ISSN 2278-3091

Volume 10, No.3, May - June 2021

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1291032021.pdf

https://doi.org/10.30534/ijatcse/2021/1301032021

Cyber Attacks Impacting on Communication Using Social Media: Systematic Review Using Data Cluster Ball

Saima Shoro[1], Abdullah Maitlo[2],Haque Nawaz[3], Inayatullah Soomro[4], Allah Dino Seelro[5].

Department Of Computer Science

[1]Shah Abdul Latif University Khairpur Mir;s, Sindh, Pakistan, shorosaima@gmail.com

[2]Shah Abdul Latif University Khairpur Mir;s, Saindh, Pakistan,Abdullah.maitlo@salu.edu.pk

[3]Madressatul Islam University Karachi, Sindh Pakistan, hnlashari@smiu.edu.pk

[4]Shah Abdul Latif University Khairpur Mir;s, Sindh, Pakistaninayat.soomro@saluedu.pk

[5]Govt Superior Science College Khairpur Mir's Sindh Pakistan, ada.seelro@gmail.com

ABSTRACT

In this advanced technological era, the internet especially social media plays an important role in our lives. Because through social media everyone can easily communicate with their relatives and loving ones. Its usage is increasing day by day which also facilitate the Cyber Criminals to perform cyber acts using these networks. There are several networks such as Instagram, Twitter, Facebook and LinkedIn etc. which are utilized by the users on daily basis, though which they can communicate and share their data with their family, friends and relatives easily. But while using these networks they are unaware of their security issues. Through hacking their accounts cyber criminals can exploit their personal data and can use it for illegal acts. This article tends to provide the systematic literature review on several cyber-attacks over social media. The main objective of this article is to present the cyber-attacks within literature which can helps to find out the security gaps.

Key words: Cybercrime, Cyber-attack, Cyber Threats, Social media, Cyber criminals.

1. INTRODUCTION

The term Cyber refers to the interconnection of computers in a network. In this world of technology on network the number of users has been increased which may increase the security risks termed as "cyber security". Cyber security can be defined as the security of data from unauthorized access over the network. Several users over the network are unaware of these security risks. Recently the use of Social Media has been increased day by day because it provides a virtual environment for communication. Social Media are the type of online applications which allows the users to interconnect with each other by sharing their images, text and profiles etc. [1]. Social Media can be defined as a network of individuals, termed as nodes and are interconnected with each other relationships, mutual interests knowledge and information exchange. [2]. Due to increased usage of internet, mostly the people prefer social networking sites to communicate with their loving ones. [3]. these sites can easily connect the peoples at remote areas to interact with each other very quickly. All social networking sites enable users to register on them before using these sites. There several social networks like as Facebook [5], LinkedIn [6], Google+ [7], Sina Weibo [8], VKontakte (VK) [9] Twitter [5], Tumblr [6]. (Shown in Figure 1)

Figure 1: Social Networks

These networks are utilized by hundreds of millions users daily. Facebook, for example, has more than 1.23 billion monthly active users, 945 million of which are active mobile Facebook users as of December 2013 [8]. Facebook users have a total of over 150 billion friend connections and upload on average more than 350 million photos to Facebook each day [11]. Regrettably, several user are not aware about the security risks of social media communication such as privacy risks [12], [13], identity theft [14], malware [15], fake profiles (also in some cases referred to as sibyls [16], [17] or socialbots [12], [18], [19]), and sexual harassment [20], [21], among others. According the investigation by Dwyer et al. [22] the users of Facebook and

MySpace have blindly trust on these social networks and their users [23].which leads to the information sharing and relationship development. Whereas from recent studies [12], [24] it is found that several social networks users are exploring their intimate and personal data such as address, contact number and pictures by directly posting on Social media. Moreover, the study by. [12]. [19], [25], found that on Facebook several users can share their data by accepting the request of unknown persons. This data can be utilized in virtual or real world for harmful or malicious acts. Because of huge amount of users these sites became the main target cybercriminals for cyber-attacks. The cyber criminals can easily access their personal information by using these sites. AS the several users are unaware of the privacy setting, so they can easily become target of privacy breach. This article tends to provide the detailed review on several cyber-attacks using social media which can helps to find out the security gaps on social media.

2. LITERATURE DATA COLLECTION AND DATA MINING METHODOLOGY

This study extends beyond the scope of a typical research survey article. The data mining techniques were used to gather literature from a range of sources in order to provide a complete picture of cyber-crime on social media. The technique for gathering relevant literature and mining the articles in this section.

2.1. High level Approach

The objective of this study is to conduct a thorough analysis of cyber-attacks and its solutions. A simple method would be to look through the papers presented at major conferences and manually choose those that are connected to cybercrime. This strategy, however, would be insufficient. While academia proposes the majority of the remedies, independent researchers and cyber-security firms have uncovered a huge number of real-world attack events and social network weaknesses, exposing critical cyber vulnerabilities. In this study, academic works are compared to literature from a variety of different sources, such as Articles, reports and conferences. This enables to provide a full picture of current cyber-attacks on social networking sites. The majority of assault instances are published online, and manually looking for them is impractical due to the fact that the majority of search engine results are either irrelevant or duplicates. To create appropriate searches, we use Google's search engine APIs [8] and domain expertise.

After that a smart web named as crawler was constructed that uses those searches, as well as meaningful combinations of them, to automatically collect everything relevant to Google's search engine. In order to filter out the irrelevant items set of heuristics were used. Then, using cutting-edge data mining algorithms, the articles were grouped together to highlight the high-impact articles. As a consequence, there are 117 clusters with at least three online reports, totally 973 articles. Finally, to find 70 distinct attacks these articles were manually evaluated. Whereas the publications that aren't specifically about cybercrime were excluded. Some papers may cover both defenses and solutions.

2.2. Article Collection

As previously stated, gathering attacks events reported by industry and individual researchers is difficult, owing to the wide range of probable sources. To solve this problem, a sophisticated web crawler was created that collects articles and reports from the internet.

The functions are described as follow:

Construction of Quires and search

The smart web crawler does an initial gathering of online articles using Google search engine APIs. In this study, the more systematic approach was utilize to creating these queries. Three keyword sets were created in particular:

A. Cyber-crime keywords

B. Social networking keywords

C. Security keywords

The queries are generated automatically by the crawler, which selects terms from these three groups: A unique combination of four words from set (c) is chosen for each word in set (a). For each word in the (b) set, the process is repeated. This method generates 2000 queries. The crawler selects the first 100 results for each query. All collected online articles are entered into a database that will be made available to the public and updated on a regular basis.

Content Parser

Finding attacks occurrences and their original published source might be difficult given the large number of online reports collected by our clever crawler. To deal with this, we created a content parser module that consists of two parts:

1. Content filter

2. Clustering of articles

1. Content Filter

The content filter's main goal is to rapidly filter out online reports that aren't related to cyber-attacks. The filter works in two stages, one after the other. The content filter removes sites in the first step. The goal of the second step of content filtering is to do more in-depth filtering. It focuses on the article's actual text content to ensure that it is relevant. The parser uses diffbot to extract the title, author, publish date and content at this point. The program next checks for the existence of the original query keywords in the title and text of the report once again. This is required to avoid the occurrence of keywords in other parts of the source code.

2. Clustering of Articles

After the removal of noise in the gathered article the next step was to concentrate on finding high impact articles. This is done by aggregating online articles describing similar attacks occurrences using clustering. To generate a collection of terms, first step is the title and content evaluation. The Title Weight to the title was assigned to reflect its prominence over the content. Then, using the title and text, the conventional natural language processing techniques like tokenization, stemming, stop word removal, punctuation, and number filtering were used to get a collection of weighted words. The characteristics vectors are then extracted using the tf-idf keyword extraction method. Finally, a minimal spanning tree was created by constructing a distance matrix based on the collected feature vectors' cosine similarity. We generate a forest where each tree is a cluster by pruning the edges that don't meet the Cluster Threshold. It's not easy to figure out what the best values for the Title Weight and Cluster Threshold are. To overcome this, we examine various combinations of these values. The ground truth was created by manually labelling 90 articles that span 25 distinct attacks subjects into different groups. Then we experiment with different numbers to see whether we can automatically cluster the 90 articles with the rest of the reports. The degree to which those identified articles are appropriately grouped together and segregated in distinct clusters is used to assess the efficacy of various combinations. The above whole clustering scenario is illustrated in Figure 2.

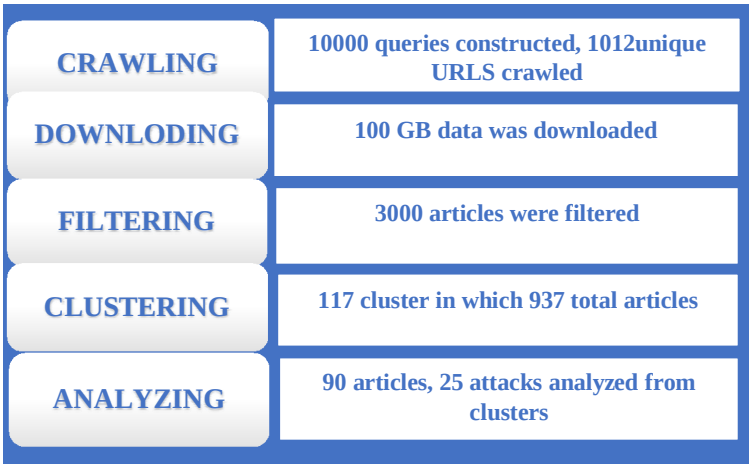

Figure 2 Clustering Articles framework For Literature Review

3. LITERATURE REVIEW:

In the articles [26][27][28] [29] and [30] [31] discussed the classic attacks attacks. Whereas [32][33][34][35][36][37][38][39][40][41][42][43][44][45][46][47][48][49][50][51][52][53][54][55][56][57][58][58][59][60]discussed several Modern attacks. [61][62][63] Discussed the cyberbullying.[64] discussed several sites of social networking to examine their cyber-attacks, their taxonomy and also highlighted their solutions . A survey was conducted by [65] to find out the users opinion about social networks security issues. [66] Investigated social network usage and the security issues faced by the university students. The three institutes of Nigeria were selected for investigation. To collect the data questionnaire was used. The investigation reveals that, several issues were faced by users. [67] Discussed several techniques to solve the privacy issues. Likewise [68] highlighted several social networking security and privacy risks and their preventions. [69] Gives the systematic review of mobile networks challenges and their solutions. [70] Discussed that there are several security issues faced by the users while using social network sites. Thus the users and organizations should pay attention to cope with these threats. In the paper [71] introduced an extremely secure authentication technique using voice recognition system for cyber threats preventions on social media, [72] argued various cyber-crimes and their detection techniques .[73] highlighted the reasons of committing cybercrimes and their methods and also highlighted an analytical approach cyber-crimes trends. [74] Explained several security issues of social media and also discussed an architecture which is useful exchange of data securely. In the research [75] discussed an analytical investigation of cyber-attacks via social media. [76] Described the emerging threats experienced the users

on social media. [77] Highlighted the patterns, countermeasures and trends of cyber threats [78] investigated the opinion of undergraduates of third party observers witnessing cyberbullying via social networking.. In the paper the main focus of [79] was how the personal information is being affected by social networks and their security and privacy risk. In the report published by [80], have discussed the teenagers social media usage, the main focus was to discuss the new security settings made by several social media sites. In the survey report [81] several security and privacy issues were published. In the paper [82] Krishnamurthy and Wills [83] Leitch and Warren [84] C. Marcum et al. [85] aware the users from several security breaches on social media. Boyd and Hargittai [86] also discussed the interest of teenager regarding social media especially facebook. F. Stutzman and J. Kramer-Duffield [87] Yabing Liu, et al., [88] introduced a method to enhance the privacy setting of personal information via social media. In the paper A. Verma et al. [89] introduced a distributed architecture to preserve the user's security on social media by using cryptographic method. The attacks found in literature in clustered graph shown in Figure 3.

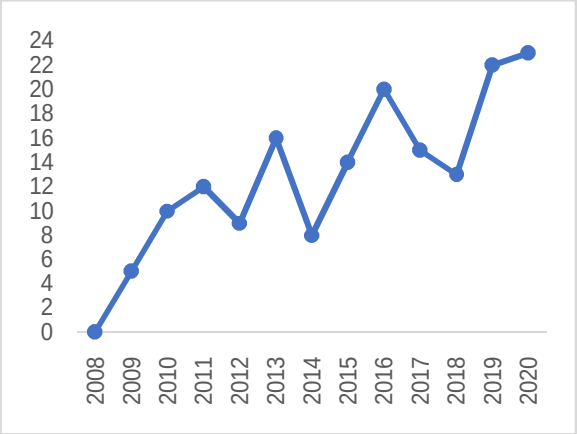

Figure 3 Clustering Cyber-attacks From Literature

3.1 Cyber Attacks

The attackers uses three types of attacks to perform their illegal acts. Several attacks were highlighted in clustered literature some of which are discussed below

3.1.1Classic attacks

The classic threats comprises of both privacy and security threats such as malware, spam, cross-site scripting (XSS) attacks, or phishing.

A. Malware
Malware, or malicious software, is any program or file that is harmful to a computer user. The first propagated malware was Koobface. [15]

B. Spammers
Spamming is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. [47] In the articles [70] and [71] discussed the spammer's attacks in 2009 and 2013.

C. Cross-site scripting
Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application In the year of 2019 the attackers used the XSS worm named as Mikeyy, to target several celebrities through twitter [73]

D. Phishing
Phishing is a type of social engineering attack often used to steal user data, In recent investigations [67] [68] [69] shows the interests towards social media and impacts of their polite nature, which may help the attackers to achieve their targets.

3.1.2. Modern attacks
These attacks are totally concerned with user's personal information. These attacks comprises of Click jacking, De-Anonymization, Fake profiles and identity clone attacks.

A. Click jacking
It is a kind of malicious technique used to target the user through clicking the spam link or messages. [76] Whereas, [77] discussed this attack attempt by the attackers in 2009 usig twitter website.

B. De-Anonymization
In these kinds of attacks attackers uses several techniques such as user group membership, tracking cookie and network topology to explore the users real identity. The [11][78][79][80][81][82][83] discussed the several techniques used by attackers for De-Anonymization attacks such as face recognition.

C. Fake profile
Fake profiles refers to the socialbots or automatic portfolio which mimic the human behavior on social network. [12][17][84][85][86] Discussed the several attacks attempted through this technique.

D. Identity clone
Through technique the attackers make the duplicate copy of users account to distract their friends and followers. [13][89] Discussed the several clone techniques used by the attackers on different social media platforms to target the confidential data of several organizations and their impact.

3.1.3. Combination attacks

These attacks are the combination of both modern and classic attacks. The attackers targeted the timeline of a user for sophisticated attack. [87].

3.1.4. Youth targeted attacks

The main target of these attacks are new generations which is fond of social media. These kinds of attacks includes cyberbullying.

A. Cyberbullying

Also termed as cyber is a type of harassment that takes place technological communication platforms such as sexual harassment. The authors [90][91][92] gives a detailed review on cyberbullying.

The Cyber Attacks are illustrated in Figure

Figure 4 Cyber Attacks

4. FINDINGS

The literature review findings are illustrated in Table 1.

FINDINGS				
Paper	**Year**	**Cyber Attacks**	**Privacy Issues**	**Solutions of Cyber Attacks**
[98] [99]	2021	✓		✓
[97]	2020	✓		
[95][96]	2019			✓
[94]	2018	✓		✓
[93]	2017	✓		✓
[75]	2016	✓		
[79]	2016		✓	
[71]	2016			✓
[76]	2015	✓		
[81][83]	2015		✓	
[74]	2015			✓
[28][29] [30][41] [73]	2014	✓		
[84]	2014		✓	
[27][47] [50][52] [64][78]	2013	✓		
[65][70]	2013		✓	
[46][49] [62][63]	2012	✓		
[68][69]	2012		✓	
[68][69]	2012			✓
[35][48] [51]	2011	✓		
[66]	2011		✓	
[80]	2011		✓	
[36][40] [45][53] [54][56] [57][59] [60][61]	2010	✓		
[67][87] [88]				✓
[34][38] [39]	2009	✓		
[33]	2008	✓		

Table 1 Findings of Literature

5. CONCLUSION:

Social Media provides a tremendous way of communication to the users, so they can interact with their relatives and friends anywhere anytime around the world. There are several benefits of social media but it also contain various security issues. Now a days the users are very fond of social media and mostly prefer these sites for communication. They post their personal data on these accounts and also add the strangers to expand their social gaps. But this might be accessed by the authorized persons through various techniques and can be utilized for illegal acts. This paper reveals the systematic review of the research presented by authors previously. Various kind of cyber-attacks were discussed which faced by the users in last decades. To avoid these kind of attacks the users must update their security setting and do not post their personal data on these kind of networking sites. .

REFERENCES

1. W. Ghari and M. Shaabi "Cyber Threats in Social Networking Websites," International Journal of Distributed and Parallel Systems, vol. 3, no. 1, pp. 119-126, 2012.
2. V. L. Yisa, O. Osho, and I. Soje, “Online Social Networks: A Survey of Usage and Risks Experience among University Students in North-Central Nigeria,” International Conference on Information and Communication Technology and Its Applications, pp. 129–133, Nov. 2016.
3. D. Hiatt and Y. B., "Role of Security in Social Networking," International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, 2016
4. Facebook, accessed Jan. 14, 2014. [Online]. Available: http://www. facebook.com/
5. Google+, accessed Jan. 14, 2014. [Online]. Available: https://plus. google.com/
6. LinkedIn, accessed Jan. 14, 2014. [Online]. Available: http://www. linkedin.com/
7. Sina Weibo, accessed Jan. 14, 2014. [Online]. Available: http://www. weibo.com/
8. witter, accessed Jan. 14, 2014. [Online]. Available: http://www.twitter. com/
9. Tumblr, accessed Jan. 14, 2014. [Online]. Available: http://www.tumblr. com/
10. VKontakte, accessed Jan. 14, 2014. [Online]. Available: http://www.vk. com/
11. Facebook, Facebook Reports Fourth Quarter and Full year 2013 Re- sults, accessed Jan. 14, 2014. [Online]. Available: http://investor.fb.com/ releasedetail.cfm?ReleaseID=821954
12. J. Feinberg, accessed Jan. 14, 2014. [Online]. Available: http://www. wordle.net/
13. Wikipedia, List of Virtual Communities With More Than 100 Million Active Users, accessed Sep. 8, 2013. [Online]. Available: http://en. wikipedia.org/wiki/List_of_virtual_communities_wit h_more_than_ 100_million_active_users
14. Facebook, Form 10-k (Annual Report)—Filed 02/01/13 for the Period Ending 12/31/12, 2013, accessed Jan. 9, 2014. [Online]. Available: http://files.shareholder.com/downloads/AMDA-NJ5DZ/2301311196x0 xS1326801-13-3/1326801/1326801-13-3.pdf
15. Y.Boshmaf,I.Muslukhov,K.Beznosov,andM.Ripeanu, “Thesocialbot network: When bots socialize for fame and money,” in Proc. 27th Annu. Comput. Security Appl. Conf., 2011, pp. 93–102.
16. A. Mislove, B. Viswanath, K. Gummadi, and P. Druschel, “You are who youknow:Inferringuserprofilesinonlinesocialnetworks ,”inProc.3rd ACM Int. Conf. Web Search Data Mining, 2010, pp. 251–260.
17. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, “All your contacts are belong to us: Automated identity theft attacks on social networks,” in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 551–560.
18. J. Baltazar, J. Costoya, and R. Flores, “The real face of koobface: The largest web 2.0 botnet explained,” Trend Micro Res., vol. 5, no. 9, p. 10, 2009.
19. Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services,” in Proc. 9th USENIX Conf. NSDI, 2012, p. 15. [Online]. Available: http://dl.acm.org/ citation.cfm?id=2228298.2228319
20. G. Stringhini et al., “Follow the green: Growth and dynamics in twitter followermarkets,”inProc.Conf.InternetMeas.Conf.,20 13,pp.163–176.
21. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu (2013, Feb.). Design and analysis of a social botnet. Comput. Netw., Int. J. Comput. Telecommun. Netw. [Online]. 57(2), pp. 556–578. Available: http://dx. doi.org/10.1016/j.comnet.2012.06.006
22. A. Elyashar, M. Fire, D. Kagan, and Y. Elovici, “Organizational intru- sion: Organization mining using socialbots,” in Proc. IEEE/ASE Int. Cyber Security Conf., 2012, pp. 7–12.
23. J. Wolak, D. Finkelhor, K. Mitchell, and M. Ybarra, “Online “predators” and their victims,” Psychol. Violence, vol. 1, pp. 13–35, 2010. [21] M. Ybarra and K. Mitchell, “How risky are social networking sites? A comparison of places online where youth sexual solicitation and harass- ment occurs,” Pediatrics, vol. 121, no. 2, pp. e350–e357, Feb. 2008.
24. C. Dwyer, S. R. Hiltz, and K. Passerini, “Trust and privacy concern withinsocialnetworkingsites:Acomparisonoffacebook andmyspace,” presented at the 13th Americas Conf. Information Systems (AMCIS), Keystone, CO, USA, 2007, Paper 339. [Online]. Available: http://aisel. aisnet.org/amcis2007/339/
25. MySpace, accessed Jan. 14, 2014. [Online]. Available: http://www. myspace.com
26. A. Acquisti and R. Gross, “Imagined communities: Awareness, informa- tion sharing, privacy on the facebook,” in Privacy Enhancing Technolo- gies. New York, NY, USA: Springer-Verlag, 2006, pp. 36–58.
27. A. Elyashar, M. Fire, D. Kagan, and Y. Elovici, “Homing socialbots: Intrusion on a specific organization’s employee using socialbots,” in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining, 2013, pp. 1358–1365.
28. T. Amin, O. Okhiria, J. Lu, and J. An, Facebook: A Comprehensive Analysis of Phishing on a Social System, 2010, accessed Feb. 1, 2014. [Online].Available:https://courses.ece.ubc.ca/412/ter m_project/reports/ 2010/facebook.pdf
29. D. Cavit et al., Microsoft Security Intelligence Report Volume 10, 2010, accessed Mar. 11, 2014. [Online]. Available: http://www.microsoft.com/ en-us/download/details.aspx?id=17030

30. E. Mills, Facebook Hit by Phishing Attacks for a Second Day, Apr. 2009, accessed Jan. 14, 2014. [Online]. Available: http://news.cnet. com/8301-1009_3-10230980-83.html
31. A.Chowdhury,StateofTwitterSpam,Mar.2010,accessedJan.14,2014. [Online]. Available: https://blog.twitter.com/2010/state-twitter-spam
32. L. Tristan, Twitter's Growing Spam Problem, Forbes, Jul. 2013, ac- cessed Mar. 3, 2014. [Online]. Available: http://www.forbes.com/sites/tristanlouis/2013/04/07/twitters-growing-spam-problem/
33. B. Livshits and W. Cui, "Spectator: Detection and containment of java- script worms," in Proc. USENIX Annu. Tech. Conf., 2008, pp. 335–348.
34. I. Paul, "Twitter worm: A closer look at what happened," PCWorld, San Francisco, CA, USA, Apr. 2009. [Online]. Available: http://www.pcworld.com/article/163054/twitter_mikeyy_worm_stalkdaily.html
35. Informed Investor Advisory: Social Networking, North American Se- curities Administrators Association (NASAA), Washington, DC, USA, Sep. 2011. [Online]. Available: http://www.nasaa.org/5568/informed- investor-advisory-social-networking/
36. J. Halliday, "Facebook fraud a 'Major Issue'," The Guardian, London, U.K., Sep. 2010. [Online]. Available: http://www.theguardian.com/technology/2010/sep/20/facebook-fraud-security
37. R. Lundeen, J. Ou, and T. Rhodes, "New ways I'm going to hack your web app," in Proc. Blackhat AD, 2011, pp. 1–11.
38. R. McMillan, "Researchers make wormy twitter attack," PCWorld, San Francisco, CA, USA, Mar. 2009. [Online]. Available: http://www.pcworld.idg.com.au/article/296382/researchers_make_wormy_twitter_ attack/
39. B. Krishnamurthy and C. E. Wills, "On the leakage of personally identi- fiable information via online social networks," in Proc. 2nd ACM Work- shop Online Social Netw., 2009, pp. 7–12.
40. G. Wondracek, T. Holz, E. Kirda, and C. Kruegel, "A practical attack to de-anonymize social network users," in Proc. IEEE Symp. SP, 2010, pp. 223–238.
41. Xing,accessedJan.14,2014.[Online].Available:http://www.xing.com/
42. O. Peled, M. Fire, L. Rokach, and Y. Elovici, "Entity matching in online social networks," in Proc. Int. Conf. SocialCom, 2013, pp. 339–344.
43. The Faces of Facebook. [Online]. Available: http://app. thefacesoffacebook.com/
44. A. Acquisti, R. Gross, and F. Stutzman, "Faces of facebook: Privacy in the age of augmented reality," in Proc. BlackHat USA, 2011, pp. 1–56. [84] J. R. Douceur, "The sybil attack," in Proc. 1st Int. Workshop IPTPS, 2002, pp. 251–260. [Online]. Available: http://dl.acm.org/citation.cfm?id=646334.687813
45. H. Gao et al., "Detecting and characterizing social spam campaigns," in Proc. 10th ACM SIGCOMM Conf. Internet Meas., 2010, pp. 35–47.
46. C. Taylor, Startup Claims 80% of its Facebook ad Clicks Are Coming From Bots, Jul. 2012. [Online]. Available: http://techcrunch.com/2012/ 07/30/startup-claims-80-of-its-facebook-ad-clicks-are-coming-from- bots/
47. N. Perlroth, "Fake twitter followers become multimillion-dollar busi- ness," The New York Times, New York, NY, USA, Apr. 2013. [Online]. Available: http://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/
48. T. Ryan, "Getting in bed with Robin Sage," in Proc. Black Hat Conf., 2010, pp. 1–8.
49. J. Lewis, "How spies used facebook to steal NATO chiefs' details," The Telegraph, London, U.K., Mar. 2012. [Online]. Available: http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to- steal-Nato-chiefs-details.html
50. M. Fire, R. Puzis, and Y. Elovici, "Organization mining using online social networks," arXiv preprint arXiv:1303.3741, 2013.
51. H.Mao,X.Shuai,andA.Kapadia,"Loosetweets:Ananalysisofprivacy leaks on twitter," in Proc. 10th Annu. ACM Workshop Privacy Electron. Society, 2011, pp. 1–12.
52. S. Torabi and K. Beznosov, "Privacy aspects of health related informa- tion sharing in online social networks," presented at the USENIX Work- shop Health Information Technologies, Washington, DC, USA, 2013. [Online]. Available: https://www.usenix.org/conference/healthtech13/workshop-program/presentation/torabi
53. L. Scism and M. Maremont, "Insurers test data profiles to identify risky clients," Wall Street J., Nov. 2010. [Online]. Available: http://
54. J.Vicknair,D.Elkersh,K.Yancey,andM.C.Budden,"Theuseofsocial networking websites as a recruiting tool for employers," Amer. J. Bus. Educ., vol. 3, no. 11, pp. 7–12, Nov. 2010.
55. L.Humphreys,"Mobilesocialnetworksandsocialpractice:Acasestudy of dodgeball," J. Comput.-Mediated Commun., vol. 13, no. 1, pp. 341– 360, Oct. 2007.
56. L. Humphreys, P. Gill, and B. Krishnamurthy, "How much is too much? Privacy issues on twitter," in Proc. Conf. Int. Commun. Assoc., 2010, pp. 1–29.
57. Z.Cheng,J.Caverlee,andK.Lee,"Youarewhereyoutweet: Acontent- based approach to geo-locating twitter users," in Proc. 19th ACM Int. CIKM, 2010, pp. 759–768. [Online]. Available: http://doi.acm.org/10.1145/1871437.1871535
58. Pleaserobme.com. [Online]. Available: http://pleaserobme.com/

59. J. Van Grove, “Are we all asking to be robbed?” Mashable, New York, NY, USA, Feb. 2010. [Online]. Available: http://mashable.com/2010/02/ 17/pleaserobme/ [100] FourSquare. [Online]. Available: http://www.foursquare.com/
60. G. Friedland and R. Sommer, “Cybercasing the joint: On the privacy implications of geo-tagging,” in Proc. 5th USENIX Conf. HotSec, 2010, pp.1–8.[Online].Available:http://dl.acm.org/citation.cfm?id =1924931. 1924933
61. K. Murphy, “Web Photos that reveal secrets, like where you live,” The New York Times, New York, NY, USA, Aug. 2010. [Online]. Available: http://www.nytimes.com/2010/08/12/technology/personaltech/12basics. html
62. M. Rahman, T. Huang, H. Madhyastha, and M. Faloutsos, “Efficient and scalable socware detection in online social networks,” in Proc. 21st USENIX Conf. Security Symp., 2012, pp. 32–32.
63. M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, “FRAppE: Detecting malicious facebook applications,” in Proc. 8th Int. Conf. Emerging Netw. Exp. Technol., 2012, pp. 313–324.
64. T.-K. Huang, M. S. Rahman, H. V. Madhyastha, and M. Faloutsos, “An analysis of socware cascades in online social networks,” in Proc. 22nd Int. Conf. World Wide Web, 2013, pp. 619–630.
65. Y. Altshuler, N. Aharony, Y. Elovici, A. Pentland, and M. Cebrian, “Stealing Reality: When Criminals Become Data Scientists (or Vice Versa),” in Security and Privacy in Social Networks, Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, and A. Pentland, Eds. New York, NY, USA: Springer-Verlag, 2013, pp. 133–151. [Online]. Avail- able: http://dx.doi.org/10.1007/978-1-4614-4139-7_7
66. S. Livingstone and L. Haddon, Child Safety Online: Global Challenges and Strategies, 2011.
67. Psychology Today Diagnosis Dictionary, Pedophilia, 2010. [Online]. Available: http://www.psychologytoday.com/conditions/pedophilia
68. M. Deans, The Story of Amanda Todd, The New Yorker, Oct. 2012. [Online]. Available: http://www.newyorker.com/online/ blogs/culture/2012/10/amanda-todd-michael-brutsch-and-free-speech- online.html
69. Lpsos, One in Ten (12%) Parents Online, Around the World Say Their Child has Been Cyberbullied, 24% Say They Know of a Child Who has Experienced Same in Their Community, Jan. 2012. [Online]. Available: http://www.ipsos-na.com/news-polls/pressrelease. aspx?id=5462
70. M. Pearce, “Florida girl, 12, found dead after bullies said ‘Kill Yourself’,”LosAngelesTimes,LosAngeles,CA,USA,Sep.2013.[On- line]. Available: http://articles.latimes.com/2013/sep/12/nation/la-na-nn-florida-cyberbullying-20130912
71. R. Jabee and M. Afshar, "Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)," International Journal of Computer Applications, vol. 144, no. 3, pp. 36-40, 2016.
72. A. Singh, D. Bansal, and S. Sofat, "Privacy Preserving Techniques in Social Networks Data Publishing - A Review," International Journal of Computer Applications, vol. 87, no. 15, pp. 9-14, 2014.
73. 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.
74. Y. Najaflou, B. Jedari, F. Xia, L. T. Yang and M. S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks," in IEEE Systems Journal, vol. 9, no. 3, pp. 834-854, Sept. 2015.
75. L. Dehigaspege, U. Hamy, H. Shehan and D. Dhammearatchi, "Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition," International Journal of Scientific and Research Publications, vol. 6, no. 10, pp. 120-126, 2016.
76. M. Prasanthi, "Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 3, pp. 45-48, 2015.
77. R. Chouhan, "Cyber Crime: A Changing Threat Scenario in the State Of Art," International Journal of Engineering Research and General Science, vol. 3, no. 2, pp. 1206-1216, 2015.
78. A. Kumar, S. Kumar Gupta, S. Sinha and A. Kumar Rai, "Social Networking Sites and Their Security Issues," International Journal of Scientific and Research Publications, vol. 3, no. 4, pp. 1-5, 2013
79. S. D. Trivedi, M. Chandani, M. Tosal and T. Pandya, "ANALYTICAL STUDY OF CYBER THREATS IN SOCIAL NETWORKING," International Conference on Computer Science Networks and Information Technology, vol. 3, no. 2, pp. 32-36, 2016.
80. R. Chandramouli, "Emerging social media threats: Technology and policy perspectives," 2011 Second Worldwide Cybersecurity Summit (WCS), London 2011, pp 1-4.
81. A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, vol. 28, pp. 24-31, 2015.
82. M. Carter, "Third Party Observers Witnessing Cyber Bullying on Social Media Sites," Procedia - Social and Behavioral Sciences, vol. 84, pp. 1296-1309, 2013.
83. Chewae M., Hayikader S., Hasan M H. and Ibrahim J. 2015 How Much Privacy We Still Have on Social Network?. International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015 Edition,page no:1.

84. Gangopadhyay S and Dhar M. D. social networking sites and privacy issues concerning youths. Article – 2 Global Media Journal-Indian Edition Sponsored by the University of Calcutta/www.caluniv.ac.in ISSN 2249 – 5835 Summer Issue/June 2014/Vol. 5/No. 1.
85. Gunatilaka D. A Survey Of Privacy And Security IssuesInSocialNetwork.http://www.cse.wustl.edu/~jain/c se571-11/ftp/social/index.html.
86. Pesce and Casas Privacy Attacks in Social Media Using Photo Tagging Networks: A Case Study with Facebook
87. D. Boyd and E. Hargittai. 2010. Facebook privacy settings:Who cares?" Journal on the Internet, 15(8), 2010.
88. Krishnamurthy B. 2010. I know what you will do next summer. acmsigcomm Computer Communication Review, 40(5):65-70, Oct. 2010.
89. Leitch S and Warren M. Security Issues Challenging Facebook.
90. Verma, Kshirsagar D. and Khan S. 2013. Privacy and Security: Online Social Networking, Association of Computer Communication Education for National Triumph (ACCENT), vol. 3, no. 8, pp. 310-315, 2013.
91. Marcum C.D. and Higgins E.G. (April 28, 2014 by CRC Press) Social Networking as a Criminal Enterprise. Criminal Justice & Law [Online]. Available at: http://www.crcpress.com/product/isbn/9781466589797 (Accessed: 31 Nov 2014).
92. Liu Y., Gummadi K.P., Krishnamurthy B. and Mislove A. Analyzing Facebook Privacy Settings: User Expectations vs. Reality
93. Chhaya L, Sharma P, Bhagwatikar G, Kumar A. Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. Electronics. 2017 Mar;6(1):5.
94. Liang G, Weller SR, Luo F, Zhao J, Dong ZY. Distributed blockchain-based data protection framework for modern power systems againstcyber attacks. IEEE Transactions on Smart Grid. 2018 Mar 27;10(3):3162-73.
95. Soni, Sumit, and Bharat Bhushan. "Use of Machine Learning algorithms for designing efficient cyber security solutions." In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1, pp. 1496-1501. IEEE, 2019.
96. Alnasser, Aljawharah, Hongjian Sun, and Jing Jiang. "Cyber security challenges and solutions for V2X communications: A survey." *Computer Networks* 151 (2019): 52-67.
97. Singh Lallie, Harjinder, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." *arXiv e-prints* (2020): arXiv-2006.
98. Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & Security* 105 (2021): 102248.
99. Al-Mousa, Mohammad Rasmi. "Analyzing Cyber-Attack Intention for Digital Forensics Using Case-Based Reasoning." *arXiv preprint arXiv:2101.01395* (2021).