, vol. 38, no. 1, pp. 86–96, 2018.

[98] M. A. Campbell, "Cyber bullying: An old problem in a new guise?" *Journal of Psychologists and Counsellors in Schools*, vol. 15, no. 1, pp. 68–76, 2005.

[99] T. F. A. Rahman, A. G. Buja, K. Abd, and F. M. Ali, "Sql injection attack scanner using boyer-moore string matching algorithm." *JCP*, vol. 12, no. 2, pp. 183–189, 2017.

[100] I. A. Saeed, A. Selamat, and A. M. Abuagoub, "A survey on malware and malware detection systems," *International Journal of Computer Applications*, vol. 67, no. 16, 2013.

[101] P. Headley and K. Collins, "Multi-channel multi-factor authentication," Aug. 23 2011, uS Patent 8,006,291.

TABLE I. FRAUDS WITH THEIR CATEGORIZATION AFTER A COMPROMISED PRIVACY

Social Engineering	**Bank Notes / Bonds**	**Direct Finance / Cash Involvement**	**Grey Areas**
Scareware	Prime Bank Note Fraud	Advance Fee Schemes	Adoption Scams
Grandparent Scam	Redemption/Strawman / Bond Fraud	Bankruptcy Fraud	ATM Skimming
Lottery Scams	Securities and Commodities Fraud	Corporate Fraud	Identity Theft
Natural Disaster Fraud	Social Security Card Fraud	Credit Card Fraud	Phishing
Online Dating Scams	Staged Auto Accident Fraud	Financial Institution Fraud	
Reverse Mortgage Scams	Stock Options Backdating	Funeral Fraud —	Online Activities
Senior Citizen Fraud	Telemarketing	Insider Trading	Pump-and-Dump Stock Scheme
Smishing	Anti-Aging Product Fraud	Prepaid Funeral Scams	Timeshare Schemes
Spear Phishing	Foreclosure Fraud	Insurance Fraud	Gameover Malware
Sports Memorabilia Fraud	Health Care Fraud	Investment Fraud	Work-at-Home Scams
Surrogacy Scam	The Internet Pharmacy Fraud	Letter of Credit Fraud	Artificial Share Value Raising Market Manipulation
Swatting	Mass Marketing Fraud	Mortgage Fraud	Ponzi Schemes
Telephone Denial of Service Fraud	Online Auction Fraud	Nigerian Letter or “419” Fraud	Pyramid Schemes
House Stealing	Online Auto Auction Fraud		
Jury Duty Scam	Telemarketing Fraud		
Online Rental Housing Scheme			

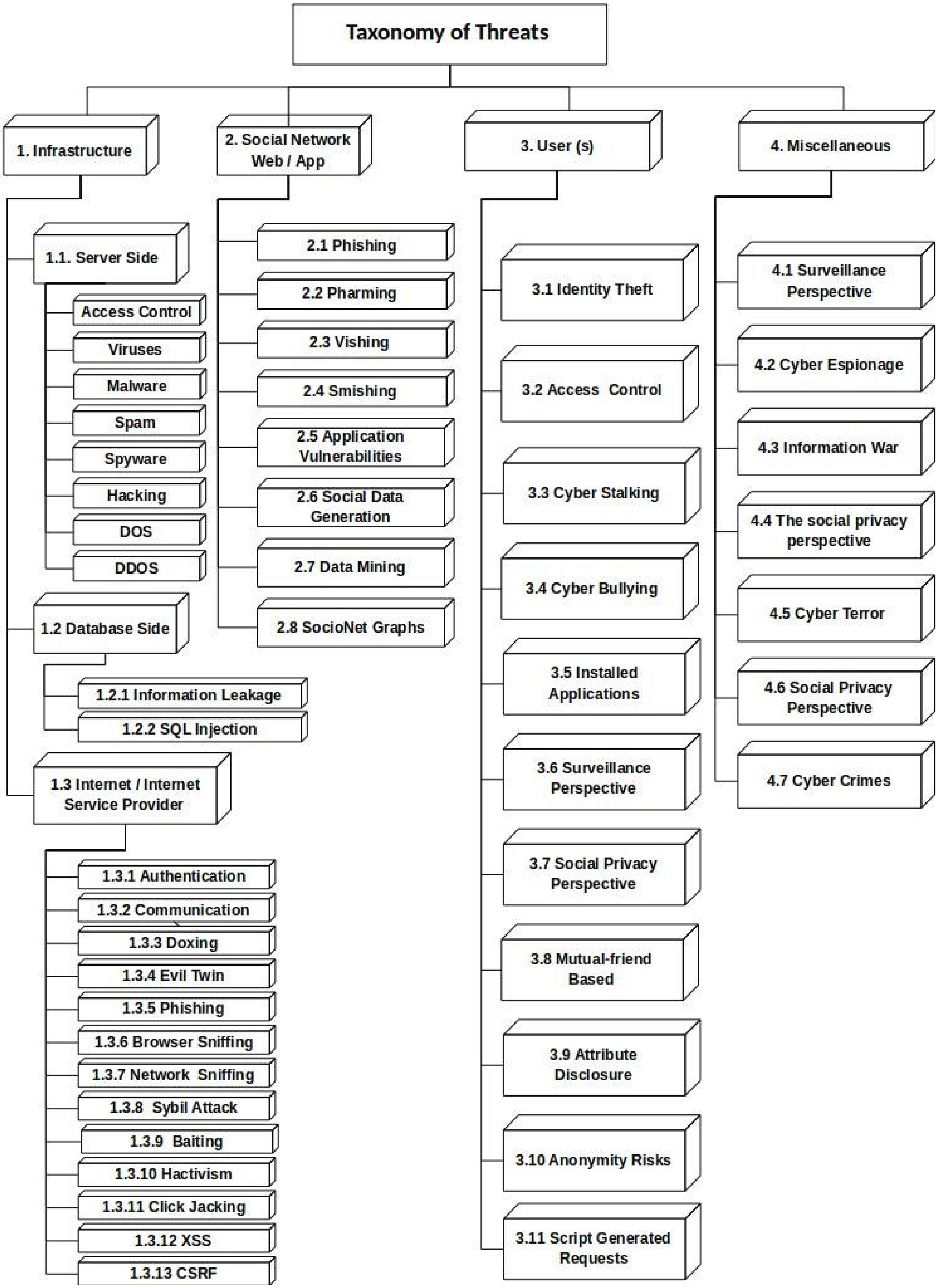

Fig. 1. Taxonomy of Threats to Online Social Networks