A Survey on Data Security in Social Networking Sites

Pragya Pradhan
M.Tech,
Department of Computer Science and Engineering
Sikkim Manipal Institute of Technology, Sikkim, India

Santanu Misra
Associate Professor,
Department of Computer Science and Engineering
Sikkim Manipal Institute of Technology, Sikkim, India

Tawal Koirala
Assistant Professor I,
Department of Computer Science and Engineering,
Sikkim Manipal Institute of Technology, Sikkim, India

ABSTRACT
The popular communication Social Networking Sites (SNS) like Facebook, Twitter, LinkedIn etc have become in style and well-liked during the past few years and are utilized by billions of individuals irrespective of their age groups for communicating either with old friends, relatives from far places or total strangers. As they allow users to both articulate their eccentricity and meet people with similar interests. Risks posed by SNS are becoming harder to conquer due to publication of social network data by user which may contain personal or confidential information. There is a high possibility of this information to be misused by people with harmful motives like stalking, identity theft, online victimization etc. Therefore there arises an urgent need to safeguard users from attacks occurring in SNS, as users are still unaware of these threats. Moreover, a user does not have control about what others reveal about them. The attackers of SNS mainly use social engineering attack to victimize the user through malicious URL links, applications, Spam messages etc. URL has an important role in detecting phishing websites. So, this focuses on the detection and prevention of malicious URLs as they are used to mount various attacks like spamming, phishing, malware etc.

General Terms
Security, issues, attacks, suspicious URLS etc

Keywords
Suspicious URLs, cyber criminals, cyber threats, SNS users, approaches etc.

1. INTRODUCTION
A social networking site is a dedicated website or application which enables users to communicate with each other, either old friends or strangers, by posting information, comments, messages, images etc. Social networking sites like Facebook, Twitter, Instagram, LinkedIn, MySpace, etc allows millions of individuals to construct public or semi-public profiles within that website and form relationships with others of the same website. To get started with any of these websites requires only a little knowledge of it and to create a profile. Among these websites Facebook is one of the most accessed websites by all age groups at recent times. The main element of social networks is to find friends and search for people that they know and then build up their own online community.

In the matter of these few decades, Researchers and Developers have an emerging interest to protect users of ever growing Social Networking Sites such as Facebook, Twitter etc reason due to being a prime target of cyber criminals. These sites are driven by a network of trust between friends who may be someone close or stranger. An entry point of malware infections is the online social trust, so a person from a trusted list can be an attacker wishing to do harm by plotting an attack to execute malware or steal personal information of a user. These malware can be a suspicious URLs designed to extract personal information or to direct users to malicious websites. Uniform Resource Locator (URL) link is an address of the web page which consists of protocol identifier and resource name and is not easy to identify legitimate URL with naked eye. These URL links sometimes contain malicious codes embedded on it and for certain pages content might also be hidden in images. Users are not informed before accessing any data in SNS, so access to such pages should ideally be denied to protect users from such unknown attacks as sometimes even the domain name of the legitimate websites may be spoofed.

2. ISSUES IN SOCIAL NETWORKING SITES
There are several issues and concerns in social networking sites arising with evolving time as it provides millions of active users interconnected to each other with respect to interests, occupation, business etc. The major issues are: identity theft, online victimization, stalking, leakage of personal information, profile cloning, spam, malware etc. This survey focuses mainly on the social network malware which is a malicious software used by cyber criminals to showcase their production. Attackers in social networking sites are most active during disaster and events [14] and they also use fan page groups or popular people to lure users to be the victim of their attacks.
The attacks used in Social Networking Sites are mainly of two types which are:

[1] Social Engineering attack: It refers to psychological manipulation of people for the purpose of information gathering, fraud or system access, a type of confidence trick. This technique is based on specific attributes of human decision-making known as cognitive biases, sometimes called "bugs in the human hardware". Social engineering targets human weaknesses instead of vulnerabilities in technical systems.

[2] Reverse Social Engineering attack: It is a person-to-person attack, where the attacker does not initiate contact with the victim. Rather, the victim is tricked into contacting the attacker herself. From [6] the combination of attractive profile with an incentive or a pretext is decisive for RSE attacks to work in practice.

3. RELATED WORK
In past years, there have been extensive researches and improvement on the security of SNS users against advanced cyber criminals. Various researchers have proposed new

techniques using multiple methodologies for security purpose and some of them are mentioned below.

Till date there are lots of attacks in social networking sites like cross site scripting, spam, online groomers, identity theft, stalking etc, which are handled using feature extraction, classification and detection algorithms. This survey describes the methodology and approaches used by different researchers to secure social networking sites data and its users.

In 2009, **Justin Ma et.al,** [1] described an approach to automatically generate features to detect malicious websites from suspicious URLs using statistical methods and URL classification algorithms like Naive Bayes, Support Vector Machine (SVM) and Logistic Regression. This approach classifies the reputation of a Web site entirely based on the inbound URL to provide inherently better coverage than blacklisting based approaches.

In 2010, **Dwen-Ren Tsai et.al,** [2] worked on the concept of proxy and proposed a real-time website security protection mechanism. Through the proxy, client side information was transmitted to the social networking website and the security threats of the website which includes web-based malware, phishing websites and malicious connection were detected and determined. This also segregates the client and the networking threat by integrating commercial protection software and online security scanning services into a security module and executing webpage security threat scan simultaneously. They have conducted cross analysis of security threats with service infrastructure of social networking website and the CIA triad and introduced the concept of website security scanning service through cloud computing to provide internet users secured networking internet.

Same year, **Gianluca Stringhini et.al,** [3] studied and analyzed the extent of spam and how spammers operate in social networking site. To detect spammers some characteristics were identified and spam detection tool was built and used on Twitter and Facebook dataset. While differentiating between real users and spam bots, it was noticed that spam bots share some common traits. Based on the strategies and activities of spam bot, four categories of bots were distinguished namely: Displayer, Bragger, Poster and Whisperer. To collect the data about spamming activity diverse set of "honey-profiles" were created in different social networking sites to collect data. This collected data was analyzed to identify anomalous behavior of users. Machine learning techniques were used to classify.

In 2011, **Hyunsang Choi et.al,** [4] proposed a similar work as Dwen-Ren but has focused only on detection of malicious URLs of all popular attack types and identifies the nature of attack. The first task is a binary classification problem and the second task is a multi-label classification problem which is solved using Support Vector Machine (SVM) to detect malicious urls and two multi-label classification methods: RA*k*EL and ML-*k*NN used to identify attack types. The discriminative features are classified into 6 groups namely: lexicon, link popularity, webpage content, DNS, DNS fluxiness, and network traffic. The link popularity features (LPOP) outperformed all the other groups of features for detecting any type of malicious URLs. The webpage content features (CONT) are useful in distinguishing malware URLs from benign ones. This is because malware URLs usually have malicious tags or scripts in their Web content to infect visitors.

Another technique called multiparty access control for online social networking was proposed by **Hongxin Hu, et.al,** [9] in 2013 which formulates an access control model to capture essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. A proof-of-concept prototype of this approach was implemented as an application in Facebook which is an authorization mechanism that provides usability study and evaluation of the method. Data sharing patterns concerning multiparty authorization in OSNs were identified. Based on these patterns, MPAC model was formulated to capture the core features of multiparty authorization requirements that have not been accommodated by existing access control systems and models for OSNs. This model contains a multiparty policy specification scheme which also supports analysis on MPAC model and systems.

In 2014, **Michael Fire et.al,** [10] presented an overview of existing solutions that provide better protection, security and privacy for users. It offers simple-to-implement platforms for users. These solutions are 1. Employing user authentication mechanisms such as CAPTCHA to ensure registering or logging user is a real person, photos-of-friends identification etc, 2. Applying user privacy settings where user can customize their privacy settings and choose which other users in the network such as Friends, Friends of Friends, and everyone are able to view their details, pictures, posts and other personal information, 3. Internal Protection Mechanisms like Facebook Immune System (FIS) by Facebook which is an adversarial learning system that performs real-time checks and classifications on read-and-write actions on Facebook's database that activates to protect its users from malicious attacks.

In the same year **Amardeep Singh et.al,** [11] described the categories of privacy breach in Social networking sites and the challenges to preserve them. They presented some techniques for the same and gave research direction for future work. The three categories of privacy breach are identity disclosure, sensitive link disclosure and sensitive attribute disclosure. Proposed algorithm is modified form of algorithms for micro data which depends on some modified algorithms developed for anonymization against neighborhoods attacks. Proposed algorithm was able to increase the level of privacy for social network users by anonymizing and diversifying disclosed information. An anonymization methodology has been proposed by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties.

Same year 2014, **Manjeet Chaudhary et.al,** [12] proposed a new technique for detecting suspicious URL detection for Twitter called WARNINGTWEET to find the correlations of URL redirect chains extracted from several tweets. They have considered correlations of URL redirect chains extracted from a number of tweets because attacker's resources are generally limited and need to be reused. The paper focused on the characteristics of URL redirect chains and the similarity of a group of users who uploaded the same URL redirect chains for immediate verification where 50 percent were chosen as the value for the labeling threshold using L1- regularized logistic regression algorithm.

In 2015, **Shital B. Mandhane et.al,** [16] presented a study on the techniques to identify and analyze poor quality content on Facebook and other social networks. It also seeks to understand the limitation on availability of data for collection and analysis posed by Facebook. This paper considered three distinct areas i.e. Facebook social graph, attack and detection

techniques with respect to malicious content on Facebook and analysis of events using online social media data.

In 2016, **Nemi Chandra Rathore et.al,** [17] proposed a simple trust-based privacy preserving mechanism called CACM (Collaborative Access Control Mechanism) to allow the users to control access of their shared resources in a collaborative manner. A Facebook application "msecure" was developed and a 'survey based user study' of the application with a user base of 50 people was done. Its primary component is Collaborative policy specification that uses user's trust. The application has a light and sleek user interface and does not use any centralized data manager for implementation. CACM allows all the stakeholders of a data item to specify the trust level which would be required to access the data item at the time of collaborative policy specification. It calculates average threshold and minimum threshold trust level that is stored in form of the access policy of the resource.

Same year a hybrid approach is proposed by **Saurabh Muthal et.al,** [18]. This approach presented a comprehensive experimental evaluation of features and algorithms including boosting and shows that dictionary-based baselines are not good enough to be high-performance URL-based topic classifiers, though they do achieve high precision. The potential use of inlinks is explored. The proposed system uses two machine learning techniques: K-means for clustering the feature values as two clusters and Naïve Bayes calculates the independent probability and classification of the feature and have five models namely: Data Collection, Feature Extraction, Manage and View, Clustering, Classification and Detection. The proposed system extracts lexical features of the URL and does not depend on whitelist or blacklist mechanism.

In 2016, **Amol C. Jadhav et.al,** [19] developed a new technique that will apply fuzzy logic based techniques on the features of URL to detect phishing sites. They extracted feature such as lexical and host-based from the phishing website sample through term frequency and then a system was developed where sample categorization or phishing website categorization into families that share some common traits are applied by using kernel k-means clustering method. This paper focused on two aspects, 1.URL in detecting phishing websites and 2. Fuzzy logic to detect phishing websites. The author has proposed the new heuristics to detect phishing website more effectively and rapidly. Then, to make the result more precise and objective, new fuzzy-based approach has been proposed such that rule set is not utilized. Finally, to make model equivalent for new dataset the threshold values used in the membership functions are derived from the big data set.

4. ANALYSIS OF RESEARCH GAP

Table 1. Table captions should be placed above the table

Sl. No.	Researchers	Description	Research Gap
1.	Justin Ma et. al, 2009	• Algorithm used: Naive Bayes, Support Vector Machine (SVM) and Logistic Regression • Obtained 95-99% accuracy.	• Cannot predict the status of previously unseen URLs. • It is not scalable.
2.	Hongxin Hu et. al, 2014	• MPAC model was formulated to capture the core features of multiparty authorization requirements.	• Privacy conflict was not resolved. • Collaborative management of shared data needs improvement.
3.	Manjeet Chaudhary et. al, 2014	• Algorithm used: L1- regularized logistic regression. • Focuses on the correlations of multiple redirect chains that share the same redirection servers.	• Dynamic and Multiple redirections need to be incorporated. • Should be more scalable.
4.	Nemi Chandra Rathore et. al, 2016	• CACM allows all the stakeholders of a data item to specify the trust level that is stored in form of the access policy.	• Need for semi-automatic mechanism to assign trust value to their contacts by user.
5.	Amol C. Jadhav et.al, 2016	• Algorithm used: Fuzzy logic, kernel k-means clustering on TF and TF-IDF for phishing website categorization.	• Feature extraction of phishing websites needs enhancement. • Anomaly detection can be used with clustering algorithm.
6.	Saurabh Muthal et. al,2016	• Algorithm used: K-means for clustering the feature values and Naïve Bayes to calculate the independent probability and classification of the feature.	• Dynamic structure of URLs needs to be addressed.

5. CONCLUSION

This survey focuses on different algorithms and methodologies used by various researches to protect users of Social Networking Sites from intended and unintended attacks. It is seen that mostly used algorithm are clustering and classification algorithms to detect the malicious behavior in social networking sites.

Other techniques like Fuzzy logic, Biometric and URL Pattern Mining were also used to make a better detection system. But again these certain techniques with high accuracy can together be combined to make an automatic system which can be integrated in Social Networking Sites for the better security of the users.

Different algorithms can be integrated in future to achieve better detection performances as attackers are perfecting their creations with various attacks and the existing methods can be enhanced using techniques other than clustering and classification algorithms.

Users of SNS should also be made aware especially during events about the attacks and the types of attacks because Cyber criminals are most active during these periods.

6. REFERENCES

[1] Justin Ma, Lawrence K. Saul, Stefan Savage, Geoffrey M. Voelker, "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs", In Proc. 15th ACM SIGKDD Int. Conf. Mining, pp. 1245–1254, 2009.

[2] Dwen-Ren Tsai, Allen Y. Chang, Sheng-Chieh Chung, You Sheng Li, "A Proxy-based Real-time Protection Mechanism for Social Networking Sites", In Security Technology (ICCST), IEEE International Carnahan Conference, pp. 30-34, 5 Oct 2010.

[3] Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna, "Detecting spammers on social networks", In Proceedings of the 26th Annual Computer Security Applications Conference pp. 1-9, ACM, 6 Dec 2010.

[4] Hyunsang Choi, Bin B. Zhu, Heejo Lee, "Detecting Malicious Web Links and Identifying Their Attack Types", InWebApps, June 2011.

[5] Lubos Takac, Michal Zabovsky, "Data Analysis in Public Social Networks", International Scientific Conference & International Workshop Present Day Trends of Innovations, 28th – 29th May 2012.

[6] Awad WA., "Machine Learning Algorithms In Web Page Classification", International Journal of Computer Science & Information Technology (IJCSIT), Vol 4, No 5, Oct. 2012.

[7] Nahier Aldhafferi, Charles Watson, A.S.M Sajeev, "Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 2, No. 2, April 2013.

[8] Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, Sapna Sinha, "Social Networking Sites and Their Security Issues", International Journal of Scientific and Research Publications, Vol 3, Issue 4, ISSN 2250-3153, April 2013.

[9] Hongxin Hu, Gail-Joon Ahn, Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms", IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 7, July 2013.

[10] Michael Fire, Roy Goldschmidt, Yuval Elovici, "Online Social Networks: Threats and Solutions", IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter 2014.

[11] Amardeep Singh, Divya Bansal, Sanjeev Sofat, "Preserving Techniques in Social Networks Data Publishing- A Review", International Journal of Computer Applications (0975 -8887), Vol. 87-No.15, February 2014.

[12] Manjeet Chaudhary, H.A Hingoliwala, "Warning Tweet: A Detection System for suspicious URLs in Twitter Stream", International Journal for Research in Applied Science and Engineering Technology (IJRASET), Vol. 2, Issue VII, ISSN: 2321-9653, pp. 297-305, July 2014.

[13] Huang D, Xu K, Pei J., "Malicious URL detection by dynamically mining patterns without pre-defined elements", World Wide 9, 1375-94, Nov. 2014.

[14] Jyoti D.Halwar, Sandeep Kadam, Vrushali Desale, "Detection of Suspicious URL in Social Networking Site Twitter: Survey Paper", International Journal of Computer Applications (0975-8887), Vol. 110-No. 8, January 2015.

[15] Neeraja M, John Prakash, "Detecting Malicious Posts in Social Networks Using Text Analysis", International Journal of Science and Research (IJSR) ISS (Online): 2319-7064 Index Copernicus Value (2013): 6.14, Impact Factor (2015): 6.391.

[16] Shital B. Mandhane, Ismail Mohammed, "A Survey on a FRAppE: Detecting Malicious FacebookApplications", International Journal of Advance Research in Computer Science and Management Studies, ISSN: 232 7782 1 (Online), Volume 3, Issue 11, November 2015.

[17] Nemi Chandra Rathore, Prashant Shaw and Somanath Tripathy, "Collaborative Access Control Mechanism for Online Social Networks", Springer International Publishing Switzerland, 2016.

[18] Saurabh Muthal, Ameya Pawar, Saurabh Harne, "A Hybrid Approach to Detect Suspicious URLs", IJARIIE-ISSN (O)-2395-4396, Vol-2 Issue-2 2016.

[19] Amol C. Jadhav, A. M. Pawar, "Enhancement in Phishing Detection Using Features Clustering", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, ISSN: 2277 128X, June 2016.