INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 6)
Available online at: www.ijariit.com

A Novel research on how to measure and optimize the security of Social Network Security (SNS) to achieve the goal of building a trustworthy, efficient, and secure SNS ecosystem

Madhumita
madhumita15.md@gmail.com
Maharshi Dayanand University, Rohtak, Haryana

ABSTRACT

Web-based social networking security is the way toward investigating dynamic web-based life information so as to ensure against security and business dangers. Each industry faces a remarkable arrangement of dangers on social, huge numbers of which have placed associations in the press or at the focal point of discussion. In this investigation, we present the different parts of social, arrange and physical security related with the utilization of informal organizations, by presenting the systems behind each and outlining important security studies and occasions identified with every theme. It has been for some time comprehended that the far-reaching utilization of person to person communication destinations can furnish aggressors with new and crushing assault vectors. In this investigation we endeavour to jump further into every method of security danger, and also affirm the security chance related to every theme by giving true budgetary/social outcomes. We perceive that while associations and people may have authentic business/individual uses for informal organizations, we prescribe explicit moves be made to support more grounded client mindfulness, more secure programming plans and also better hierarchical responsibility. Interpersonal organizations are extremely prevalent in this day and age. A huge number of individuals utilize different types of interpersonal organizations as they enable people to interface with loved ones, and offer private data. Be that as it may, issues identified with keeping up the protection and security of a client's data can happen, particularly when the client's transferred substance is sight and sound, for example, photographs, recordings, and sounds.

Keywords— *Social network service, Security and privacy, Multimedia data, Security threats, Social media*

1. INTRODUCTION

A Social Network Service (SNS) is a sort of web benefit for setting up a virtual association between individuals with comparative interests, foundations, and exercises. An SNS enables its clients to discover new companions and grow their friend network. Information sharing is another key component of an SNS where clients can share their interests, recordings, photographs, exercises, etc. As of late, SNS, for example, Twitter and Facebook have turned out to be wanted media of correspondence for billions of online clients. These administrations join client made profiles with a correspondence system that empowers clients to be associated with their companions, families, and partners. The noticeable quality of these administrations is because of the way that clients can refresh their own data, interface with different clients, and peruse other part's profiles. SNSs can be extremely useful for clients since they recoil financial and land fringes. Likewise, they can be used for accomplishing objectives identified with occupation looking, amusement, and instruction. Be that as it may, the prominence of SNSs makes a high hazard for their clients. The substantial measure of individual information that clients share on SNSs makes them an attractive focus for assailants.

For a newcomer to the web field, informal communication destinations are a perpetually prominent route for individuals to remain associated. Some may even dare to state business openings are shaped and lost on the web, as our web nearness turns into an indispensable piece of our own lives. In a period where our online character eclipses our real character, as well as other key budgetary and individual frameworks also, the potential security dangers related to these informal organizations can't be focused on enough. Throughout the years, analysts and programmers alike have distinguished a bunch of security dangers extending from individuals, the procedure to the application. The reason for this examination is to give a broad diagram of the significant security subjects encompassing informal organizations today and present the basic components behind each. We catch up with some unmistakable outcomes that each hazard may have, lastly give a heading to take a gander at as far as an arrangement.

In numerous SNSs, for example, Facebook, for the most part, sight and sound information is created and shared. As per a report from Zephoria Digital Marketing (ZDM), roughly 136,0 0 photographs are transferred each 60 s on Facebook. An arrangement of measurements from Social Media Today demonstrates that the normal survey and sharing rate of

recordings on Facebook is expanding step by step. As of now, roughly 8 billion recordings for each day are seen on Facebook, which is twofold the sum seen in 2015. Because of the tremendous measure of mixed media information accessible on Facebook, security dangers are likewise expanding. A malignant client can share noxious data on an SNS by covering it inside sight and sound information. Also, thusly, an aggressor can without much of a stretch discover the client's vital data, for example, client character and area. Some SNSs, similar to Twitter, don't enable clients to uncover huge private data, however, aggressors can construe the sequence of a client's posted substance on an SNS and can uncover their undisclosed private data. In 2005, MySpace was assaulted by the Sammy worm, which abused the vulnerabilities in MySpace and transmitted rapidly. It didn't take clients' close to home data, however, regardless it dangerously affected MySpace's general tasks. In April 2009, Twitter was assaulted by the Mikeyy worm, which additionally did not take clients' close to home data, but rather supplanted their information with some unusable information. In May 2009, Facebook was assaulted by the Koobface worm, which stole huge data, for example, a client's secret phrase.

Fig. 1: Social network security

With the expanding measure of customary dangers and dangers because of mixed media information in SNSs, numerous specialists and security partnerships have proposed different answers to alleviating these dangers. Such arrangements incorporate watermarking, steganalysis, and computerized blankness for securing SNS clients against dangers because of sight and sound information. Then again, different arrangements, for example, spam location and phishing recognition, have been proposed to moderate conventional dangers. Be that as it may, many implicit security arrangements, for example, verification instruments and security settings, and business arrangements, for example, minor screen and social assurance application, likewise fill in as protections against the two sorts of dangers in SNSs.

2. NORMAL SECURITY PROBLEMS

In spite of these legitimate security worries about the Web, a portion of the reasons a man's online networking account is imperilled are self-prompted. Five normal slip-ups that can uncover a record include:

2.1. Neglecting to log out

Increment the security of your web-based life account by continually logging out when you step far from your PC or PC. It's best to go above and beyond and shut down the program you were utilizing to see your record. On the off chance that you leave your record signed in, you set yourself up to be hacked in light of the fact that any individual who can get to your PC can get to your record, change the secret phrase or even post things and speak with your companions as though they are you. Logging out and closing down the program is significantly more imperative on the off chance that you utilize an open PC.

2.2. Tapping on enticing ads

Infections and malware frequently discover their direction onto your PC through those irritating, yet once in a while luring advertisements. Be that as it may, on the Web, much the same as, in actuality, on the off chance that an offer appears to great to be valid, it presumably is. Spare yourself a potential security cerebral pain - don't click.

2.3. Associating with strangers

Be cautious of who you acknowledge solicitations from when assembling your online system. Associating and imparting data to individuals you don't know can be unsafe. On the off chance that you get companion demands from outsiders, it's best to remain away. Further, in the event that you get companion demands from individuals, you do know, yet are as of now associated with by means of a similar site, it's conceivable that somebody has set up a phony record. Abstain from tolerating copy demands, rather checking in with the 'genuine' individual to check whether the demand is legitimate.

2.4. Utilizing third party apps

Some portion of the intrigue of online networking locales are all the different diversions and applications. Despite the fact that countless are sheltered, you do allow the application a specific dimension of consent concerning your data. Ensure you recognize what the application is survey and sharing before consenting to the terms.

2.5. Uncovering too much information

Ensure you comprehend the dimension of protection or absence of security - you are consenting to while volunteering individual data.

2.6. Neglecting to utilize security settings

Web-based life locales give you the capacity to confine who approaches your data. For instance, Facebook (like others) gives you a chance to choose who your companions are and what content they can see. One practice to build your record's security is to cripple a large portion of the choices and after that re-open them once you comprehend what the settings explicitly mean to your record.

3. ELECTRONIC SOCIAL NETWORKING

There are countless networks accessible to anybody with an Internet association.

3.1. General sites

In case you're keen on associating with loved ones, there are two essential destinations on the Internet that anybody can join. Facebook and MySpace are both exceptionally well known and gloat a powerful element set. These destinations likewise make it simple to scan for individuals with explicit interests and attributes, so they have turned into an extraordinary gathering ground for making new companions.

3.2. Business sites

Informal communication destinations designed explicitly for organizations, for example, LinkedIn and Opportunity, enable you to associate with partners and business contacts. These two

locales have a lot of highlights that are outfitted explicitly to vocation improvement. With these sites you can:

1. Create and join business-related gatherings
2. Give and get positive proposals and references
3. Get acquainted with business contacts through your system
4. Find work or look for potential representatives

3.3. Social bookmarking sites

Another harvest of social bookmarking destinations, for example, Reddit, have sprung up that enable individuals to bookmark and vote on connections, and the more votes a connection gets, the more individuals it is appropriated to. These administrations can give a ton of fascinating perusing in the event that you are searching for data on explicit themes.

3.4. Blogging services

Utilizing a blogging administration is an extraordinary method to interface with other individuals. These destinations not just give you a place to record your contemplations, yet in addition enable you to coordinate with others.

Live-journal enables you to make a blog and check your posts open, private, or companions as it were. The site additionally houses a huge number of dynamic networks on any number of points, which are an extraordinary place to visit with others and meet new individuals.

Fig. 2: Electronic social networking

4. SOCIAL INTERACTION VS ELECTRONIC MEDIA USE

Social interaction is an exchange between two or more individuals and is a building block of society. Social interaction can be studied between groups of two (dyads), three (triads) or larger social groups. By interacting with one another, people design rules, institutions and systems within which they seek to live.

Electronic media are media that use electronics or electro mechanical audience to access the content. This is in contrast to static media (mainly print media), which today are most often created electronically, but do not require electronics to be accessed by the end user in the printed form.

Here are three areas in which technology may negatively impact relationships:

- **Intimacy:** Intimate relationships often have their own challenges, and changing technologies can contribute even more to the stress of modern relationships.
- **Distraction**: Technology can be an effective distraction in the current moment, over a long period of time, and even in its absence.
- **Depression**: Heavy use of social media has also been shown to negatively affect mental health.

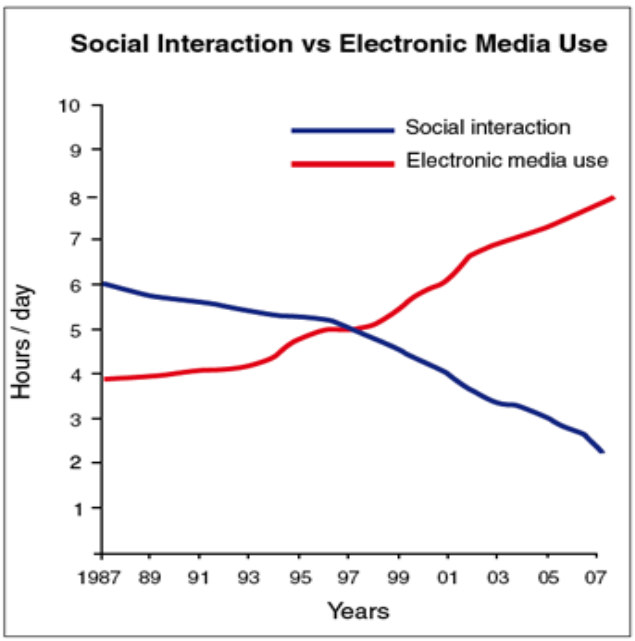

Fig. 3: Graph of social interaction vs. electronic media use

5. SECURITY THREATS IN SNS

These days, the Utilization of SNSs is expanding quickly around the world. SNSs, for example, Facebook, Flickr enables billions of clients to share their own data and sight and sound information with companions, relatives and other online clients. Client's data, including interactive media information, is being caught and unlawfully utilized by malevolent clients and outsider associations for raising their income. There are numerous security dangers in SNSs which put client's shared information at dangers.

5.1. Shared connects to interactive media content

Because of the broad assortment of interactive media positions, for example, JPEG and PNG, it is exceptionally troublesome for one structure to help all organizations. In addition, a considerable lot of these may be powerless to various sorts of assaults, or they may have information that requires manual checking (i.e., intuitive glimmer recordings). More often than not, SNSs don't bolster all sight and sound arrangements and clients can't share a discretionary mixed media record in any configuration.

5.2. Static connections

For the most part, most SNS clients utilize static connects to share sight and sound information, which is on the grounds that these connections give a proficient and ideal route for information to be dispersed. Nonetheless, sharing the static connection can influence the security of clients and make the likelihood for some assaults to happen. At the point when a client shares the static connection of an image with a gathering of chosen clients, each individual from the gathering approaches the image and can share it without the consent of the image's proprietor

5.3. Re-appropriating and straightforwardness of server farms

The straightforwardness of put away media is a noteworthy issue that can influence the security of SNS clients in two different ways. Initially, the multi-media information put away

in an SNS isn't scrambled. Consequently, if a malignant client has an immediate connection to this information, the individual can get to it without experiencing an approval procedure. Second, the information put away in an SNS can be seen by the specialist co-op.

5.4. Phishing

This is the place assailants utilize counterfeit sites and messages to uncover a client's delicate private data. They endeavour to make an indistinguishable bogus duplicate of a unique site. Aggressors can likewise utilize SNSs to complete a phishing assault. For this situation, an assailant first gathers a client's close to home data from SNSs and dependent on this the person sends a phony message, which looks authentic, to the client by means of SNS. This created message can contain an aggressor's requests, for example, the client's charge card number, secret key, and the sky is the limit from there.

5.5. Malware

This is a pernicious program that comprises of Trojan ponies, infections, and worms. For the most part, SNSs work upon the associations of various client's frameworks. Consequently, malware can essentially exchange between various clients' frameworks by means of these associations. Numerous SNSs don't have the best possible component to decide if a URL is vindictive or not.

5.6. Sybil assault and phony profile

With this kind of assault, assailants make a tremendous measure of phony characters that assistance them to accomplish real advantages in the disseminated framework and shared framework. A Sybil assault is a noteworthy issue for SNS security since it contains an extensive number of clients who are associated as friends conveying in a shared system, which implies that one online element can oversee and handle a few phony personalities in an SNS. By working these phony personalities, aggressors can outvote the real clients like Byzantine disappointment resistances.

5.7. Spamming

In a spamming assault, assailants send spontaneous messages (spam) in mass to web clients. This kind of assault gives off an impression of being more fruitful in SNS contrasted with customary spamming assault where email is utilized to spread spam. This is because of the social connections that exist between clients in SNS, which implies that it is anything but difficult to convince the focused on the client to peruse garbage information and trust it to be protected.

5.8. Snap jacking

This is a developing danger to SNSs where aggressors cover up malevolent applications behind the delicate UIs' or catch to take the snaps of clients and utilize them for malignant purposes. Click-jacking has varieties, however, the most prominent are Like-jacking and Cursor-jacking. In Like-jacking, an assailant partners malevolent codes contents with Facebook's "Like" catch, which shows up on the client's profile. Cursor-jacking utilizes the UI changing procedure to adjust the area of the cursor, where the assailant swaps the real cursor with a counterfeit one to divert the client to a pernicious site.

5.9. De-anonymization assault

In a few SNSs, like Facebook and Twitter, clients can shield their secrecy and security by utilizing an assumed name or false name. The de-anonymization assault utilizes diverse techniques, for example, client amasses participation, arrange topology, and following treats, to reveal the client's actual personality. This assault is likewise conceivable in SNSs where an outsider can discover the client's character by connecting the data that the client has unveiled in an SNS.

5.10. Media content dangers

Information sharing is an essential element in SNSs, where clients can share their photographs, recordings, exercises, interests, etc. One of the crucial parts of this sort of information sharing is sight and sound information. Present day SNSs allow their clients to share high-goals recordings and pictures. In any case, the headway in sight and sound recovery methods, for example, area estimation, confront acknowledgement, web looks, and geo-labelling can build the odds of these things being unlawfully used. For example, a mutual picture can uncover a client's area by means of the use of geo-labelling.

5.11. Shared Possession

Shared interactive media information onto SNS may identify with various clients. For example, two companions may snap a picture together at an occasion and both of them could transfer the photograph onto SNS with his or her security settings and without the assent of the other. This may uncover the security of another companion on the grounds that such a photograph has a place with the two companions. Since just a single client can settle on his or her favoured security settings for the mixed media information that has a place with various clients, it could be imparted to the favoured protection settings that are chosen by one of the clients. The favoured protection settings are not chosen by the crossing point of every individual client's security settings, which would be sensible.

5.12. Metadata

This is a kind of information that contains and conveys data about other information. In SNSs, mixed media substance go about as metadata in light of the fact that this substance may contain gigantic measures of other profitable information, for example, IDs and area. While this may be significant for the client, it additionally may open the client to assaults in the event that it is unveiled. One sort of sight and sound metadata that could uncover clients are geo-area labels. A few of the most recent cell phones embed the GPS (Global Positioning System) arranges in the clicked pictures, which reveal the area data of the client.

5.13. Re-appropriating and straightforwardness of server farms

The straightforwardness of put away media is a noteworthy issue that can influence the security of SNS clients in two different ways. In the first place, the multi-media information put away in an SNS isn't scrambled. Accordingly, if a malignant client has an immediate connection to this information, the person can get to it without experiencing an approval procedure. Second, the information put away in an SNS can be seen by the specialist organization.

5.14. Video meeting

These days, numerous SNSs bolster both talk and video conferencing administrations, as video-conferencing can give more between activities between clients. Be that as it may, with this, more data can be revealed. A malevolent client can capture the communicate video stream by abusing the conceivable vulnerabilities in the basic correspondence design

5.15. Unapproved information revelation

Numerous SNSs give an information sharing office to their clients. By and large, information sharing means uncovering the information to a clear an arrangement of clients. At the

point when a client imparts content information to a gathering of clients, it may be that an individual from the gathering uncovers the information. For the most part, this sort of exposure isn't viewed as lawful in light of the fact that it tends to be controlled. Thus, sight and sound information are likewise pliant, when a client imparts an image to a specific gathering of clients, any individual from the gathering can download it and re-transfer with his or her new security settings.

6. INVESTIGATION OF SNS SECURITY SOLUTIONS

In a previous couple of years, SNS security has pulled in the consideration of numerous security analysts in both the business and scholarly fields. An assortment of arrangements has been proposed to manage these previously mentioned security dangers. In this Section, we examine and give a few techniques and methodologies proposed in the writing on SNS security to counter the productive security arrangements and to accomplish dependable, secure, better protection cognizant SNSs biological community.

The rundown all techniques and methodologies are portrayed as underneath:

6.1. Watermarking

Advanced watermarking is a technique for inserting information into media content with the reason for demonstrating responsibility for. Regularly, the watermarking procedure can be imperceptible or unmistakable. Obvious watermarking is typically noticeable content or a logo that unmistakably distinguishes the proprietor and is implanted in the picture. This sort of watermarking will in general cover the greater part of the information and is hard to evacuate. A few SNS, for example, Badoo utilizes unmistakable watermarking. Undetectable watermarking is imperceptible to the human eye and can be hearty, semi-delicate, and delicate. In hearty watermarking, the information can be recouped after a malignant assault or flag handling is completed. Delicate watermarks can't be recuperated or confirmed after normal flag preparing is finished.

6.2. Co-possession

The co-possession demonstrate enables numerous clients to apply their protection settings to co-claimed recordings and pictures. This model has been perceived by many research works. They additionally exhibited a client investigation of this inside Facebook, which demonstrated that clients like the idea of community security the executives and that it is valuable for ensuring the protection of their mutual media information. They proposed a multiparty approval system for Facebook. This system characterizes the intelligent portrayal and assessment of access control approaches. Legitimate portrayal oversees strategy clashes by making a harmony between two parameters. One is the necessity for security assurance and the other is the client's longing to share information.

6.3. Steganalysis

SNSs enable clients to transfer vast and high goals sight and sound information. Be that as it may, suspicious clients can utilize this information as cover items to spread malignant data. Thusly, it is viewed as basic to utilize steganalysis programming or systems to discover this data inside interactive media information. Be that as it may, numerous SNSs don't utilize these sorts of instruments or commonly yield of such systems isn't informed to the clients. Numerous conventional steganalysis instruments have been proposed to recognize noxious pictures. These systems depend on regulated machine learning strategies in which an expansive dataset of pictures is aggregated to prepare a general model, and after that these photos can be arranged by utilizing the prepared model.

6.4. Advanced insensibility

This is where a lapse time is set on computerized information with the goal that nobody can get to the information after it has terminated. These days, clients distribute an ever increasing number of private information on SNSs and, accordingly, the information stockpiling limit of SNSs is expanding step by step. In this way, computerized obscurity can be utilized to secure the protection of a lot of information. A few arrangements have been proposed to give advanced insensibility in SNSs.

6.5. Capacity encryption

Numerous SNSs don't have their own server farms and them for the most part store the client's information in outsider server farms. These focuses can impart this information to other information wholesalers or numerous political and geospatial occasions may uncover the client's information to different associations without their consent or advising them. This issue is exceptionally basic in light of the fact that numerous restorative and wellbeing SNSs exist. Clients share a ton of touchy data on these SNSs and if this data is uncovered it can affect clients both rationally and monetarily

6.6. Metadata expulsion and security

Numerous methodologies exist for expelling metadata and alleviating the spilling of metadata security in SNSs. This strategy encodes media metadata and stores it in the sight and sound record.

7. CONCLUSION AND FUTURE DIRECTION

SNSs have turned into a coveted vehicle of correspondence for billions of web clients, in that capacity administrations enable individuals to share their interests, photographs, recordings, and draw in with companions without land and monetary constraints. Notwithstanding, these ser-indecencies can open clients to genuine digital security dangers. In this paper, we gave a best in class examine on a few sorts of protection and security issues in SNSs that emerge from a portion of their critical highlights, for example, sharing pictures, remarking, labelling, and blogging. To comprehend the issues, we outlined different late assault measurements and security reports that have been discharged by a few security associations and web journals. Moreover, we tended to the security province of SNSs by depicting three classes of dangers: Multimedia content dangers, Traditional dangers, and Social dangers. In this way, we directed an investigation of the conceivable and existing plans for ensuring SNS clients against these dangers. We additionally com-pared different SNS security assaults dependent on specific parameters and talked about some open research difficulties and future bearing. At long last, we introduced some simple to-apply reaction procedures that can be effortlessly trailed by SNS clients to all the more likely ensure themselves against different security dangers.

As we have just talked about, various security and protection dangers can put SNS clients in danger. There are numerous investigates that exhibited their own answers to secure clients against these dangers. Be that as it may, these inquire about still need to give reasonable subjective and quantitative examination of SNS security. With respect to essential attributes of late SNS and constraints in past examines, in this segment, we present a novel research course, which underscores on the most proficient method to gauge and streamline the security of SNS to accomplish the objective of building a reliable, effective, and secure SNS biological community.

8. REFERENCES

[1] A. Aggarwal, A. Rajadesingan, P. Kumaraguru, Phish Ari: automatic realtime phishing detection on Twitter, in eCrime Researchers Summit (eCrime), IEEE, 2012, pp. 1–12.

[2] A. Barinka, Bad Day for Newsweek, Delta Amid Social-Media Hackings, https://www.bloomberg.com

[3] A.C. Squicciarini, H. Xu, X.L. Zhang, CoPE: enabling collaborative privacy management in online social networks, J. Am. Soc. Inf. Sci. Technol. 62 (3) (2011) 521–534.

[4] A.C. Squicciarini, M. Shehab, J. Wede, Privacy policies for shared content in social network sites, VLDB J. 19 (6) (2010) 777–796.

[5] A. El Asam, M. Samara, Cyberbullying and the law: A review of psychological and legal challenges, Comput. Hum. Behav. 65 (2016) 127–141.

[6] A. Hai Wang, Don't follow me: spam detection in twitter, in Proceedings of the International Conference on Security and Cryptography (SECRYPT), IEEE, 2010, pp. 1–10.

[7] A. Kamilaris, G. Taliadoros, A. Pitsillides, D. Papadiomidous, The practice of online social networking of the physical world, Int. J. Space-Based Situated Comput. 2 (4) (2012) 240–252.

[8] A.M. Alattar, N.D. Memon, C.D. Heitzenrater, Media Watermarking, Security, and Forensics, Spie Press, 2015.

[9] A. Mendelson, Does social media distort reality? http://www.scoop.it

[10] A. Mislove, B. Viswanath, K.P. Gummadi, P. Druschel, You are who you know: inferring user profiles in online social networks, in Proceedings of the Third ACM International Conference on Web Search and Data Mining, 2010, pp. 251–260.

[11] A.P. Schepis, A. Caola, Techniques for multimedia metadata security, U.S. Patent No. 9,268,964, 2016.

[12] A. Viejo, J. Castella-Roca, G. Rufián, Preserving the user's privacy in social networking sites, in Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, Berlin Heidelberg, Springer, 2013, pp. 62–73.

[13] A. Zigomitros, A. Papageorgiou, C. Patsakis, Social network content management through watermarking, in Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012, pp. 1381–1386.

[14] B. Greschbach, G. Kreitz, S. Buchegger, The devil is in the metadata—new privacy challenges in decentralised online social networks, in Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE, 2012, pp. 333–339.

[15] B. Sams, Facebook photo exploit allows you to view any albums of non-friends, https://www.neowin.net

[16] CareerBuilder, Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade, http://www. careerbuilder.com

[17] Check Point Software, SocialGuard Privacy Scan, https://www.facebook.com

[18] C. Ho Sin, N.A. Kim, B.W. Go, K.S. Min, J.D. Lee, J.H. Park, Realizing the right to be forgotten in an SNS environment, in: H. Jeong, M.S. Obaidat, N. Yen, J. Park (Eds.), Advances in Computer Science and Its Applications, Lecture Notes in Electrical Engineering, 279, Springer, Berlin, Heidelberg, 2014, pp. 1443–1449.

[19] C. Patsakis, A. Zigomitros, A. Papageorgiou, E. Galván-López, Distributing privacy policies over multimedia content across multiple online social net- works, Comput. Netw. 75 (2014) 531–543.

[20] D.H. Lee, Personalizing information using users' online social networks: a case study of CiteULike, J. Inf. Process. Syst. 11 (1) (2015) 1–21.

[21] D.V. Medhane, A.K. Sangaiah, ESCAPE effective scalable clustering approach for parallel execution of continuous position-based queries in position monitoring applications, IEEE Trans. Sustain. Comput. (2017) 1–13, doi: 10.1109/TSUSC.2017.2690378.

[22] D. Wang, N. Wang, P. Wang, S. Qing, Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity, Inf. Sci. 321 (2015) 162–178.

[23] [23] E. Novak, Q. Li, in A Survey of Security and Privacy in Online Social Networks, College of William and Mary Computer Science, 2012, pp. 1–32. Technical Report.

[24] Facebook, How to Report Things, www.facebook.com

[25] F. Ahmed, M. Abulaish, A generic statistical approach for spam detection in Online Social Networks, Comput. Commun. 36 (10) (2013) 1120–1129.

[26] F. Li, K. Wu, J. Lei, M. Wen, Z. Bi, C. Gu, Steganalysis over large-scale social networks with high-order joint features and clustering ensembles, IEEE Trans. Inf. Forensic Secure. 11 (2) (2016) 344–357.

