Social Network and Security Issues: Mitigating Threat through Reliable Security Model

A. A. Obiniyi
Department of Mathematics
Ahmadu Bello University
Zaria, Nigeria

O. N. Oyelade
Department of Mathematics
Ahmadu Bello University
Zaria, Nigeria

P. Obiniyi
Omicroservices Inc
Washington DC Metro Area
USA

ABSTRACT
Social network sites have become de factor in establishing and maintaining good relationships across different continents and countries. Associations or connectivity has proven beneficial to people who share same interests professionally, research wise, in casual social connectivity, and companies have employed the social network in advancing their marketing strategies and it which have proven profitable. However, like other web applications that attract a great influx of visitors, the security of personal information of users in social network sites had suffered different security threats. This paper focuses on highlighting social network users on some security issues that are peculiar with social network. It proposes an algorithm and a model to circumventing security threats which are categorized into user authentication, data confidentiality and integrity.

Keywords: Social Network Sites (SNS), Security,

1. INTRODUCTION
Social networking sites (SNS) are a type of Web 2.0 sites that enables users to create online accounts that capsules their profiles. They are a group of websites that provide people with the opportunity to create an online profile and to share that profile with others (Timm *et al.*, 2008). It can also be defined as web-based services that allow individuals to; construct either a public or semi-public profile within a bounded system, articulate a list of other users in the system whom they share connection, and view or traverse the list of connections and those made by others in the system (Boyd *et al.*, 2008). Some popular SNSs are Facebook, Twitter, MySpace and LinkedIn. Social Networking Sites have provides users with platform for establishing and maintaining relationships from different points of life. Most of these SNSs are specialized and dedicated to particular fields of life which includes academies, research, religious, workforce, and social platforms. Almost every person who is computer literate is on one social network or the other. In fact, the advances made in mobile devices technology are gradually enlarging the influx of users onto most of the available social networks.

SNS combines different functionalities that glue their users to them for a long time. Companies and institutions are now seeking to coin out policies that will be employ in controlling their workers and students respectively in the amount of time they spend on the Internet. Due to the long list of connections a user may have on his SNS, they may have several persons to view their profiles, posts, or comments, thereby making the art of using this websites time consuming. However, the sites have provided its users with quite a lot of benefits, which have made SNS to enjoy wide usage. Facts have proven that most of the users of such sites post risky information online not aware of the security and privacy issues tied to it (Kumar *et al.*, 2013). SNS users have always been deluded by the transparent anonymity they enjoy on their desired social network. However, some of the security issues that is discussed in this paper reveal that nothing contained in a user profile is secured. Cooperate organizations have also embraced the use of social networks in advancing the interest of their company. Survey on companies that use social networks reveals that 70 percent of the respondents attest to the fact that they use SNS in their business and over 40 percent of such companies have employees whose job function included spending time on social networking sites in order to maintain an organization presence (Chi *et al.*, 2011). Of the Fortune Global 100 companies, 65 percent have active Twitter accounts, 54 percent have Facebook fan pages, 50 percent have YouTube video channels, and 33 percent have cooperate blogs (ISACA, 2010). Social media poses some security challenges to organizations. Some of these security issues include contention on limited network bandwidth by employees using it for SNS purposes and other employees using it for business reasons, malware attack, and inadvertent divulging of sensitive information.

Based on the security threats that confronts users of social networking sites, though they had provided users with enormous benefits, this paper concentrates on tackling some of the major security issues that may not lie on the side of the user to combat or mitigate them. These security solutions are deployed in ensuring user authentication, sustaining confidentiality and integrity of information in SNS.

2. AN OVERVIEW OF SOME SOCIAL NETWORKING SITES
Web 2.0 comprises of social networking sites. And these social media includes, though not limited to, Facebook, MySpace, LinkedIn, Twitter, YouTube, Google+, Flickr, Bing, Ning, Skype, MyChurch, CyWorld, Skyblog and others. Some of the functionalities that are typically provided their users for the purpose of interaction or data communication are chat, messaging, email, video, voice chat, file sharing, blogging and discussion groups (Sharma, 2012). They attracts users based on the nature of the service been rendered by their sites. Facebook has three most popular features of Facebook are ability to add friends, update status and run applications such as games (Dinerman, 2011).

Facebook is a social media with highest level of registered users. It boast of over 1.15 billion registered users with about 751 million accessing their account from mobile devices. Already, since most of the social media provides developers with API for connectivity, there are already over 10 million Facebook apps. Most of these registered users of Facebook check their account at least five times daily, and they make up about 21% of the total users. 350 pictures are uploaded daily.

74% of marketers believe Facebook have profited their lead generation strategy (Bernstein, 2013). Twitter is another social media that is seen as a micro blogging site. The fastest growing demographic on Twitter is the 55-64 year age bracket and this has grown since 2012. While 45-54 year age bracket is the demographic on Facebook and Google+ (Cooper, 2013). Active users on Twitter are averaged to be over 288 million. Over 400 million tweets are been sent per day with an average of 208 tweets per account and 28% of retweets by users is as a result of an inclusion of 'please RT'. Like Facebook, 60% of Twitter's users access their account from their mobile devices, though it was also observed that around 20 million users account on Twitter are fake (Bernstein, 2013).

LinkedIn when compared with Facebook, Twitter, Google+ and Pinterest, has lower percentage of users and every second 2 new members join LinkedIn, it further reveals that it is growing at over 30% (Bullas, 2013). The total number of Linked groups is 1.5 million and 27% of the users access it using different mobile devices. 50% of the users on LinkedIn have their Bachelor's or graduate degree and 42% update their profile regularly. Since business outfits have taken advantage of social media, survey reveals that over 3 million LinkedIn company pages already exists while there are 1 billion LinkedIn endorsements (Bernstein, 2013).

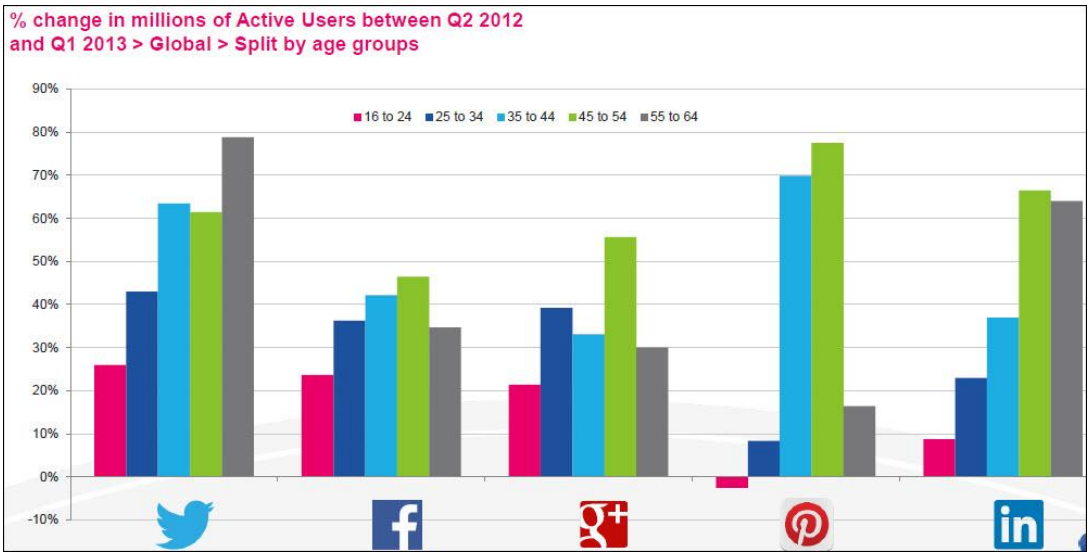

Figure 1: Demographic distribution of social media users (Source: Bullas, 2013)

YouTube is another video sharing social media that have gained a very wide range of acceptability with over 1 billion unique visitor on a monthly basis. YouTube reaches more U.S youth in the age range of 18-34 than any cable network. Google+ is a Google proprietary social media that is integrated with the Google search engine. Google's Gmail account holders are been coerced into owning this account at the point of registration for an email account. Google+ has over 500 million users with about 343 million of them as active users. Survey shows that more female users are actively using their Facebook account than their male counterpart. However, in Google+, male constitutes 67% of the users. Demographic statics of social media may open up great insight to researchers who are studying user's acceptability of social media based on gender. Hence, Figure 1 shows a demographic distribution of users of some of the popular social media discussed in this paper. In Google+, animated Gif are still the most uploaded post. 80% of users on Google+ login to it at least once in a week while 60% are approximated to login daily. Marketers are not also resting their hoarse as far as Google+ is concerned. This is why 40% of marketer's use Google+, 70% desires to learn more and 67% plans to increase Google+ activities (Bernstein, 2013).

3. RELATED WORKS

A great number of the security threats mitigating the efficiency of SNS can be categorized into three groups; confidentiality of data, integrity of data and availability of service. And in the next section, some of these security threats shall be elaborated upon. When the security of SNS is confronted from the understanding of these categories, then tackling such threats become narrowed down to these three categories. Analytic Hierarchy Process (AHP) has been applied in mitigating SNS security challenges. AHP is a proposed process for reducing complex tasks, assign relative ratings to them and analyze the results of the outcome. AHP was proposed by Saaty (2008) and was employed by Kim (2012) by applying AHP to SNS. In identifying the security challenges confronting the social media trust zones, Kim used some criteria for simplifying the evaluation process. And these criteria are the strong elements of all three aspects of security. The result of the evaluation shows that under confidentiality, a major security leakage has to with data interception through unauthorized users. While under integrity criteria, security threats consist of data damage, data falsification, software bugs and unauthorized access. The last evaluation criteria, availability, includes the following security bridges; loss of communication, system damage and disruption. After deriving all the security threats, proposed solution for tackling each of them listed security threats above were further provided.

Companies have suffered loss in aspects such as financial, information leakage, and network resource wastage. Dinerman (2011) highlighted that individuals and companies must be attentive to the information they post or tweets on social media. He suggested that employee may pose serious public relation and financial consequences, there demanding that policies be forged to curtail such leakages. He further pointed out that users of social media and online banking or day-to-day purchase of goods online must be aware of email that claims to be sent from this SNS but is just but hoax which may contain malicious content. Suggestions raised in this work are the use of software for identifying legitimate

messages from the hoaxes. Some of the software are up-to-date email client such as Microsoft Outlook, up-to-date antivirus/anti-malware, and been sensitive by using common sense in clicking links online. One non-technical company based social media threat was outlined in ISACA (2010). Some of them include excessive employee use of SNS during working hours and the upload of images or pictures, information, or posts that reveals cogent organizational business strategies. This portends considerable loss to the enterprise when criminals have access to them. The research work proposed provision of content filtering mechanism or limit network bandwidth on social media, while the HR department also works out policy to mitigate such security loop holes.

4. SOME SECURITY ISSUES IN SOCIAL NETWORK

Social media had been compromised from the security perspectives thereby posing great threat to users with respect to their personal, intellectual, career property. This section seeks to outline the security issues that are prone to social media and it users. These security threats ranges from privacy setting threats, identity related attack, social attack, anonymity attack and information leakage attack. Though some of these threats can be combed by simply enlightening the users on the potential threats. For instance, a survey reveals that 25% of Facebook users don't bother with privacy settings (Bullas, 2014).

4.1 Malware

Malware stems from malicious and software. They are comprises of viruses, Trojans and worms. Survey shows that 36% of companies have had their systems infected with malware through social media 2009 while it has risen to 70% in 2010 (Vanheuangdy *et al*, 2010). Some common malware are Koobface and Twitter Worm. Koobface is a worm that spread across social media like Facebook. This type of worm is spread through the messages that users send to their friends; this messages could be in the form of video. When the friend receives such message with an attached link for the video, the user after clicking that link may be required to download or update the Flash Player, on accepting to download the Flash Player the user's computer will be filled with worms that can damage the computer system (Gunatilaka, 2011). Twitter Worm is another attack common with users of Twitter site. One of these worms is Profile Spy worm, which allows attacker to tweet link for downloading third party application call Profile Spy, then when user want to download the app, it will prompt a form to collect user personal details, and with these details, it will keep tweeting malicious messages to the followers of the Twitter user. Another worm known with Twitter is a worm that creates a fake invitation link which directs users to a malicious attachment containing email addresses from compromised computers and spreads by coping it onto removable drives and folders (Qing, 2014).

4.2 Digital Dossier of Personal Information

In this scenario, an attacker gathers profile information of targeted victims on storage space and thereafter uses it for injurious purposes on the victim's personality. Since most of the social media sites provide search for user's profile, the attacker can mine out the prospective victim into his storage system and then use it to damage the image of the profile holder (Al Hasib, 2008).

4.3 Spam

Spams are unwanted or unsolicited messages sent to online email or social media account holders. Most often, such messages are malicious, though some have sought to use it as advertisement strategy. The use of spam dates back to when communication networks came into use on the Internet, and they have grown with the advances in the communication networks, not to enhance it but as a circumvent the well-intended communication of the legal account owners. Survey have shown that in the first half of 2013, the growth of social spam media have risen to 35% just on typical account, pointing out that one of seven social posts contain spam (Nguyen, 2014). Really, social spam are been propel using different medium. These include text-based, image or picture based and URL based. The URL based social spam usually omits the text, leaving only the link for the user to view-thereby dousing the alertness of the unsuspecting victim. Image based social spams comes as attractive images or advertisements with the potency of luring the social network users to click it. This usually leads the user to other online computers that download Trojans into the computer. The text based social spam is sent with phishing in mind. The security measure to be imbibed in this case is to use available message filtering functionalities that are been provided by the SNS that the user have created account with. Moreover, their third party applications that detect major social network security threat like spam.

4.4 Cross-Site Request Forgery and Cross Site Scripting

This attack occurs when a malicious website, email, blog or program, opened on a user computer, uses the user's browser to initiate connectivity to another website, and then uses login details (submitted to a website that the legal user may have currently connected), of the unsuspecting user to carry out malicious attack on the website it has connected. An example of cross-site request forgery may be achieved using RESTful API. RESTful API has been employed in realizing interactivity between applications and social networks. Social network sites have provided APIs for such apps to retrieve user information. Mashup application like HootSuite was used to access more than needed data from Facebook. When HootSuite was authorized to connect to Facebook, it was able to access basic information such as profile information, relationship and family information, friend list and others (Zhang *et al.*, 2013).

4.5 SQL Injections

Web application developers have had their database attacked by attackers through the use of SQL injection. SQL injection is a technical approach used by attackers to gain access to database. Mitigating this attack is mostly left to the developers of the social network so that profile information of users of such social network will be secured. Hackers are able to execute malicious SQL query against underlying databases of vulnerable social network apps. A report by Slow PC (2014) revealed that Facebook and Twitter were the sites that have suffered maximum SQL attacks compared to government websites.

4.6 Identity Theft

Identity theft in social network has become in rampant in popular social networks. The social network juggernaut, Facebook, users have continuously suffered this attack. Mali (2014) stated that 12 million people became victims of identity theft and fraud in 2012, and the financial loss of this attack was pegged at $21 billion. Identity theft occurs when

attackers steal other users identifying data such as profile picture, date and place of birth, and then use it to create another account. Such account is mostly used for fraudulent purposes.

4.7 Phishing

Phishing in a sense is a tricking of online users to give out some details such as password, to an illegitimate website. A report by the Symantec Cooperation on internet security threat pointed out that there was a drop in the phishing attack experienced generally by email users from one in 299 emails in 2011 to one in 414 emails in 2012. The observation was that decline in such threats does not indicate recline by the attackers but rather, a redirection of attack unto the social media. Wood (2013) had enumerated some precautions that social network user must take to avoid been attack by phishers. The social network address must be checked for to ensure it is not a typo squatting site which is usually used to capture users credential. Furthermore, users are to look out for the social websites' certificate for scrutiny to ensure logging details are not divulged into the hands of scammers. Though users are continuously been encouraged to use security software, they must as well learn to use different passwords across different online accounts without bowing to prompts requesting for password saving by the browser.

4.8 Mobile Phone Attack

By the end of 2014, the number of cellular subscribers will have almost matched the number of people on earth, corresponding to a penetrating 96%, ICT Facts and Figures (ITU).

4.9 Stalking and Cooperate Espionage

Information leakage cost such organizations great loss either on financial terms or reputation ground. Social networks continue to serve as platform to engage employees in unconsciously divulging sensitive company data. Some of this information are released to social network without knowing that they can be use more than they intended. For example, Scott McClellan, Hewlett-Packard vice president on cloud services, once slip up on his LinkedIn profile, when he gave out detail plan of HP's cloud computing platform. However, before he could delete the secret from his LinkedIn page, the news media got wind of it, and this led Microsoft and Amazon to have a peep into HP's plan in this respect (Hill, 2011).

4.10 De-Anonymization Attack

Anonymization in social network allows users to hide information that can make them known. Such information could include their names, pictures, address and other sensitive data. The reason for this anonymity is to ensure user is protected from advertisers, application developers and data mining researchers who will infringe on users privacy. However, there have been some researches that have proven that this de-anonymization of online social network users is possible. Wondracek *et al.,* (2010) indicated the use of public records such as marriage and birth data to de-anonymize an online user and even the membership group the user belongs to on the social network. Furthermore, paper revealed that a combination of information can be generated from some social networks about an individual as a basis for de-anonymizing the user. Hence, de-anonymization attack has become another attacker on social network used by attackers in bypassing user's privacy settings.

4.11 Awareness

There are general and personal security measures that a user's must take, though this is only dependent on the awareness a user have access to. Most social networks sites have their security settings information that prospective users are supposed to read. As a user, it is important you run through them and secure the best setting that will provide you with required privacy. Setting hard to guess password is also a good security measure on the side of the user. When browsing social network sites, what the users sees and contribute or share may be a loophole through which an attacker can gain entrance to attack. For what you view, always be wary of fancy story, images and URLs. Consider the benefit versus the danger of clicking links, images or text you do not trust. As for what we share, here is a piece of advice "Is the information I'm about to share really worth sharing? Will I be okay if future employers, family members, and friends see it? What if total strangers see it? If any of the questions evoke a "No," you may want to rethink your update." TrendMicro (2012).

5. PROPOSED SECURITY ENFORCING ALGORITHM AND MODEL FOR SOCIAL NETWORKING SITE

In this section, we shall develop some security schemes for mitigating a predominant security breaches associated with social networks. Majorly, the approach in tackling this security palaver can be categorized into three: information/data confidentiality, integrity and authentication. Confidentiality is the assurance to an entity (data or information) that no one can read or access it except by a recipient that is explicitly stated by the sender. Integrity of an entity (data or information) entails that there is assurance to such entity that no alteration has been carried out on it either intentionally or unintentionally. And lastly, authentication is an assurance to an entity (system, data or information) that another entity (which can be a user, agent or accessor) is who its claims to be. Cryptography plays a major role ensuring confidentiality and integrity of data. Hence, in this paper, leverage on it.

5.1 Authentication

In this subsection, an algorithm for authenticating account owners of a social website as proposed. Here, the research is based on behavioral profile. This implies that there is a need to keep a log of user's interactivity at every login session. The logs file monitors certain parameters that constitute the behavior of the user. These parameters are tied to the thematic, spatial, and temporal and mode of session login of a user. The thematic parameter gathers information relating to the typing skill and the kind of information shared for each time user logs in. The spatial and temporal parameters capture the location and time of session login respectively. And lastly, the mode of session login checks the frequent device type and IP address user's login from.

Some notations used in realizing this algorithm are hereby defined. First, a set of G collects the returned values of functions ƿ (denotes user typing and discussion pattern over a period of time), the spatial parameter ɭ (denotes common location from which user logs into the site), and the mode of entry parameter ɱ (device type user used in login) and lastly temporal parameter t' is also defined. Algorithm 1 illustrates our proposed secure authentication scheme in a SNS.

First ensure user login details are correct. This is achieved by comparing a hashed password in the database, with hashed value the user is using to access its account now. When they are equal, then the user is partly authenticated; else, the first authentication step fails. For example ILoveZaria in MD5 is `97ded75d8a1ce26174a7934316a71e83` while ILiveZaria in this same hashing function is `d61edb43c864bad88fc17bb410d96440`. So, if the comparison is not same, deny user access. If the first authentication steps succeed, then go further to test the four parameters discussed in this section.

Algorithm 1: Authenticating Users

Note: G ={ p, ɱ, ļ , t'}

1 Let *p* be user password for session login

2 and *P* be user's real password in DB

HASHfunc(*P*)=HASHfunc(*p*) then step 3 else go to step ERROR.

3. read G between a given period Z

- g(ɱ) is equivalent to all ɱ in G.

  let μ =ɱ for this session

  if pattern(μ, g(ɱ), threshold(ɱ)) **then**

  i. improve learning on ɱ
  ii. log μ

  else go to step ERROR.

- g(p) is equivalent to all p in G.
  generate typechar

if equal(typechar, user(typechar)) and test_behavoir() **then**

i. continue

else go to step ERROR.

- g(ļ) is equivalent to all ļ in G.

  let ή = ļ for this session

  if pattern(ή, g(ļ), threshold(ļ)) **then**

  ii. improve learning on ļ
  iii. log ή

  else go to step ERROR.

- g(t') is equivalent to all t' in G.

  let α = t' for this session

  if pattern(α, g(t'), threshold(t')) **then**

  i. improve learning on t'
  ii. log α

  else go to step ERROR.

4. let t_{begin}=now() be time at this time.

5. login user, go to step 7

6. ERROR: Wrong user.

7 **if** use logs out **then**

let t_{end}=now() be time at this time.

save in DB G[$t_{end} - t_{begin}$]={ μ , ή , α, Ɛ}

close session.

else

while user in session

Ɛ+= post_type and typing_pattern

end while

5.2 Confidential and Integrity of User Post

A model is developed to show a security measure to ensure information confidentiality and integrity between users of a social network. The encryption algorithm employs the use of symmetric and asymmetric-like algorithms for encoding the plain text into cypher text. First, the Message Authentication Code (MAC) algorithm is used for the initial encryption of the user post. Though MAC uses same key for encrypting and decrypting of the data, however, the key sameness property was modified by proposing the use of public and private keys in place of the same key MAC uses. For example, if user A sets a privacy setting that allows users B to be able to see certain posts on his (user A) profile, then whenever user A sends a post to user B (or those in that category), user A's private key would be used alongside the MAC function to encrypt the post. The output of MAC's encryption becomes an input into 3DES symmetric algorithm. When user B receives the post, first, the post is sent into 3DES for the initial phase of decryption. The result of 3DES's function will be sent as input into MAC. Then, user B uses user A's public key in the MAC function to decrypts post into the actual plain post sent by user A.

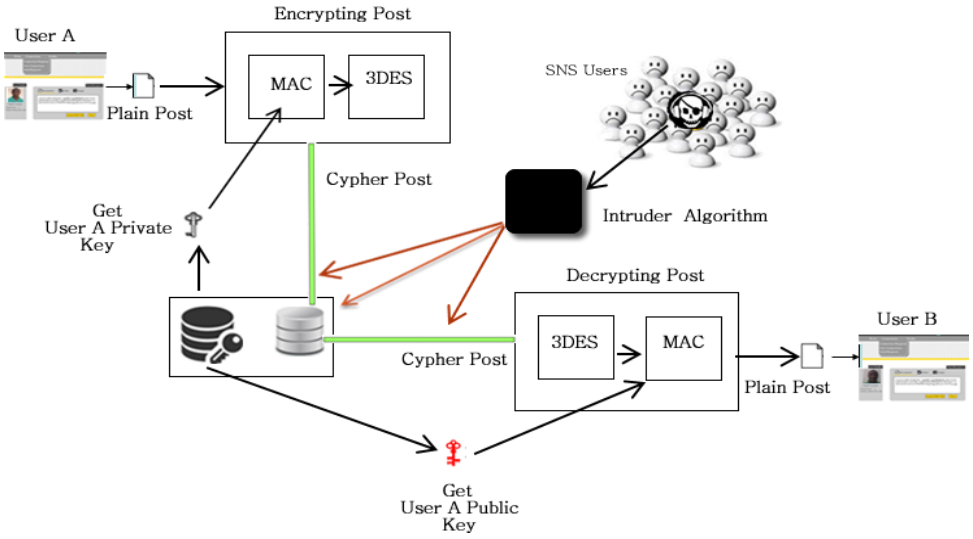

Figure 1: User-to-User Encrypted post model

The use of MAC is proposed because of its reputation of being capable of ensuring data integrity and message origin authentication service, and it is practically infeasible to produce a correct MAC for a message without the knowledge of the needed key for decrypting the cipher test. (Buttyán *et al.*, 2007). Furthermore, MAC is easy to compute and has computation resistance: this implies that the key is non-recovery and though the reverse is not true.

6. RESULTS AND DISCUSSION

In this paper, some security challenges in SNS were mitigated. Majorly, some security weaknesses encountered in SNS are centered on user authentication, data confidentiality, integrity and non-repudiation. Hence, Algorithm 1 technically circumvents an attacker's moves to gain access into user profiles. Here, the use of user's behavioral profile and a hash function to frustrate an attacker's illegal intrusion are employed

Furthermore, the use of a cryptographic model shown in Figure 1 was also used to curtail illegal access or manipulation of user's post. This tackles confidentiality and integrity of data. Two algorithms were considered in a bid to greatly reduce, and most possibly completely eliminate, compromising user's privacy settings that were targeted at keeping information secret between users.

7. CONCLUSION

Social networking sites are becoming very useful among people of different fields and profession. College and higher institution students have taken to popular social network sites as a means of socializing and making new friends. Businesses organizations have are also leveraging on the social network in promoting business interest and cooperate image. Hence, this paper first identified some major social network sites and their pros and cons. Major security pitfalls that are rampant in most of these social networks were discussed. Finally, two approaches in mitigating a few of the loop holes observed with social network sites were proposed. More so, it was noted that users of social network are at a more advantage position to personal curtailing some security breaches that may be lunched against them. For example, a user who carelessly posts very confidential information to the public is a costly security let down. Harmonizing the contribution demonstrated by Algorithm 1 and the model in Figure 1 will go a long way in mitigating security breaches with users of SNS.

8. REFERENCES

[1] Al Hasib, A., (2008). Threats of Online Social Networks, *International Journal of Computer Science and Network Security* (IJCSNS), Vol.9 No.11, 288-293.

[2] Boyd, M. D. and Ellison, B. N., (2008). *Social Network Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication, Vol. 13, No. 1, pp.210-230.

[3] Bernstein, J. *http://socialmediatoday.com/jonathan-bernstein/1894441/social-media-stats-facts-2013*. Retrieved on 9th June 2014.

[4] Bullas, J. (2013). *http://www.jeffbullas.com/2013/07/04/5-insights-into-the-latest-social-media-facts-figures-and-statistics/* Retrieved on June 9, 2014.

[5] Buttyán, L., and Hubaux, J (2007). Introduction to Cryptographic Algorithms and Protocols, http://secowinet.epfl.ch/ Retrieved on 2nd August 2014.

[6] Chi, M. and Wanner, R., (2011). *Security Policy and Social Media Use*, SANS Institute InfoSec Reading Room. Retrieved from www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-mediaorganization-33749 on August 9 2014.

[7] Cooper, B. B. (2013). Retrieved from *www.huffingtonpost.com/belle-beth-cooper/10-surprising-social-medi_b_4325088.html* on June 9, 2014.

[8] Dinerman, B., (2011): *Social Networking and Security Risks*, http://www.fieldbrook.net/TechTips/Security/SocialNetworking.asp Retrieved on August 9, 2014.

[9] ISACA (2010). Social Media: Business Benefits and security, Governance and Assurance Perpectives, Available at http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Social-

Media-Business-Benefits-and-Security-Governance-and-Assurance-Perspectives.aspx

[10] Gunatilaka, D., (2011). A survey of privacy and security issues in social networks, Retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.html on August 9 2014

[11] Wondracek , G., Holz, T., Kirda, E., Kruegel, C. (2010). A Practical Attack to De-Anonymize Social Network Users, Security and Privacy, SP 2010 Proceedings of the IEEE Symposium on Security and Privacy, pp. 223-238.

[12] Hill, K. (2011). The Spy Who Liked Me. Retrieved from http://www.forbes.com/sites/kashmirhill/2011/11/02/the-spy-who-liked-me/ on 28 July 2014.

[13] Kim, H. J., (2012). Online Social Media Networking and Accessing its Security Risks, International Journal of Security and Its Application, Vol. 6 No. 3, pp. 15-16.

[14] Kumar, A., Gupta, K. S., Rai, K. A. and Sinha, S. (2013). Social Networking Sites and their Security Issues, International Journal of Scientific and Research Publications, Vol. 3, No. 4, pp. 1-5.

[15] Saaty T., (2008). Decision making with the analytical hierarchy process, International Journal of Services Sciences, vol. 1, no. 1, pp. 83-98.

[16] Sharma, R., (2012): Analyzing the Role of Semantic web in Social Networking Sites, International Journal of Scientific Engineering Technology, Vol. 1 No. 3, pp. 125-131.

[17] Timm, M. D. and Duven, J. C. (2008). Privacy and Social Networking Sites, Available at www.interscience.wiley.com published online by Wiley InterScience,.

[18] Vanheuangdy, V. (2010). Security Threats of Web 2.0 and Social Networking Sites, Retreived from http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Security%20Threats%20of%20Web%202%20and%20SNS%20V%20Vanheuangdy.pdf on August 9 2014.

[19] Qing, Liau Yun. Top 5 Social Networking Business Threats - Security - News. ZDNet Asia. Retrieved August 9 2014, from. http://www.zdnetasia.com/top-5-social-networking-business-threats-62060912.htm.

[20] Nguyen, H., (2013). Research Report 2013 State of Social Media Spam, NextGate Publication, San Francisco. Retreived from http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf on August 9 2014.

[21] Mali J. Retrieved from http://www.lifehack.org/articles/technology/identity-theft-through-social- networking-lessons-take-now.html on 28 July, 2014.

[22] Slow PC. Retrieved from http://www.spamfighter.com/News-13034-Hackers-Prefer-SQL-Injection-Attack-Social-Networks-Websites.htm on 28 July, 2014.

[23] TrendMicro (2012). A Guide to Threats on Social Media, Trend Micro Incorporated, Internet Security Threat Report 2013**.** Symantec Cooperation Volume 18, pp. 45. http://www.trendmicro.com/us/security-intelligence/research-and-analysis/threat-reports/

[24] Wood, P. Phishing on Social Networks: What's the value of your small biz Twitter account? Looked up July 12, 2014. http://www.symantec.com/connect/blogs/phishing-social-networks-what-s-value-your-small-biz-twitter-account

[25] Wondracek G., Holz, T. ; Kirda, E. ; Kruegel, C. (2010). Published in: Security and Privacy (SP), 2010 IEEE Symposium Conference, pp. 223 – 238.

[26] ICT Facts and Figures, ITU, the world in 2014. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf on August 9, 2014.

[27] Zhang, Y., Wang, X., Luo, Q., and Liu, Q (2013). Cross-Site Scripting Attacks in Social Network APIs. Retrieved from *www.w2spconf.com/2013/papers/s3p1.pdf* on July 28, 2014.