Bio-metric Social Media Network Secure.

L.S. Wickramaarachchi , W.G.P. Prabashini , J.A.L.T. Hemachandra, S. Babiththira, J.Sanjeevan Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (PVT) Ltd

Abstract- The aim of this research paper is to make a security in social media network. Social media networking sites offer a straight forward way for people to have a simple social presence through web. They provide a virtual environment for people to share each and every activity, their interests, and their circle of acquaintance with their family, friends, or even the unknown. Usage of social media network is very high in nowadays, hackers have found very easy ways to steal personal information through these networking sites. The use of social media for communication is becoming more prevalent worldwide, with people from countries of varying economic development increasingly accessing the Internet to participate in networking sites. In present the social media has security risks. It is used to damage the reputation of popular person, criminals for fraudulent activity, gathering business intelligence, stealing sensitive information etc. This paper will demonstrate the security level increment & the methods that make the popular person's social media network profile more secure.

Index Terms: Social media network, social media network security, Social media networking sites, BioMetric Security, Popular personality

I. INTRODUCTION

Today internet is becoming part of our lives. Unlike in the past, today people have less relationship with each other. In the years we have witnessed a rapid development in information technology. It's commonly known as social media. There are popular social media sites such as Facebook, Twitter, My space, Google+ and instagram etc. It has been shown in figure 01.

Today Social media networks have over 2.13 billion active users It has been shown in figure 02, table 01 and figure 05 in Appendix A[18].And who spent more than 9.7 billion minutes per day on the social media network sites [16]. Half of all Social media network users have more than 200 friends [17]. Anyone can create profiles easily. Two kinds of people create profiles, normal people and special personalities like Cricketers, actors, politicians whom belong to special personality category.

Figure 01: Social media networks
(Source:http://www.cyberneticsltd.com/services/webservices/Social-media-marketing/)

Special personalities create profiles and the possibility to hack these profiles is vast. There are instances of complaining about hacking special personalities profiles. Some hackers have logged in such profiles and uploaded photos and private information into the internet. It's a tragic circumstance. So many special personalities hate to create profiles. They have no trust in security either. A solution for this research paper tries to introduce a new technology to protect profiles.

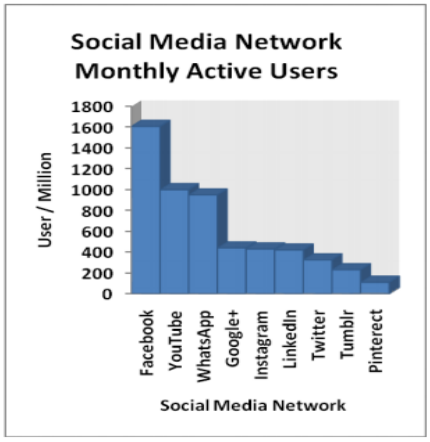

Figure 02: Social media network monthly active users
(Source:http://www.socialnomics.net/2016/02/09/social-media-user-statistics-2016/)

II. BACKGROUND AND RELATED WORKS

The human factor in the social media security combining education and technology to reduce social engineering risks and damages, is demonstrating the cyber security risks and mitigations, focusing on the human factor and social media. Formal policy to guide how employees can use social media sites is not enough, and complementary layers are needed: education starting at elementary school, interactive and adaptable training and innovative technology means. To strengthen the human factor, should put effort in education, starting as early as the first grade, at the age that the children are exposed to the internet. Unusual approaches to cyber security training should be considered. Also put more effort on technological means of helping humans make fewer errors and avoid falling into cyber traps. Privacy settings can limit access to the user's information. Social media site monitoring tools can help organizations keep track of malicious activities and threats against them. Technology can help to check the reliability of the person suggesting friendship. Social networks can also be used to identify an organization's insider threat, by analyzing the social media content. Combining education and training with best-of-breed technology may reduce social engineering risks and damages. Disadvantage of this is give education and training to peoples are get long time period, to overcome this problem Biometric Social Network Secure is develop by using new networking technologies [1].

User awareness of social media security the public sector framework is to examine factors affecting user security concerns among social media users in the educational sector. The researchers employed a quantitative research approach because the subject matter needs further definition. This aids researchers in determining a suitable research design and data collection method, as well as to examine the hypotheses and proposition developed in the current Problem. Disadvantage of this is hypotheses and proposition develop are get long time period and want many statistical data, to overcome this problem Biometric Social Network Secure is develop by using new technologies to secure social media [2].

A new social media security model, is increases in functionality and popularity, it has become more vulnerable. It is no secret that social media vendors exclude security during development, hence leaving it to users' discretion which raises a serious cause for concern. The aim of this is to study existing vulnerabilities of online social media and propose practical solutions. The importance of studying social media vulnerabilities provides a clear understanding in developing a new security model to prevent social engineering attacks. Investigate key security vulnerabilities eroding the trust placed on social media such as profile cloning, single factor authentication, weak password creation, weak account activation systems, privacy vulnerabilities, unethical posts and multiple login sessions. Disadvantage of this is key security is not a most suitable secure method it might be hack by in social media, to overcome this problem Biometric Social Network Secure is develop by using biometric fingerprint key to secure social media[3].

Social media security policies: guidelines for organizations, is introduction of Social Media into the workplace has created the need for a new way of thinking for people. Social Media's growth into corporations has opened opportunities and benefits that many corporations did not foresee in the past. However, the use of these services has also created many risks for the company's reputation and has developed vulnerabilities in corporate culture and security policies. Some risks are so great that businesses are putting an all-out ban on the use of the Social Media services. This examines the impact of social networks on corporate culture as well as on corporate information security policies. Guidelines are offered for an organization to enhance their presence with social networks as well as employee participation. Disadvantage of this is its only depends on the security policies, to overcome this problem Biometric Social Network Secure is developing by using combination of security policies and new networking technologies for advance Social media security [4].

Countering Social Engineering through Social Media: An Enterprise Security Perspective is increasing threat of social engineers targeting social media channels to advance their attack effectiveness on company data has seen many organizations introducing initiatives to better understand these vulnerabilities. This examines concerns of social engineering through social media within the enterprise and explores countermeasures undertaken to stem ensuing risk. Also included is an analysis of existing social media security policies and guidelines within the public and private sectors. Disadvantage of this is its depends on the security policies, to overcome this problem Biometric Social Network Secure is develop by using biometric fingerprint key to secure social media [5].

Security model to control on social media using visualization and forensic approach is providing cyber security controls on social media is becoming critical particularly for the enforcer in community. Controlling on social media contents are much more demanding than the conversational media. Moreover, the enforcer has identified the real and virtual information should be protected from any devastating physical, logical or cyber impact. In this long term project, this research has focused on cyber impact to society and also identified cyber problems area like illegitimate rumors, fake non textual content, wrong perception, unfeasible to trace the irresponsible writers and detecting any malicious data on social media contents. At the end of this project, it's expected to produce controlling rumors propagation model, network forensic analyzer prediction model and intelligent image to identify factors on shaping appropriate perception on social media readers activities. Disadvantage of this is forensic analyzer prediction model and intelligent image are might be sometimes give error figures, to overcome this problem Biometric Social Network Secure is develop by bio-metric fingerprint key using new networking technologies [6].

Security Management real versus perceived risk of commercial exploitation of social media personal data, is covers one of the issues in security management, which is that people react

more on their perceived risk rather than on their real risk. This work is designed to be the first one to consider that user's behavior is a mix between perceived risk and accepted risk. This research defines two dimensions of risk analysis and it has designed a real and perceived risk test measuring prudent vs. risky behavior and feeling safe vs. At risk, then this work introduces the idea that there are four types of personality depending on the perceived degree of risk and the real and accepted degree of risk are conscious, paranoiac, unconcerned, and paradoxes. Disadvantage of these two dimensions of risk analysis is not enough to secure social media networks, to overcome this problem Biometric Social Network Secure is developing by using combination of risk analysis and new networking technologies for advance Social media security [7].

A robust finger print based two-server authentication and key exchange system, is based user authentication systems are highly secured and efficient to use and place total trust on the authentication server where biometric verification data are stored in a central database. Such systems are, prone to dictionary attacks initiated at the server side. Compromise of the authentication server by either outsiders or insiders do all user private data to exposure and may have serious repercussions to an organization. In this present a practical fingerprint based user authentication and key exchange system employing novel two-server architecture. Here, make use of Image processing techniques to extract a biometric measurement from fingerprint image. In this system, only a front-end service server engages directly with users while a control server stays behind the scene. Also the system is secure against offline dictionary attacks mounted by either of the two servers. Disadvantage of this is use a simple sever to store fingerprints are not a most suitable secure method it might be hack, to overcome this problem Biometric Social Network Secure is develop by using bio-metric fingerprint keys are store in social media network central database [8].

Biometrics verification techniques combing with digital signature for multimodal biometrics payment system which consists of functions like finger print authentication, using a digital signature, hand/face authentication. This lacks functions like using a smart card to store biometric data, Finger print authentication for automatic teller machine, Using Short Message Service for user authentication, Utilizes a minutiae matcher for fingerprint, using finger print verification for online transactions, Using on card comparison for finger print verification. Disadvantage of this is only for payment systems, to overcome this problem Biometric Social Network Secure is developing for this Social media security by using new technologies to secure social media [9].

Symmetric key encryption technique, cellular automata based approach and cellular automaton is one of the most engrossing fields of studies. At the present digital world where almost every communication is being done via the internet, requirement of security and privacy of information is a must. For securing big or small data over internet, cryptographic techniques are essential. Usage of cellular automata characteristics in the field of cryptography is still not much explored. Here, the presents a symmetric key cryptographic technique of block cipher using cellular automata rules. Disadvantage of this is only for cellular automata systems, to overcome this problem Biometric Social Network Secure is develop by secure browser to social media central sever communication using new encrypt and decrypt method, using new networking technologies [10].

Social Networking Sites and Their Security Issues is Social networking sites offer a straightforward way for people to have a simple social presence through web. They provide a virtual environment for people to share each and every activity, their interests, and their circle of acquaintance with their family, friends, or even the unknown. With so much sharing, Found hackers and thieves in social networks, very easy ways to steal personal information through networking sites. This calls for advances in security protocols to safeguard against hackers. This discusses some of the privacy and security concerns, attacks and their respective prevention techniques. Disadvantage of this is only use of security protocols to safeguard social network is not enough, to overcome this problem Biometric Social Network Secure is develop by using biometric fingerprint keys to secure social media networks [11].

Estimating the sentiment of social media content for security informatics applications is Inferring the sentiment of social media content, for instance blog posts and forum threads, is both of great interest to security analysts and technically challenging to accomplish. This presents two computational methods for estimating social media sentiment which address the challenges associated with Web based analysis. Each method formulates the task as one of text classification, models the data as a bipartite graph of documents and words, and assumes that only limited prior information is available regarding the sentiment orientation of any of the documents or words of interest. The first algorithm is a semi supervised sentiment classifier which combines knowledge of the sentiment labels for a few documents and words with information present in unlabeled data which is abundant online. The second algorithm assumes existence of a set of labeled documents in a domain related to the domain of interest, and leverages these data to estimate sentiment in the target domain. Disadvantage of this is only use of algorithms to safeguard social network is not enough, to overcome this problem Biometric Social Network Secure is develop by using biometric fingerprint keys to secure social media networks [12].

Online social media networking and assessing its security risks are presents the security risks of online social media networking and then attempts to develop the model for assessing its security risks. This can help security professionals for assessing security risks in the existing information systems and designing new security systems of enterprise. Disadvantage of this is only use of algorithms complex multi layered informational system is not enough, to overcome this problem Biometric Social Network Secure is develop by using bio-metric fingerprint keys to secure social media networks [13].

Security policy and social media use is intended to demonstrate that the existing information security policies already in place at many organizations can easily be extended to cover social media. Therefore, organizations do not need to issue security policies and guidelines specifically for social media. This attempts to demonstrate that the main security threats posed by social media and would be addressed by a good overall security awareness program, along with and technical and administrative safeguards. Disadvantage of this is only use of security policies to safeguard social network is not enough, to overcome this problem Biometric Social Network Secure is develop by using biometric fingerprint keys to more secure social media networks [14].

Security and privacy in an online world is describe the amazing advances in information and communications technologies, peoples are heading for an online world in which convenience goods have unprecedented computing power and are permanently connected to the internet or stored in the cloud. The internet is everywhere, and now people are talking about the Internet and its things. Look at your own belongings; it's likely that you carry around at least one or possibly several handheld devices such as smart phones that are permanently connected to the internet. Now people use internet to download and play songs and movies, access social media, run e-mail or messenger software, or access any of the other myriad apps people have created recently. This is mainly described usage of the internet [15].

Background and related works Comparison has been shown in table 02 in Appendix B.

III. Proposed solution

This research paper introduces a smart solution to protect the profiles of the special personalities. It is a technology to protect their profile from unauthorized users in very safety way. Up to date social media network profiles have two security methods. One is password and other one is security code method. But these methods have less security. When the users miss the password or if someone can guess the password and if they get it, then he or she can use the social media network profile as his own one.

So this research paper introduces a new advanced technology. These profiles are considered as special profiles. Their appearance is same as the normal profiles but they are totally different in creating profiles, login the profiles and their security. Here in this paper finger print is used as the password. This is a very safe method as one's finger print shows user own identity.

Monthly Active Users	
Facebook	1.609 Billion
YouTube	1 Billion
WhatsApp	950 Million
Google+	440 Million
Instagram	430 Million
LinkedIn	420 Million
Twitter	325 Million
Tumblr	230 Million
Pinterest	110 Million

Table 01: Monthly Active Users in social media networks.

A. Creating a profile.

Creating a profile is totally different from the normal one. First, the user must send his finger print to the social media network headquarters. Social media network users are worldwide. So getting connections with the social media network headquarters is not an easy task. To solve this problem centers have been established in every country. Then the user can visit these centers and give their finger print, email and phone number. These centers send this data to the social media network headquarters. Social media network headquarters will create pre generate user profile and send to the user by email fellows. It enriches the information pool of your paper with expert comments or up gradations. And the researcher feels confident about their work and takes a jump to start the paper writing.

B. Login to profile.

Then user can go to the link and start login. First user must enter the email id and the password as usually. Then the user has to buy a finger print device and connect it to the USB port. Then only he can insert the finger print. Mostly modern phones have this function. After inserting the correct finger print, security code comes to the phone. As the third step he must enter the security code. After satisfying these three requirements the user can log to the social media network profile.

As we know finger prints are also transferring as binary codes. Another 19 finger prints are created in this technique. Thus 20 binary codes are encrypted. These encrypted 20 binary codes are transferred to social media network headquarters. Hackers will get a less possibility to hack these profiles in this method. Social media network headquarters know the correct finger print but hackers are not be able to select the correct finger print among the 20 finger prints. This system allows putting a finger print once only. It is very difficult to hack the profile because of these reasons. The user is Notified that the hacker enter the profile by getting a phone alert. Then the user can take action immediately.

Not only that, user can see all the login time, place, ipaddress, all the records, phone message when necessary. In this research paper it introduces a most secure and smart method to protect the profiles of the special personalities.

C. *Secure data communication.*

Data communication between web browser and social media network sever to create better secure data communication, this can develop a new encrypt – decrypt method, using encrypt key for user input biometric fingerprint key and use decrypt key for stored biometric fingerprint key in the social media network sever side biometric fingerprint database. It has been clearly shown in figure 03.

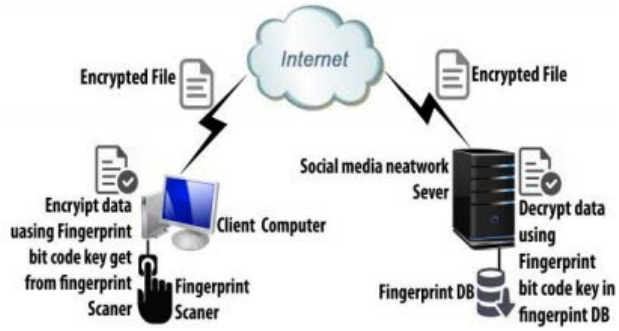

Figure 03: Social media network secure data Communication

IV. FUTURE WORKS

Future Works has been at the forefront of social media network login security and online data transfer between web browser and social media network server, and through experience and dedication. We continue to learn what works and what does not. This paper believes in social media with a biometric fingerprint to secure social media login and also online data transfer between web browser and social media network server using new encrypt and decrypt method develop using biometric fingerprint as a key. Our social media activity is not focused over roll social media network society, this develop only for just selected special persons like actors and actress, politicians. Also this biometric fingerprint key login system will help to identify our username & the password once we place our fingerprint in the device. Now this will help taking social media network security to the next level, this can help develop login security and secure data transfer to social media security to meet future needs.

V. CONCLUSION

Today in this World widely risen problem is hacking popular person's profiles or pages such as singers, actors, actress etc., social media network Profiles and creating fake profiles by editing their personal details such as images, videos etc. Such a kind of issues and damage the popular person's reputation. To avoid this problem this research has implemented and demonstrated the smart user friendly biometric finger print key by using encrypt-decrypt method to secure the special social media network profiles.

REFERENCES

[1.] David Tayouri (2015), "The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages", Research Gate [David Tayouri / Procedia Manufacturing 3 (2015) 1096 – 1100[David Tayouri / Procedia Manufacturing 3 (2015) 1096 – 1100 page 87, online: December 2015] Available: https://www.researchgate.net/publication/28396 1973_The_Human_Factor_in_the_Social_Media_Security_Combining_Education_and_Technology_to_Reduce_Social_Engineering_Risks_and_Damages [Accessed: Feb. 27, 2016].

[2.] Ali Hussein SalehZolait, Reem R. Al-Anizi, SuhairAbabneh, Fatima BuAsalliand NooraButaiba (2014), "User awareness of social media security: The public sector framework", Research Gate [Int. J. Business Information Systems, Vol. 17, No. 3 page - 55, 2014,online: JANUARY 2014] Available:https://www.researchgate.net/publication/286851196_User_awareness_of_social_media_security_The_public_sector_framework [Accessed: Feb. 27, 2016].

[3.] EhinomeIkhalia (2013), "A New Social Media Security Model (SMSM)", Research Gate [Volume XI, No. 1, 2010 page - 82, online: July 2013] Available:https://www.researchgate.net/publication/256667959_A_New_Social_Media_Security_Model_SMSM [Accessed: Feb. 27, 2016].

[4.] Nipul Patel (2010), "Social media security policies: guidelines for organizations", Research Gate [International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153 page 117 ,online: January 2010]Available:https://www.researchgate.net/publication/267989825_SOCIAL_MEDIA_SECURITY_POLICIES_GUIDELINES_FOR_ORGANIZATIONS [Accessed: Feb. 27, 2016].

[5.] Heidi Wilcox, Maumita Bhattacharya (2015), "Countering Social Engineering through Social Media: An Enterprise Security Perspective", Research Gate [Caroline Oehri, Stephanie TeufelUniversity of Fribourg, online:SEPTEMBER2015]Available:https://www.researchgate.net/publication/283731466_Countering_Social_Engineering_through_Social_Media_An_Enterprise_Security_Perspective [Accessed: Feb. 27, 2016].

[6.] MohdNazri Bin Ismail, MohdAfizi Bin MohdShukran, Kamaruzaman Bin Maskat(2015),"Security Model to Control on Social Media using Visualization and Forensic Approach", Research Gate [online: September 2015] Available:https://www.researchgate.net/publication/281740474_Security_Model_to_Control_on_Social_Media_using_Visualization_and_Forensic_Approach [Accessed: Feb. 27, 2016].

[7.] Lionel Khalil, Nancy AbiKaram(2015),"The Security Management: Real versus Perceived Risk of Commercial Exploitation of Social Media Personal Data", Research Gate [online: December 2015] Available: https://www.researchgate.net/publication/283953903_Security_Management_Real_versus_Perceived_Risk_of_Commercial_Exploitation_of_Social_Media_Personal_Data [Accessed: Feb. 27, 2016].

[8.] RajeswariMukesh, A. Damodaram, V. SubbiahBharathi(2008),"A robust finger print based two-server authentication and key exchange system", Research Gate [online: February 2008] Available: https://www.researchgate.net/publication/4346284_A_robust_finger_print_based_twoserver_authentication_and_key_exchange_system [Accessed: Feb. 27, 2016].

[9.] JuCheng Yang, (2010), "Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System", Research Gateway [online: October 2010], Available: https://www.researchgate.net/publication/232616118_Biometrics_Verification_Techniques_Combing_with_Digital_Signature_for_Multimodal_Biometrics_Payment_System [Accessed: Feb. 27, 2016].

[10.] DeepikaParashar, Satyabrata Roy, NilanjanDey, Vipin Jain, U. S. Rawat (2015) " Symmetric Key Encryption Technique: A Cellular Automata based Approach ", Research Gateway [online: December 2015] Available:

https://www.researchgate.net/publication/282780050_Symmetric_Key_Encryption_Technique_A_Cellular_Automata_based_Approach [Accessed: Feb. 27, 2016].

[11.] A Kumar, SK Gupta, AK Rai, S Sinha (2013) "Social networking sites and their security issues", Google Scholar [online: April 2013] Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.435.5624&rep=rep1&type=pdf[Accessed: Feb. 27, 2016].

[12.] Kristin GlassAffiliated, Richard Colbaugh(2012) "Estimating the sentiment of social media content for security informatics applications", Springer Link. [online: December 2012] Available: http://link.springer.com/article/10.1186/2190-8532-1-3/fulltext.html[Accessed: Feb. 27, 2016].

[13.] Hak J. Kim (2012) "Social Online Social Media Networking and Assessing Its Security Risks", Google Scholar [online: July, 2012] Available: http://www.sersc.org/journals/IJSIA/vol6_no3_2012/2.pdf [Accessed: Feb. 27, 2016].

[14.] Maxwell Chi (2011) "Security Policy and Social Media Use", Google Scholar [online: March, 2011] Available: https://www.sans.org/readingroom/whitepapers/policyissues/reducing-riskssocial-media-organization-33749[Accessed: Feb.27, 2016].

[15.] Rolf Oppliger(2011) "Security and Privacy in an Online World ", IEEEXplore [online: September 2011] Available:http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6017170&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6017170[Accesse: Feb. 27, 2016].

[16.] Socialbakers (2016) "Facebook statistics directory ", Socialbakers [online: 2016] Available:http://www.socialbakers.com/statistics/facebook/ [Accessed: Feb. 28, 2016].

[17.] Theguardian (2016) "Facebook: 10 years of social networking, in numbers ", Theguardian [online: 2016]Available:http://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbersstatistics [Accessed: Feb. 27, 2016].

[18.] Statista (2016) "number-of-worldwide-socialnetwork-users ", statista [online: 2016]www.statista.com/statistics/278414/number-ofworldwide-social-network-users [Accessed: Feb.27, 2016].

Appendix A:

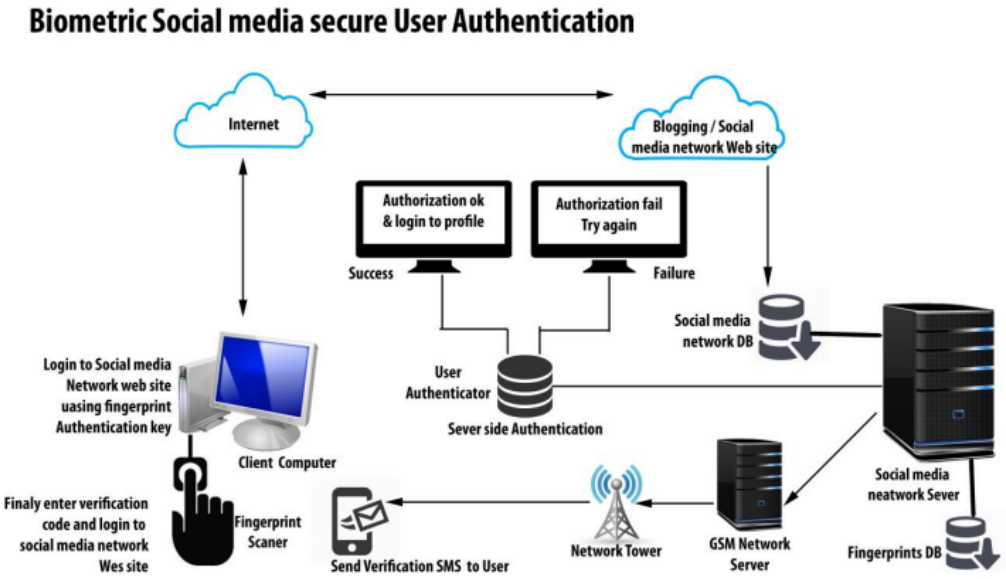

Figure 04: Bio-metric social media user authentication

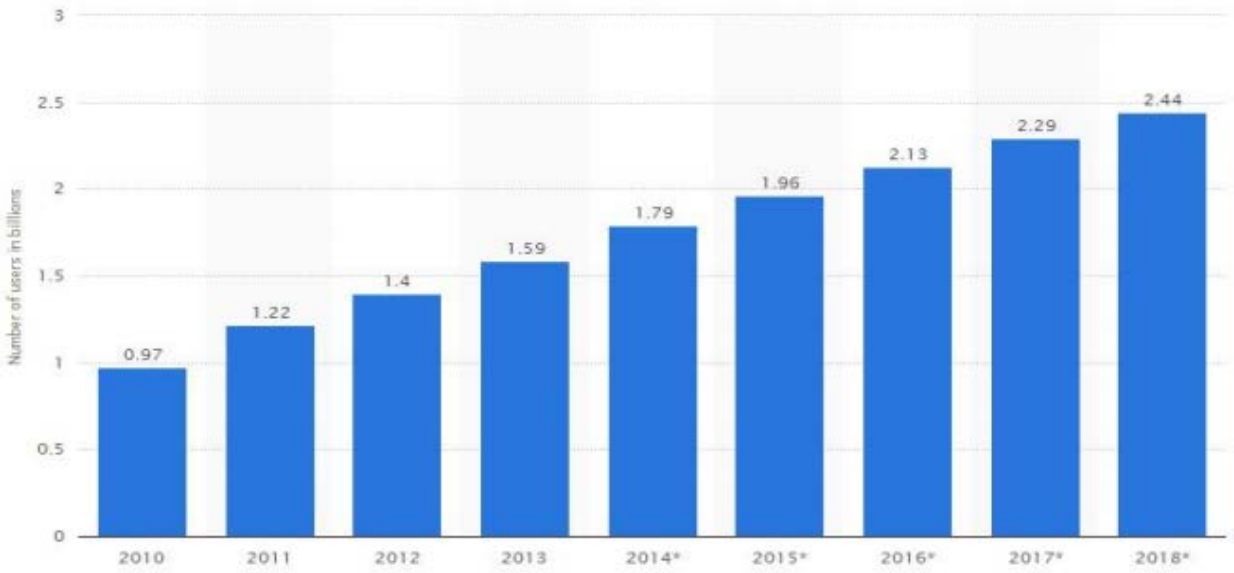

Figure 05: Number of worldwide social network users 2010-2018
(Source: http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/)

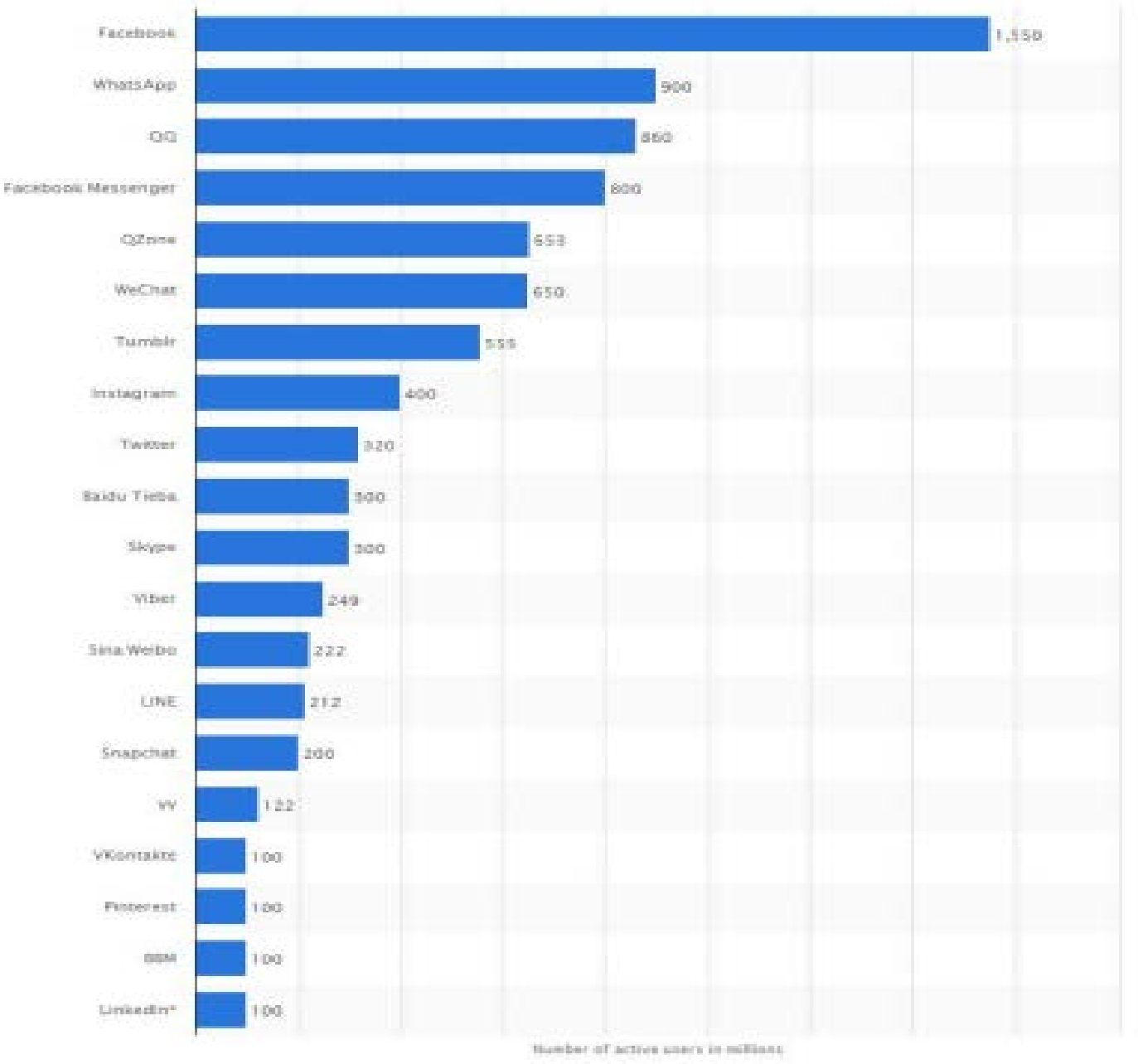

Figure 06: Leading global social networks 2016
(Source: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/)

Appendix B:

Table 02: Literature Review comparison

Functions	Analyzing the social media content	Examine the hypotheses and proposition developed	Investigate key security vulnerabilities eroding	Security policies guidelines	Explores countermeasures Undertaken to stem ensuing risk	Produce controlling rumors propagation model	Biometrics Verification Techniques	Symmetric Key Encryption	Use of security protocols	Use algorithms to create social network security
Research										
The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. [1]	√	X	X	X	X	X	X	X	X	X
User awareness of social media security: The public sector framework. [2]	X	√	X	X	X	X	X	X	X	X
A New Social Media Security Model (SMSM). [3]	X	X	√	X	X	X	X	X	√	X
Social media security policies: guidelines for organizations. [4]	X	X	X	√	X	X	X	X	X	X
Countering Social Engineering through Social Media: An Enterprise Security Perspective. [5]	X	X	X	√	√	X	X	X	X	X
Security Model to Control on Social Media using Visualization and Forensic Approach. [6]	√	X	X	X	X	√	X	X	X	X
Security Management: Real versus Perceived Risk of Commercial Exploitation of Social Media Personal Data [7]	X	X	X	X	√	X	X	X	X	X
A robust finger print based two-server authentication and key exchange system[8]	X	X	X	X	X	X	√	X	X	X
Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System [9]	X	X	X	X	X	X	√	X	X	X
Symmetric Key Encryption Technique: A Cellular Automata based Approach. [10]	X	X	X	X	X	X	X	√	X	√
Social Networking Sites and Their Security Issues. [11]	X	X	X	X	X	X	X	X	√	X
Estimating the sentiment of social media content for security informatics applications [12]	X	X	X	X	X	X	X	X	X	√
Online Social Media Networking and Assessing Its Security Risks [13]	X	X	X	X	X	X	X	X	X	√
Security Policy and Social Media Use. [14]	X	X	X	√	X	X	X	X	X	X
Security and Privacy in an Online World [15]	X	X	X	√	X	X	X	X	X	X
Biometric Social Secure	√	X	X	√	√	√	√	√	√	√