Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition

L.S.Y. Dehigaspege, U.A.A.S. Hamy, H.A.H. Shehan, S.A. Dissanayake, H.P. Dangalla, W.H.I. Wijewantha and Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Abstract- Advance development of technology internet plays an important role. When pointing out internet social networking is an essential thing to people, the usage of social networking sites is dramatically high compared to other websites. Reason behind this is people who lives in 21st century has been addicted to social networking sites to keep connection with others. Social networking sites are not only to communicate or interact with each other currently it is used as a way of business promotion. Due to tremendous growth of social networking sites it also under arrested to cyber-attacks. This issue has led even with data sharing process, this raise number of cyber issues on security and privacy through social networking sites. Since people are connected to social networking sites with their own devices they have been caught to various threats. A cyber threat can be o f various ways it can be intentional or unintentional, targeted or non-targeted it can be occurred in many ways may be from an information warfare, criminals, hackers etc. Existing systems such as antivirus systems, internet security systems are just not enough to protect the threats that occur to the social networking sites. Introducing an effective and highly advance cyber security system has become essential. This paper aims to provide a highly secured way to access social networking sites. The proposed framework is based on an algorithm which includes a voice recognition system which logs the user to their private account by tracking their voice as a login method along with that the algorithm includes a location identification system. Moreover, the concept CAPTCHA's program to distinguish the bots from human users has been included to the proposed algorithm. The purpose of this study is to introduce a disenchanting cyber-attack defense system which involves an algorithm by including above mentioned aspects.

Index Terms- Social networking, cyber-attacks, algorithm, voice recognition, location identification, CAPTCHA's.

I. INTRODUCTION

Online social networking sites now have been developed rapidly all among the world it is now been used by hundreds of millions of people daily to keep contact with each other. However, through social networking sites people post their daily routines, real life connections, backgrounds etc. When it comes to social networking sites there are numerous number of sites among those some popular social networking sites which people tend to use are Facebook, Google+, Instagram, Twitter etc.

Social networking sites allow space for users to add personal information such as birthday, gender, relationships, interests, education, employment history and contact information. Furthermore, online social networking sites such as Facebook allow users to access another friend's timeline by posting on their walls, inserting images etc. These facilities are now famous among people to keep contact with each other. Even though social networking sites give users many advantages as everything it too contains a side of disadvantages. As people tend to post their personal information on social networking sites the eye of the hackers is now been followed to many social networks. They keep track of the profiles in the sites to do various criminal activities.

Cyber criminals targeting on social networking sites are in many ways they are "Daniel of service" (DOS), this is an attack which makes a computer or a network unavailable to the user. DOS is being created to interrupt the users temporally or permanently which is connected to the internet. DOS can affect to social networking sites by slowing the access of the profiles, making unavailable the account, making spam messages to other friends with use of DOS. "Distributed Daniel of Service Attack" (DDOS) is an attack that can make whole online social network unavailable for users. DDOS attacks mainly broadcasted to large networks because it can spread to a large network. The attack that are spread through the networks are defined as Botnets. Once the botnet is infected the devices can be controlled remotely without the owner. Figure 1 below shows a brief idea about DOS and DDOS attack.

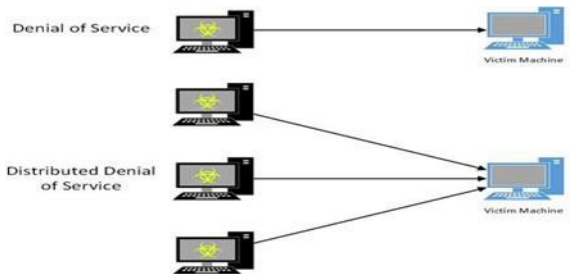

Figure 1: DOS & DDOS Attack (Source: http://www.dillonhale.com/files/cache/74691619a94df15a86363fd5dee1c3eb_f80.jpg)

A major attack which is been running through social networking sites is the "Brute Force" attack this is a software which is developed to guess passwords of the private accounts. Brute force attacks the user in the front door which means it tries to hack the password by gaining access to error attempts. Figure

2 below shows an interface image of a software that have been implemented to brute force attack.

Figure 2:Brute Force Attack (Source: http://hackspc.com/wpcontent/uploads/2012/0/bruteforce-2.jpg)

Moreover, a main threat which run throughout social media is the "Phishing Attack", through this it runs a spam link all along the profiles asking the confidential information. Figure 3 gives a brief idea of a phishing attack on a social networking site.

Figure 3: Phishing Attack (Source: http://facecrooks.com/wp-content/uploads/2012/08/they_were_recording_you_phishing1.jpg)

Considering the types of attacks mentioned above there are many ways for criminals to access the social networks. Though there are many ways to handle the situation the main problem arise is the security which is caused when the user tries to log into their accounts. The proposed research is based on an intelligent way to access social networks by introducing a highly secured log in method.

Section IV will discuss about the approach to the proposed research by going through the discussion on findings on section II.

II. DISCUSSION ON FINDINGS

"Security Policy and Social Media Use" developed by Maxwell Chi introduced a secure way to access the social networking sites. The research paper concludes series of privacy systems to access social networking sites such as keeping a strong password, CAPTCHAs, clearing the browsing history and desktop security. Considering the above facts research group concludes that the system they introduced was not highly secured with the hackers. The proposed research "Defending Social Networks from Cyber Attacks" includes an algorithm which consists of voice identifier when login, location identification system and the concept CAPTCHAs [1].

Mobile social networking security named LAMSN developed to identify the location was developed by Aaron Beach, Mike Gartrell, and Richard Han. The scope of the research based on mobile social networking to overcome the security issues while login with mobile devices they introduced a method of location based service. The researchers implemented only a security method to mobile devices and the method is not that enough to defend the cyber-attacks to social networking sites. The proposed research includes with more functionalities to defend the task [2].

Research based on configuring the settings of social networking sites named "Privacy in Online Social Networks" developed by Michael Beye et al. The research consists of methods how to operate a social networking site such as messaging, multimedia, tagging and preferences. The methodology of them is a good practice to keep the private profiles safely but the system does not cover a method to login to the account in a safe manner. The proposed research is enhanced with more privacy aspects while the user sign ins [3].

Social networking sites and their security issues is providing architecture for secure request response exchange of data among users. This architecture improves the customization of profiles. According to this architecture if the visitors or friends request for any information through this application which is between the visitor and the user. The application requests to the user for the response then the user can response from any one of the databases according to his trust on the person who has requested for the information. Other functionality of this architecture is that user can have two different databases with different information provided. The user may select data from any one of the two databases to response a particular request. Disadvantage of this request- response architecture is not effective and reliable way of cyber protection. To overcome this problem bio- metric voice recognition system will give effective solution for cyber-crimes [4].

Photo-Based Authentication Using Social Networking research is based on photo based authentication frame work known as Lineup. Lineup mainly used "CAPTCHA" mechanism. Lineup application can help site administrator or content publisher to check and confirm a client membership by user needs to identify the group of photos. This authentication system provides facility to enter the web site without remembering the password. Disadvantage of this system if another person knows the photos which are provide by the system then that person can easily log in to the system. To overcome this problem bio-metric voice recognition system will provide better solution for this problem. In voice recognition system, only the users' voice will be recognized and validated by that algorithm [5].

Mitigating Cybercrime and Online Social Networks Threats in Nigeria research is introducing centralized data base with users' "activity log" feature. The system authenticates and uniquely identifies every social network user. System will generate a special identification number in signing up. User will have unique user name and password. When user logs in to system, system will track the users' Internet Protocol (IP)

address. In this system there are some fundamental issues. There are some issues with that system some of them are user need to complete long process in order to getting register to the system and user need to log into email to get pin code. Researches have been introduced some solutions. Those solutions are not giving exact and reliable solutions for the above mentioned problems. Bio metric voice recognition algorithm will provide ideal solution for above mentioned problems [6].

"Cyber Threats in social Networking Websites "is in the current world billions of people use the social media networking for many different uses throughout their daily lifestyle. To be InTouch with friend's family and get the latest updates about celebrates and etc. Users also provide their personal details to these websites. Introduction of Facebook social network this was increased rapidly. Nowadays people tempt to use the social media network as a medium to share their top personal and secret files. This is very risky, also they authorize the unwanted programs via their social media accounts. These programs will be able to gather the information that is very classifies. Also the tracking of the user behavior is very important fact. Social media network owners can gather the user behavior and they will provide services according to your interests. What will happen if this information gets hacked by hackers or this information are passed into dangerous hands? [7].

"Security and privacy measurements in social networks" are one of the crucial topics concerned at present. According to this topic research team can realize what are importance of discussing this topic. This one is relevant to the current society that is why group decided to use this topic for group research. There is many research relevant to the topic had done by many researchers. "Security and privacy in online social networks" is one of the researches done by Levcio Antonin Cutillo based on the relevant topic. Centralized online social networks pose a threat to their user's privacy as social network provider have unlimited access to user's data this idea includes in the research done by the institute of Royal Institute of technology. [8].

Network security and protecting intellectual information against digital theft. Exchange of information through these networking media websites. The rise of social media sites where people can share events from their daily lives now place of importance. Companies, not wanting. People connected to each other over social networking sites. Peoples exchange of thoughts, ideas, and experiences over social network. Social networking sites to keep people connected to each other. People exchange thoughts, ideas, and experiences. This social network site has risk. People exchange lot of information among people. This information can be stolen. For avoid this problem have to protect this information. Using cryptography and steganography will protect information. This should be control exchange data among social network. Breakdown these types of attacks, research team suggest focusing on the technique [9].

Internet is competent and useful ways to communicate and sharing the information. More people are concerning about the privacy and it has become an important issue. This paper will discuss how the privacy become a risk and overcome that issue. Internet users use social networking website to communicate with their friends, share their thoughts, photos, and videos. Personal information that user provide on social network can be easily found by the hacker if user do not protect the cookies. This research paper has stated some security and privacy awareness that can be practiced in order to be more aware of social network threats. Computer users to be aware about computer security and privacy and to know what steps to take to defend against attacks. And also we have to identify threats that can affect the users on social network [10].

The central authority can control Sybil attacks easily. For example, if the system requires users to register with government-issued social security numbers or driver's license numbers then Sybil attack becomes much higher. The central authority may also instead require a payment for each identity. Defending against Sybil attacks without a trusted central authority is much harder. This paper discussed limited progress on how to defend against Sybil attacks without a trusted central authority, each of these Sybil attackers can potentially create an unlimited number of "malicious users". This paper presented Sybil Guard, a novel decentralized protocol for limiting the corruptive influences of Sybil attacks, by bounding both the number and size of Sybil groups [11].

"Secure Authentication and cybercrime Mitigation for social Networking sites" by Anjitha and Harsha for a university research is about the advent of online social networking sites and its usage of how it dramatically grown. It is proposed a frame work as Online Social Networking and the RSA algorithm is used [12].

"How much privacy We still have on social Network" is researched by for Malaysia university student and they have discussed that internet is one the most efficient and effective way to communicate and sharing information especially in terms of terms of social network sites. They reviewed how the current privacy plays on social network sites and analyzed [13].

Many online social network (OSN) users are unaware of the numerous security risks. According to the recent studies, OSN users input personal and private details. If this details gone into a wrong person both in real and virtual. This risks become even more severe when the user is children. In this research paper, include different security and privacy, how OSN users caught for these type of threats and also solution for better protection, security and privacy for OSN users. Social network has dark side ripe with hackers, fraudsters and online predators. There are some solution to project the privacy and security. Protect the user details have to develop some algorithm and bio metric system [14].

This research "On Cybersecurity, Crowdsourcing, And Social Cyber-Attack" is conducted by the author, Rebecca Goolsby for her Ph.D. This is discussed that cyber security efforts must take into account the growing potential for cyber-attack using social media, where hoax messages are incorporated into a stream of otherwise legitimate messages, and understand how quickly mobile apps and text services can disseminate false information. Furthermore, the darker aspects of their capabilities should not be ignored. Disaster responders, humanitarian relief workers, and a new breed of digital volunteers who provide technical support during and after a crisis may need to be particularly cautious. As part of solutions she suggested that all social media users need to develop a healthy skepticism about the messages that they receive, learn to check sources, and refine their skills of discernment. Social media watchdog groups also

play a role in the education of the user community, spreading the word about hoaxes, scams, and attacks very quickly and widely—if only users will pay attention [15]

III. ATTEMPTS THAT HAVE BEEN TAKEN TO PREVENT CYBER ATTACKS ON SOCIAL NETWORKING SITES.

Online social networking users are facing to various privacy and security threats while using social networks. There are many software's and solution that have been provided to users to securely access their social networks. Some basic ways that cyber-crimes that can be mitigate are as follows.

- Keep a strong password.
- Keep the firewall turned on.
- Keep the computer up to date.
- Making use of the privacy settings defined by the social networks.
- Do not add personal information.
- Do not accept the requests from strangers.

However, users use the above mentioned aspects user does not get the solution for the problems that they face while using the social networking sites. Somehow there are methods that the hackers have found to hack the personal accounts by implementing regardless software's. Implementing an essential solution for social network authentication can reduce the attacks. Section IV introduce the approach for the proposed methodology.

IV. OUR APPROACH

Section III above shows the basic steps that have taken to prevent the cyber-attacks on social networking sites. The research group identified that the attempts that have been taken to prevent cyber-attacks on social networking sites (Section III) are not enough to prevent the attacks from hackers due to less secureness with the login method.

The proposed methodology is based on a login method that includes a voice recognition system. Along with the voice recognition system the proposed method consists of a CAPTHAs method and a location identification method using global position system (GPS).

a. Voice Recognition

Voice recognition is a method that the computer or the mobile device identifies the speech that is given by the user in order to access the social networking site. This means that the device must identify the speech that is given by the user and in order to recognize the voice the user must give the speech according to the accent they use since the system needs to identify it while the user gives it again when trying to access the account. The proposed method is highly secured with the voice access because the voice is a unique thing to person the attacks to hack the method is quite difficult compared to other login methodologies. The voice recognition registering steps access as follows.

- First when the user is signing up for the account they must provide a voice record that is minimum to 10 seconds.
- The voice record can be of any word or number that can be identified by the system.
- To confirm the voice while registering to the account the system will ask the user to input voice for 3 times.
- After registering the voice, it will be saved to the database of the social network.
- To register for the social network a computer can be used with a connected micro phone and from mobile devices the user can register for their accounts.

b. How the Voice Recognition Works?

Voice recognition method is working on a voice platform, web servers, authentication servers along with voice bio metric matching engines. Once the user gives the voice command the system will automatically generated to a vocal password. The entered voice will be check with the stored data in the database server and if the voice of the user is valid the user can securely login to their accounts. Incase if the entered voice is a fraudulent one it will be recorded by the server and stored in the database to listen to the actual user of the account. Moreover, while concerning about the voice that we provide it will capture the voice along with the noise so that users can enter any voice command as the vocal password since the system will identify it by the noise and voice of the user. However, in some attempts to login using with use of vocal password can be failed to overcome the task the user is given three attempts to give the voice to the login attempt and after the attempt the system will matching the voice with the stored voice in the database. Furthermore, if the user needs to reset the voice the user can login with the given voice and change the vocal password by giving the new vocal password to the account. The following figure 4 shows the architecture diagram of the proposed voice recognition methodology.

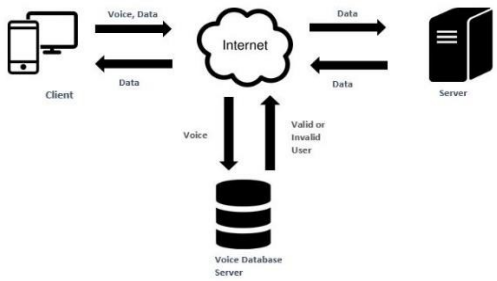

Figure 4: Architecture of the proposed voice recognition

The figure 4 describes the main method that is been implemented in voice recognition methodology. Client sends the data to the server using the internet and the voice will be stored to the database server. Authenticate a user the request will go to the server after the request is made voice database will contact the server to identify the given voice match with the voice which is been stored in the database currently. If the user

entered voice is correct user can log to the account easily incase if the voice does not match with the voice in the database, it will store the voice in the database while the user does not grant permission to access the social networking site. The process will happen continuously when a user tries to login the client request from the server and the server respond to the request.

Today many web sites especially social network sites want high security and protection. However Web access control mechanisms remain fairly cumbrous; administrators must maintain access control lists and user accounts, and users must want to remember and handle a large collection of passwords. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), the method that research group used to best security solution to protect the social network sites.

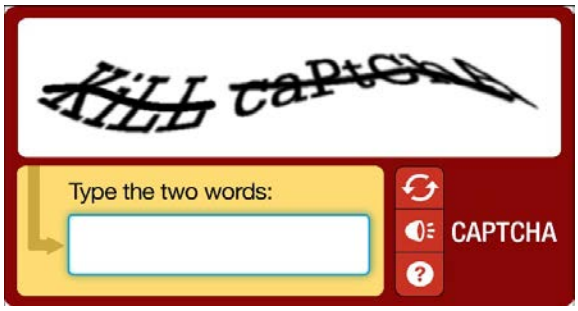

Figure 6: CAPTCHA (Source:https://regmedia.co.uk/2013/ 08/05/captcha_kill er.jpg?x=1200&y=794)

The purpose of CAPTCHA is to block form submissions by spam bots (not human), which are automated copy that post spam content everywhere they can. The CAPTCHA module provides this feature to virtually any user facing web form on a Drupal site (Open-source content management system). To prevent bots from overrunning sites with spam, fake registrations, fake sweepstakes entries, and other horrible things, creators responded by testing users to see if they were human or not. CAPATCHs present automatically generated graphical images to a user that contains some text and asks the user to identify the order of characters that is presented in the graphic. CAPTCHAs implementations can be found on more than 4 million sites globally, and human beings solve CAPTCHAs implementations more than 500 million challenge to response the test to the users or humans. They are classified based on what is distorted that is whether alphabetic or numeric values. CAPTCHs have many advantages like advanced security, ease of use and creation of value. There are four types of CAPTCHs that can use for the security.

- Text based CAPTCHAs
- Image based CAPTCHAs
- Audio based CAPTCHAs
- Video based CAPTCHAs

Text-based CAPTCHAs is mainly target to the research paper as figure 6 CAPTCHs can create by using PHP or ASP.Net.

d. How to create a new CAPTCHAs

The following steps show the working of CAPTCHAs;

- Create Random Value: Firstly, user generating CAPTCHAs is to create some random words numbers. These random values are often hard to do light-reading and guess.
- Generate an Image: Images area used as there are harder to read by the Internet bot and are nice and readable to humans. It is an important step in CAPTCHA as simple text in images can be broken easily.
- Store It: The random string generated that is also in the image is stored for matching user input. For this session variables are exhausted.
- Matching: After these steps, CAPTCHA is drawn and shown on some form which one want to protect from being reviled. User fills form along with CAPTCHA text & submits it.
- Now one has the following:
- All submitted form data.
- CAPTCHAs string input by the user.
- CAPTCHAs string (real one) from session variables. Session variable is currently used as to keep stored values across page requests.
- If match is found, then it is ok, otherwise not, in that chance the message showing to the user is that the CAPTCHAs they had submitted are wrong.

CAPTCHs means verify the login account. In CAPTCHAs values are type wrong user cannot access the site. User can changed the CAPTCHs order to get easy value or voice spelling sound to enter the CAPTCHs. The system is mainly targeted on voice recognition which user to login their account using a voice tracking method and also CAPTCHA's method.

e. Location Identification

Normally social networks can be accessed via smart phone, tablets and personal computers. While that a person wants to login to his or her own social network account, the location will be capture in sign in process. Once the user going to logs in to the user account, GPS tracking system will use to track user's current location, before the voice recognition process begins. With this implementation we can store user's location so that it is easy to find out where the user id currently logged in. This can be composed of hardware facilities, software interfaces via a web server or using Google maps. This can be achieved with a voice tracking system which includes a General Packet aid of message transmission. The usage of some micro controller's temporary information to store the location can be acquired to transmit user's details in real time. This can be specially maintained with the process of using message transfer protocol that get accurate location and robust the stability and security of social networks. In user act as an embedded device with a GPS module to identify users' location and that is periodically transmitted to server. The information about the user's location that is stored in database can be search and display using Google maps or other relevant map service. This implementation it is easy to reduce numerous cyber-attacks that are widely spreader in the world.

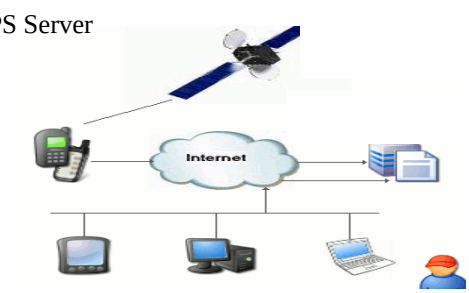

Figure 7: Architecture of location tracking (Source: http://www.bigbrotherme.co.nz/images/howitworks.gif)

V. FUTURE WORKS

In order to defend the cyber-attack this paper has mainly introduces voice recognition technique to prevent cyber-attacks with CAPTCHA's mechanism and location identification. The main technique addressed in this paper known as Voice recognition technique, the user authenticates by comparing according to the voice of the user which is stored in the database with the provided voice at the login. In some situation the voice may be change of that particular user such as when the user's voice changes due to physical problems or in another condition Authentication should be done accordingly. Then the voice should be identified and user needs to authenticate by the system without any trouble. Therefore, the system should recognize that sort of changes of particular voice which we did not discuss in this paper. Researches can focus on above mentioned situations in the future. Through that security mechanisms will become more reliable.

VI. CONCLUSION

Fast development of information technology impacts to the human life styles. However, with the development social networking came to the world and cyber-attacks take place to the social networks to attack them. Secure authentication is a method to get over the issues that are made through cyber-attacks. This paper introduces an algorithm to defend the cyber-attacks with the field of voice recognition methodology for login along with CAPTHAs to identify the spam bots and location identification to track the location using GPS to take the place from where the social networking account accessed.

REFERENCES

[1] M Chi, (2011), "Security Policy and Social Media Use" SANS InstituteInfoSec Reading Room, [Online], Available: https://www.sans.org/reading- room/whitepapers/policyissues/reducing-risks-social-media- organization-33749 [Accessed: 16 July 2016]

[2] A Beach, M Gartrell, and R Han, (2009), "Solutions to Security and Privacy Issues in Mobile Social Networking", International Conference on Computational Science and Engineering, vol. 4, pp.1036-1042 [Online], Available:http://www.cs.colorado.edu/~rhan/Papers/smw09_solutions_securi ty_privacy.pdf [Accessed:19 July 2016]

[3] M Beye, A Jeckmans, Z Erkin, P Hartel, R Lagendijk, Q Tang, (2010) "Literature Overview - Privacy in Online Social Networks", University of Twente Publication [Online], Available: http://doc.utwente.nl/74094/1/literaturereview.pdf [Accessed: 20 July 2016]

[4] A Kumar, S.K Guptha, A.K Rai, S Sinha, (2013), "Social Networking Sites and Their Security Issues", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 [Online], Available:http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.300.4675&rep=rep1&type=pdf. [Accessed: 18 July2016]

[5] S Yardi, N Feamster1, A Bruckman, (2008), "Photo-Based Authentication Using Social Networks", ACM Sigcomm Workshop on Online Social Networks [Online], Available: http://yardi.people.si.umich.edu/pubs/Yardi_AuthenticatingSocial Network08.pdf. [Accessed: 17 July 2016]

[6] Adu M. K, Alese B. K, Adewale O. S, (2014) "Mitigating Cybercrime and Online Social Networks Threats in Nigeria", Proceedings of the World Congress on Engineering and Computer Science 2014, Vol I WCECS 2014, pp.22-24, October 2014 [Online], Avalable: http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp4 13-417.pdf [Accessed: 20 July 2016]

[7] W Gharibi, M Shaabi "Cyber Threats in Social Networking Websites" College of Computer Science & Information Systems Jazan University Available: https://arxiv.org/ftp/arxiv/papers/1202/1202.2420.pdf [Accessed:21 July 2016]

[8] Zanero, S, D Keromytis , " Security and privacy measurements in social networks". Available: http://nsl.cs.columbia.edu/papers/2014/lessons.badgers14.pdf [Accessed: 25 July 2016]

D Gunter , Solomon S, "The Danger of Data Exfiltration over Social Media Sites" , Western International University, Available: https://media.blackhat.com/bh-us-12/Briefings/Gunter/BH_US_12_Gunter_Sonya_SNSCat_WP.pdf [Accessed: 19 July 2016]

[9] M Chewae, S Hayikader , M H Hasan,(2015), "How Much Privancy We Still Have on Social Network", International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015, 1, [Online: January 2015], Available: http://www.ijsrp.org/research-paper-0115/ijsrp-p3755.pdf [Accessed: 26 July 2016]

[10]

[11] H Yu, M Kaminsky, P B Gibbons, Aflaxman,(2006), "SybilGuard - Defending Against Sybil Attacks via Social Networks", Association for Computing Machinery(ACM), Available: http://www.math.cmu.edu/~adf/research/SybilGuard.pdf [Accessed: 17 July 2016].

[12] Anjitha T, Harsha V, (2016) "Secure Authentication and Cyber Crime Mitigation for Social Networking Sites", International Journal of Science and Research (IJSR) ISSN 2319-7064 [Online], Available: https://www.ijsr.net/archive/v5i5/NOV163284.pdf [Accessed:19 July 2016]

[13] Hayikader S, H Hasan, M. Chewae, M.C. Ibrahim J, (2015), "How Much Privacy We Still Have on Social Network.", International Journal of Science and Research (IJSR), Volume 5, Issue 1, [Online: January 2015], Available: http://www.ijsrp.org/research-paper-0115/ijsrp-p3755.pdf (Accessed: 8 September 2016).

[14] Michael Fire, Roy Goldschmidt, Yuval Elovici, (2014), "Online Social Networks: Threats and Solutions", Ieee Communication Surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter [ONLINE] Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6809839, [Accessed 8 September 2016].

[15] Shanley L, Lovell A, Center W, (2012), "On Cybersecurity, Crowdsourcing, And Social Cyber-Attack", Available: https://www.wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf, [Accessed: 8 September 2016]

AUTHORS

First Author – L.S.Y. Dehigaspege, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Second Author – U.A.A.S. Hamy, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Third Author – H.A.H. Shehan, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Fourth Author – S.A. Dissanayake, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Fifth Author – H.P. Dangalla, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Sixth Author – W.H.I. Wijewantha, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Seventh Author – Dhishan Dhammearatchi, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd