IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 8, Issue.12, December 2020 E-ISSN: 2347-2693

Online Intrusion and Security Measures in Social Networking Environment – A Survey

Jamuna Rani S.[1*], Vagdevi S.[2]

[1]Department of Computer Science, Visveswaraya Technological University, Karnataka, India
[2]Department of Science and Technology, Delhi University, Delhi, India
[2]Department of Computational Sciences and Technology, Delhi University, Delhi, India

[*]*Corresponding Author: research.jamuna@gmail.com, Tel.: +91-7892767517*

DOI: https://doi.org/10.26438/ijcse/v8i12.3945 | Available online at: www.ijcseonline.org

Received: 08/Dec/2020, Accepted: 11/Dec/2020, Published: 31/Dec/2020

***Abstract*—** Social networking has become the topmost application among users to share and communicate information. With the advancement in communication and smartphone capabilities increasing number of users are connected to social network. News items, memes and marketing campaigns are all hosted on social network. Enterprises are also using social network to reach to more customer bases. The popular online social networking platforms such as Twitter, Facebook, Instagram etc. have attracted public helping them connected to family, friends, and relatives. People share videos, texts, pictures, and some confidential information knowingly or unknowingly through these sites and thus, OSNs have become the main source of targets for cyber attackers. Cyberattacks have been increasing for the last few decades throwing a serious threat to the internet world. Security of personal data on social network user is important. In this survey, the various methods of intrusion of social networks for gaining access to private information and the countermeasures are studied. The goal of study is to identify open issues, so that a more secure solution can be designed to solve the problem and discuss about various OSN threats such as misuse of identity, malware, phishing attacks etc. and recommends some of the threat's preventive measures.

***Keywords*—**Online Social Networks, Cyberattack, Identity theft, Security

I. INTRODUCTION

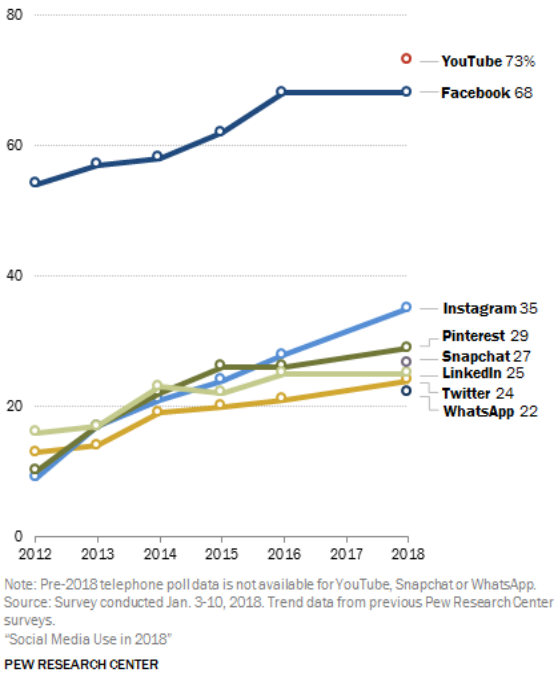
Social Network Services like Facebook, Twitter and Instagram has become popular application for community communications and sharing of information. Various facilities like creating friendship-based links, posts, comments, status, expressing interests etc create overwhelming interests among social network users. There is continuously increasing user base for social network. Recent Pew Research Centre survey of U.S (2018) shows the increasing proliferation of social network user base.

But the hidden problem in social networks is leakage of personal information of the users. This personal information can be used for various purposes like advertisement campaign, password thefts, identity theft etc.

Information shared on social network comes under different categories like:

1. Subscription information: The personal information user has shared while subscribing to the social network service.
2. Shared Information: This information refers to personal information shared in posts, comments, photos, locations and visited places etc.
3. Behavioural information: From this information, the behaviour profile of the user, his interests can be extracted.

Most of user information on social network have public view by default and has higher chances of information leak. Figure1 shows the Facebook features and their default privacy settings.



SECURITY THREATS OF ONLINE SOCIAL NETWORKING PLATFORMS

Few security threats of the social networking sites/platforms are discussed below.

1. Social Engineering- It is a technique of handling persons to obtain private data such as passwords, bank details and access to your personal computers. Cyber criminals use social engineering techniques to earn your trust fooling you and then get access to your sensitive data.
2. Phishing – is one of the ways of social engineering attacks used to steal user's data such as credit card information, login credentials. The victims are attracted to open mails or text messages and then are tricked into a malicious link allowing the installation of malware to extract sensitive information.
3. Fake Accounts-It is a type of cyber-attack where fake account is created and connections are established with random people from various organisations such as defence, government, software companies etc to fetch personal or critical information.
4. Misuse of celebrity names- is one of the famous security threats today. Hackers create a new account in celebrities' name and spread wrong message or rumours about them. They misuse their personal information to spoil their reputation in public. Real time verification of proof of identity is needed to shelter against these dangers.
5. Site Compromise-An attacker introduces a malicious code in the social networking sites. Malicious codes are inserted through advertisements and third-party applications to fetch users' personal information. Any guest to the site will be prone to attack.
6. Spreading Spams and Malwares-OSN sites such as Facebook, Twitter are used to blowout spams and malwares. Cyber criminals today are using shortened URLs making hard for the users to recognize whether it is an unaffected or malicious site.
7. Sensitive Information Leakage-It deals with leaking of technical information by employees to the public. For example, a Twitter remark stating that the customer is tired of constructing a specific firewall product at work or a status message representing that the customer finally found a means around a web proxy product being used and is now capable to post to his profile again. An invader could use this information to recognize the security software of the customer or the company.

II.RELATED WORK

In [1], authors proposed a framework for user-controlled sharing of sensitive personal information. The work advocates user centric security provisioning more than the service provider. To support user centricity the work proposed two strategies 1) ontology-based privacy attribute management and 2) authenticated dictionary-based selective disclosure. In the first strategy, the attributes of user are classified to private attributes with different level of privacy factors and rating. In the second strategy method for sharing of private attributes or subset of attributes is proposed. For every single attribute, it is very difficult for user to configure the private rules and it can be used only for expert users. For naïve users without sufficient knowledge of privacy this solution is very complex.

In [2], authors proposed FaceCloak to provide privacy and security for user privacy attributes. The solution works by positioning between user and Facebook and translating the privacy attributes to fake information and providing to Facebook. By providing the translation of privacy attributes, FaceCloak ensures the seamless service of social network. The problem in this solution is that FaceCloak in addition to translation also stores the private attributes in encrypted form to separate server. This solution can only save subscription information, but it cannot preserve inferred information from posts and comments.

In [3], authors proposed a framework for access control applying ontology. Social network user must do policy refinement to populate ontology with the inferred authorizations/prohibitions. Once authorizations/prohibitions are inferred, security policy enforcement can be carried out. Access control and filtering policies are evaluated upon an access request being submitted. The ontology must be provisioned by user, which is quite difficult considering the various new features launched every time.

In [4], authors proposed a machine learning approach to detect suspicious accounts in online social networks. The solution uses the difference of location characteristics between normal and suspicious accounts on the graph to identify suspicious accounts. When any user is trying to access another account attribute, analysis is done to identify if it is a fake account and the access is denied for fake account.

In [5] authors proposed an anomaly detection technique based on Principal Component Analysis (PCA). This technique models the behaviour of normal behaviour and identifies significant deviation from normal as anomalous. They successfully applied this technique on Facebook to detect fake, compromised, and colluding Facebook identities. The accounts identified as anomaly is blocked to safeguard other users. But the approach is not effective as the attackers can create new accounts and still threaten others privacy.

In [6] author proposed a framework xBook for building privacy-preserving social networking applications. xBook provides three types of enforcement that encapsulate the privacy requirements in a typical social network setting: (1) user-user access control (e.g., access to only friends) for data flowing within one application, (2) information sharing outside xBook with external parties; and (3)

protection of the application's proprietary data. While (1) and (2) protects the privacy of a user from information leaks, (3) prevents the application's proprietary data or algorithm from being leaked to the application users.

In [7] author presented a novel spammer classification approach based on Latent Dirichlet Allocation (LDA), a topic model. In this method, two new topic-based features are extracted and used to discriminate human-like spammers from legitimate users. Authors extracted historical tweets of each user as a document and use the Latent Dirichlet Allocation (LDA) model to compute the topic distribution for each user. Based on the calculated topic probability, two topic-based features, the Local Outlier Standard Score (LOSS) which captures the users interests on different topics and the Global Outlier Standard Score (GOSS) which reveals the users interests on specific topic in comparison with other users, are extracted. The two features have both local and global information, and the combination of them can distinguish human-like spammers effectively.

In [8] author suggests a new approach to tackle the security and privacy problems with emphasis on the privacy of users with respect to the application provider in addition to the defence against intruders or malicious users. For detecting privacy violations, the solution relies on cooperation of other users who are also the users of the application. Trust is calculated for the application by different users and communicated with other users, so that attributes to be shared to application can be controlled by the users. But malicious accounts can be created, and false trust can be communicated to deceive the user. There is no protection against malicious accounts in this approach.

In [9] author proposed a model to measure the susceptibility of users against attacks and predict the victims of attack. Based on network, behavioural and linguistic features, the level of susceptibility of user is calculated. Regression tree model is done using the features and the model was able to predict the victims in social network. Though the approach has not proposed any mechanism for protecting the privacy of the users, it was able to predict the attack for the users.

In [10] author explores how to launch inference attacks using released social networking data to predict undisclosed private information about individuals. To protect privacy, authors sanitized both trait (e.g., deleting some information from a user's on-line profile) and link details (e.g., deleting links between friends) and explored the effect they have on combating possible inference attacks and concluded that just sanitizing trait information or link information may not be enough to prevent inference attacks.

In [11] author introduced a novel social access control (SAC) strategy using multi-level security (MLS) for protecting data on social networks. In MLS, the data objects and subjects are classified in hierarchical levels based on security clearance and access controlled accordingly. Instead of clearance levels, they used trust levels to annotate objects and subjects. The trust level of an object is specified by the creator. The trust level of a subject is obtained from a trust modelling process. Reading a data object is controlled using the relative trust values of subjects and objects.

In [12], authors proposed a privacy monitor for social networks users. Authors considered three threats in social networks Out-of-context information disclosure, In-network information aggregation and Cross-network information aggregation. The monitor crawls the social network profile of user and extracts sensitive information and moves to repository. The information is guarded and not leaked.

In [13], authors presented a method for the detection of these malicious profiles by using the social network's own topological features. Through this method spammers and fake profiles in social networks are detected. Their algorithm uses the fact that social networks are scale-free and have a community structure. This fact ensures that most of the users in the network have a small degree and are connected only to a small number of communities. Fake profiles, on the other hand, tend to establish friendship connections with users from different communities.

In [14] authors proposed a method to detect spammers in social network based on latent user features and user interaction. Features are extracted from text content and social interaction phenomena. Hinge loss in Support vector machine is used as classifier.

In [15] author proposed a honeypot-based approach for detecting spammers in social network. Placement of social honeypot for collecting deceptive spam profiles in social network and statistical analysis of the collected spam profiles are two characteristics of the proposed solution. Features like content similarity, profile similarity learnt from the spam profiles are used to train machine learning classifiers to classify spam accounts in social network.

In [16] authors studied the identify theft issues in social networking platforms and the personal information present in social networking sites has become a breeding ground for information hackers. Authors proposed a set of prevention techniques against data theft consisting of

1. Never Display Details of Personal or Financial Documents:
2. Turn Off Automatic Login Features
3. Avoid Posting Location Updates
4. Setting Stringent Privacy Settings
5. Use of Strong and Unique Passwords
6. Always Connect with Authentic People
7. Using Double Authentication

8. Avoid Using Same Passwords for Multiple Accounts
9. Avoid Geo-Tagging Photos

In [17] authors developed software called Social Privacy Protector to improve the security and privacy of Facebook users. It identifies user's friends who may pose a security threat and restrict friend's exposure to user's personal information. For each friend credit score is given based on analysing the strength of connection. The strength is calculated based on:

1. number of common friends between the user and their friend
2. the number of pictures and videos the user and their friend were tagged in together
3. the number of groups the user and their friend were both members in
4. the number of messages passed between the user and their friend

This system also proposes an easy way to manage the privacy setting in Facebook based on 4 different profiles. User can choose among these 4 profiles, so that each profile has different values for Facebook privacy settings.

In [18] authors developed PoX, an extension for Facebook. Pox makes private data explicit for user and allows user to exert fine grained access control on what data can be shared to individual applications. Pox is implemented as a client-side proxy. It executes entirely in the user's browser and accepts profile data requests from Facebook Platform applications. The proxy scrutinizes each request and enforces access control decisions by verifying that the application sending the request can access the desired information. Requests that pass this check are forwarded to the Facebook servers by the client-side proxy, and the results are passed back to the application.

The summary of the survey is given below.

Table 1 Summary of Survey

Paper	Solution	Limitations
1	User centric controlled sharing of sensitive personal information	It is very difficult for user to configure the private rules and it can be used only for expert users
2	Translating the privacy attributes to fake information and providing to Facebook	Protect subscription information only and cannot preserve inferred information from posts and comment
3	Ontology based policy enforcement	Not adaptive to new attacks
4	Machine learning to detect suspicious accounts	Not effective as attack signature varies over time
5	PCA based anomaly detection of accounts	Not effective as account features are dynamic
6	Privacy wrappers over privacy settings of social network	Difficult to configure setting for each privacy attribute
7	Topic modelling on content to identify spams	Training based and extensive training is not feasible
8	Trust calculation for third party applications	Trust is calculated based on user feedback, so fake accounts can be created to increase the trust value and deceive the users.
9	Regression model to predict the victims.	Cannot solve the Zero-day attack. It can only predict over a period.
10	Sanitizing profile information and friendship links	False positive is high, it can remove even genuine friends
11	Hierarchical security levels of data	Difficult to configure for the users of social network
12	Crawls and add private information to repository	It is not real time by the time secure information is identified, it would have been leaked.
13	Fake profile identification based on community structure	Not effective as the structure can be faked
14	latent user features and user interaction	Cannot prevent privacy leaks to genuine accounts which later turns hostile
15	Collect deceptive spam profiles and classify based on it.	Not effective with rate of accounts created, it cannot prevent information leakage
16	Precautionary rules for ensuring privacy	Very difficult to remember the rules and some of the rules are not quantitative for software implementation
17	Credit scoring of friendship links and 4 security profiles.	Security profiles are limited and not adaptive.
18	fine grained access control on user data	Facebook has around 100 security setting, very difficult to configure each setting and the solution works only for third party applications.

III.METHODOLOGY

Social Networking site encourages their users to reveal great deal of personal information by promising a better user experience. When user signup to social networking sites like Facebook, the sites send constant reminders to update their profile with more personal information such as date of birth, hometown, workplace, schools to find more friends. This is also the case when it comes to posts and other shared information. In [19] analysis is made on the access setting of user's contents shared in Facebook. The survey was conducted on Facebook user set of 200 random users in May 2011. These users had an average of 248

friends, and had uploaded an average of 363 photos, 185 status updates, 66 links, 3 notes, and 2 videos. Only 45 users had uploaded fewer than 10 photos (of which 7 users had uploaded none). 81 out of our 200 users had also created at least one friend list, with a total of 233 observed friend lists. Thus, the average user who had created at least one friend list had 3 friend lists. The user is presented with a few options, which approximates the privacy settings currently allowed by Facebook

1. Only Me (Me) Indicating that the photo should be private to the user.
2. Some Friends (SF) The user is asked which of his friends should be able to access the photo. The user can select friends individually from a list or can specify users using any friend lists they have created.
3. All Friends (AF) Indicating that all the user's friends should be able to access the photo.
4. Friends of Friends (FoF) Indicating that all the user's friends, and all their friends, should be able to access the photo.
5. Everyone (All) Indicating that all Facebook users should be able to access the photo.

Feature	Default privacy setting
Profile picture/ Profile Background picture.	Public
Work and Education: Workplace, professional skills, college, high school.	Public
Places the user has lived in including current city and hometown.	Public
Contact and basic information: email, mobile phone, address, birthdate.	Friends
Other information: gender, language, religious views, political views.	Public
Family members' names and Facebook profiles, relationship status.	Public
Posting thoughts, videos, or pictures to timeline.	Friends
Tagged pictures.	Friends and friends of anyone tagged in the picture

Figure 1 Facebook Privacy Settings

Figure2 shows the Twitter features and their default privacy settings.

Feature	Default Privacy setting
Username and profile name	Public
Photo (profile and background)	Public
Bio (the user can type any brief information about themselves)	Public
Location (which country or city the user lives in)	Public
Website (if the user has one)	Public

Figure 2 Twitter Privacy Settings

Two observations were made in the study.

Type	Count	Me	SF	AF	FoF	Net	All
Photo	65,182	<0.1%	17%	37%	18%	1.3%	26%
Video	428	0.5	5.6	32	11	3.5	48
Status	37,144	0.1	9.7	35	4.5	3.4	47
Link	13,197	<0.1	5.4	36	9.2	2.0	47
Note	602	0.5	6.3	28	5.8	9.8	50
Total	116,553	<0.1%	13%	36%	13%	2.0%	36%

Figure 3 Privacy Settings for content items

Out of 116,553 content items, 41,437 (36%) are shared with default privacy settings, meaning they are easily visible to over 750 million Facebook users. This fraction is significantly higher than those users indicated their desire (20%, discussed in Table below), suggesting that the users have not bothered to change the privacy setting from the default.

Actual setting	Desired setting					
	Me	SF	AF	FoF	All	Total
Me	3	5	2	3	2	15
SF	3	12	28	3	0	46
AF	38	2	184	25	42	291
FoF	16	8	80	15	22	141
All	46	23	171	56	118	414
Total	106	50	465	102	184	907

Figure 4 Actual Privacy Setting

The leakage of information comes under two categories of direct information and inferred information. The extracted information can be used to launch various attacks like targeted advertisements, personal threats, forged message delivery, password hacking etc. These necessities appropriate security measures build into social network to secure the theft of user's private information. The users are unaware of how this private information can be misused by the attackers. As latest feature post which are location tagged are also shared in social network which could bring attacks like kidnap and robbery.

Intrusion like spamming, phishing, identify theft are common in Facebook. Phishing and identify theft are dangerous as they are launched with sole intention of gaining access to users' personal information. The overview of some of the attacks means in social network is given below.

Table 2 Attack Means

Attack	Brief
Sensitive data retrieval	Attackers can collect users' personal data
Sensitive attribute inference	Attributes of user are often correlated. Using this correlation relationship attacker can infer information
Automated User profiling	Retrieval of user's sensitive data by querying social networks for registered e-mail addresses and crawling every profile found to collect personal information
De-anonymise OSN users	Use group membership information that is available on social networking sites to profile users

It is very difficult to evade attackers from social network as they invent new means to intrude into the network every time security measure is launched, so it is better to tighten the data privacy and security. In this aspect leakage of personal information due to security lapses becomes the scope of study for this work. Following are studied in the scope of this work

1. Leakage of information through poor privacy settings
2. Leakage of information to 3rd party application
3. Leakage of information to 3rd party domain

In this work, a survey is done on various means, the private information is leaked through social network and the counter measures to provide security against information leakage. The information can be leaked even by the social network providers in form of datasets for research and analysis. It is not considered for the scope of work. The information leakage caused due to careless handling of data by the user, so that intruder can extract information directly or through inference is considered in this scope of work.

IV. OPEN ISSUES AND DISCUSSIONS

By survey of the existing solutions following problems are found.

1. The current mechanism relies on user to configure their privacy profiles and increasing features provided in social network, configuring an elaborate privacy profile is difficult.
2. There is no way to measure the risk for data and alert the user and make steps to ensure the private data is protected.
3. There is no comprehensive method to prevent privacy exposed through various means like subscription, posts, comments etc.
4. The current solutions are not adaptive to privacy leakage through new features
5. The solution must work for privacy attack from users and third-party applications.
6. There is no way to categorize friends based on the privacy information that can be shared.

Issue 1: Most existing solutions have limited security profiles and tries to fit the users to any one of the security profiles. For each security profile, mapping to privacy setting of social network is done. It gives the convenience to user by not attending to all the privacy settings of social network. Security profiles are very rigid, and user cannot personalize the security settings for this need. Also, Security profile is fixed and not dynamic, so a new personal attribute in introduced into social network, the security profile does not have information on how to manage that attribute.

Issue 2: There is no way in social network to measure the risk of the account. The risk must be measured in terms of probability of information loss. It is very much necessary to measure the risk and notify the user as this early warning can allow user to make informed decisions. Current Social media information give default public access to all information of users through which direct or in direct inference can be made about personal information.

Issue 3: Most existing solutions focus only on the security of profile attributes and do not give importance to leak of personal information via posts, messages, comments, likes. More than profile attributes, this secondary information is source of wealth of information for attackers. Attackers can learn a lot about users in terms of user interest, user personality traits. Information extracted about users can be used for many purposes like targeted advertisements, blackmails etc.

Issue 4: Social networks are evolving in terms of new features. Social network providers add upgrades and features frequently to attract user interest and remain competitive. Each feature collects additional personal information from users. With more personal information feed into social network, the risk of data theft also increases. Most existing solutions are fixed for certain attributes are not scalable for new attributes. Without adaptation to new attributes, the solution is not full proof.

Issue 5: Data theft attacks on social networking accounts can be launched by other users, third party applications and third-party domains. The means deployed for data theft is different for these attackers. So, the security solution must be full proof against all means. Most existing solution focus only on any one of attack sources leaving the rest thus the solutions are not full proof.

Issue 6: Friendship link is the main theme of social networks. In social network a friendship link is always assumed to be trustworthy, but it is not always the case. Also, some of friendship links accepted is only for purpose of increasing the likes and shares. These links can also leak personal information later. So, there must be way to access the creditability of friendship link frequently.

IV.CONCLUSION

The paper summarizes the current works in protection of privacy for social network users. The solutions are addressed from the scope of leakage of user private information through other users or third-party applications. Though these surveys open issues were addressed in existing solutions. This serves as motivation for designing solutions to solve the open issues.

REFERENCES

[1] Shin, D., R. Lopes, W. Claycomb, G. Ahn, "A Framework for Enabling User-controlled Persona in Online Social Networks," in 33rd Annual IEEE International Computer Software and Applications Conference, **pp. 292–297, 2009.**

[2] Luo, W., Q. Xie, and U. Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking Sites," in Proc. of PASSAT-09, **pp. 26-33, August 2009.**

[3] Carminati, B., E. Ferrari, R. Heatherly, M. Kantarcioglu, B. Thurainsingham, "A Semantic Web Based Framework for Social Network Access Control" in Proc. SACMAT'09, **pp. 177-186, June 2009**

[4] Bo Feng, Qiang Li, Xiaowen Pan GroupFound: "An effective approach to detect suspicious accounts in online social

networks", International journal of distributed sensors 19 **February 2017.**
[5] Viswanath B, Bashir MA, Crovella M, et al. Towards detecting anomalous user behavior in online social networks. In: Proceedings of the 23rd USENIX security symposium (USENIX security 14), San Diego, CA, 20–22 **pp.223–238, August 2014.** USENIX Association
[6] K. Singh, S. Bhola, and W. Lee, "XBook: Redesigning Privacy Control in Social Networking Platforms," Proc. 18th Usenix Security Symp. (SSYM 09), Usenix Assoc., **pp. 249–266, 2009.**
[7] LinqingLiu, YaoLu, YeLuo "Detecting Smart spammers On Socia lNetwork: A Topic Model Approach" Proceedings of NAACL-HLT **2016**
[8] L., Molva, R., Strufe, T.: Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Communications Magazine 47(12), **94–101, 2009.**
[9] Claudia Wagner "When social bots attack: Modeling susceptibility of users in online social networks" 1012 Proceedings on International conference on World Wide Web
[10] Jack Lindamood, Raymond Heatherly "Inferring Private Information Using Social Network Data" WWW 2009, **April 20–24, 2009**
[11] Richmond Hill "A trust-based approach for protecting user data in social networks" CASCON '07 Proceedings of the 2007 conference of the center for advanced studies on Collaborative research
[12] Bo Luo; Lee, D., "On Protecting Private Information in Social Networks: A Proposal," Data Engineering, 2009. ICDE '09. IEEE 25th International Conference on, vol., no., **pp.1603,1606, March 29, 2009-April 2, 2009**
[13] M. Fire, G. Katz, and Y. Elovici," Strangers Intrusion Detection Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies", HUMAN, 1(1), **pp: 26-39, 2012.**
[14] Hua Shen, Xinyue Liu "Detecting Spammers on Twitter Based on Content and Social Interaction" International Conference on Network and Information Systems for Computers **2015**
[15] Lee K, Caverlee J, Webb S. Uncovering social spammers: social honeypots+ machine learning. Proceeding of the 33rd international ACM (SIGIR) conference on Research and development in information retrieval, Geneva, Switzerland, 2010:435-442.
[16] Shareen Irshad1 and Tariq Rahim Soomro "Identity Theft and Social Media" IJCSNS International Journal of Computer Science and Network Security, **VOL.18 No.1, January 2018.**
[17] Michael Fire, Dima Kagan, Aviad Elishar, and Yuval Elovici "Social Privacy Protector - Protecting Users' Privacy in Social Networks" The Second International Conference on Social Eco-Informatics SOTICS **2012**.
[18] M. Egele, A. Moser, C. Kruegel, and E. Kirda, "Pox: Protecting users from malicious facebook applications," in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on. IEEE, **pp. 288–294, 2011.**
[19] Y. Liu, K. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. ACM, **pp. 61–70, 2011.**

AUTHORS PROFILE

Ms. Jamuna Rani S pursued Bachelor of Engineering from Visveswaraya Technological University, India in 2007 and Master of Technology from Visveswaraya Technological Unoversity in year 2014. She is currently pursuing Ph.D. and currently working as Research Associate in Department of Digital Business and Analytics,Jagadish Sheth Schoolof Management (formerly IFIM B School),Bangalore,India since 2018.Her main research work focuses on Technology Readiness Index, Technology Adoption Model, Data Security and Privacy, Big Data Analytics, Data Mining, Computational Intelligence based education. She has 5 years of Industry and Consulting experience and 4 years of Research Experience.

Dr.Vagdevi.S pursued Bachelor of Engineering from UVCE, Master of Science from UVCE, and Master of Science from BITS-Pilani. Completed her Ph.D from VMU, Salem during 2011.she is currently working as Visiting Professor in Department of Information Science and Engineering, DSATM, Bangalore since 2019. She is a member of IEEE & ISTE.She has published more than 20 research papers in reputed international journals and conferences including IEEE and it's also available online. Her main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Data Security and Privacy. She has 30 years of teaching experience and 10 years of Research Experience.

