DOI: https://doi.org/10.46632/daai/2/6/10

Data Analytics and Artificial Intelligence

Vol: 2(6), 2022

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

Digital Security & Social Networks

C Kalpana

S.S.T College of Arts & Commerce, Maharashtra, India

*Corresponding Author's Email: rkalpz@gmail.com

Abstract: Social networks are of utmost popularity in current era. People from various age groups are part of them as it attracts the user and totally engage them. As most of the social networks are publicly available for everyone, digital security is being compromised due to careless use of it. There arises number of vulnerabilities of threats which mostly the user is not aware of. These vulnerabilities could be addressed by possible counter measures. This paper is a comprehensive study on social networks, possible attacks on digital data and various security measures that user should adopt to protect his identity and information on social networks. Answers to general question of "What to share?", "how much to share" and "how is being shared?" are being discussed that will give necessary awareness to the non- professional user to be in social network smartly; in secure and protected environment as before.

Keywords — social media; digital security; social network; privacy; security; network.

1. INTRODUCTION

Social networking has become need of today's life. It seems that a person can forget to breath but doesn't forget to check notifications from various social media accounts. This is the way to connect various people from different background, cultures, nationalities, domains, age groups, gender and many more which seems impossible if not have existence of social networking. This is giving chance to socially be close with each other and also find much more of your interest under the common platform. [1].

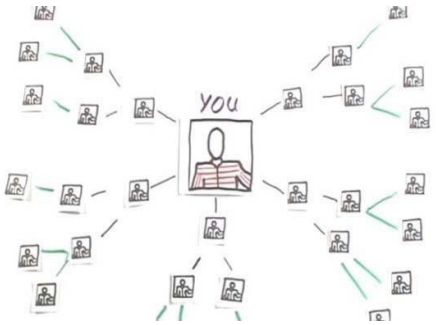

FIGURE 1: Connecting People through Social networking

Social Media: social media and social networking are used side by side to represent any activity socially using electronic medium. Social media is used as a tool to convert your thought, idea, message, or any other kind of information to set of audience or broadly. In social networking, people do engage themselves in some network like group, any site or in application and make a kind of network of people to communicate with each other and make relationships [2]. Social Networking platforms: As it is stated, social media and social networking are interlinked, so this can be at various platforms with the usage of applications or through simple websites. This is the era of mobility. So there exists more than one way to approach any social networking tool or social media website. Like Facebook can be accessed through website, through mobile application using any kind of computing device such as laptop, desktop computer, mobile, handheld device etc. Also, they are being designed in such a friendly style that it doesn't require any kind of training to use it. It enhances its usage by all age groups and from diverse background. Following (Fig.2) is the data collected from www.statista.com representing number of social media in billions from 2010 to 2021(Expected) [3] .

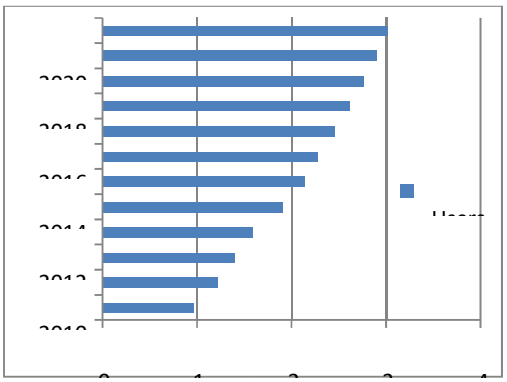

FIGURE 2. Number of Social media users worldwide

So, from year 2010 to year 2018, no of social media users have tremendously increased and same trend is being followed from the very beginning of social media intrusion in the open market for public and common users. This is stating its popularity.

TABLE 1: NUMBER OF SOCIAL MEDIA USERS WORLDWIDE

Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Users in billions	0.97	1.22	1.4	1.59	1.91	2.14	2.28	2.46	2.62	2.77	2.9	3.02

TABLE 2: ACTIVE USERS OF SOCIAL NETWORKING

Social Medium	**Active Users in millions**
Facebook	2234
YouTube	1900
WatsApp	1500
Facebook Messenger	1300
Wechat	1058
Instagram	1000
QQ	803
Qzone	548
TikTok	500
Sina Weibo	431
Twitter	335
Reddit	330
LinkedIn	303
Baidu Tieba	300
Skype	300
Snapchat	291
Viber	260
Pinterest	250
Line	203
Telegram	200

Digital security: Digital security is the security of distal contents like text, pictures, video, audio and many more [4]. Digital contents sharing over social networking sites has become the emerging trend of today's life [5, 6]. management of digital contents is crucial as the user is relying on trustworthiness that the network provides and rely on their security claims too. So, if anything is going to be public, it must remain secure enough not only authentically, but also resist attacks, vulnerabilities and threats to your digital contents too [7]. Attacks on social media: There can be variety of attacks on social media and social networking portals. Here a brief description of attacks is being given. Identify Theft: It causes the

attacker to control the victim's profile and the n misuse it for his own unauthorized use. Spam attack: It makes attacker to capture information of the user and then send spam messages or data. Aim is to build network congestion and to consume maximum bandwidth which can lead to bottle neck too as sometimes complete unavailability of the legitimate information of the user, as well. Malware attacks: They are the most common attacks that cause unauthorized access to the legitimate user device. Attacker can send URL or any image and text that contain malware. If user clicks on that link, malware will be installed on that device. Malware could be virus or a worm which will have propagating feature and will badly affect the computer in terms of performance, and efficiency. Sybil attacks: In Sybil attacks, fake profiles are mostly used that can be used for spreading fake, junk or unauthentic information. Even messages containing viruses or worms can also be spread with these attacks. Phishing: Here, attacker targets sensitive information of the user through any source like fake website, but for user, that fake website or email seems to be authentic. Like employee can receive any request data from another employee of the same organization, first employee doesn't know second employee but as used the fake information of the organization, can open the information sent by him and could become the victim of the attacker. Impersonation: Attacker can target a particular user and create fake profile to show him as authentic and real user. It is very common attack in social media that not only affect the privacy of the user but also spoils contact list that the user have by sending unethical messages, images etc. Hijacking: Hijacking is a kind of adverse attack that enable attacker to take complete control on user's profile. This is mainly possible because of taking access to authentication details by any source. Password could be guessed too if any particular user is targeted, and attacker knows that person as normally we choose password that are not strong enough and based on some personal information. So there is more possibility of hijacking the account authorization details and become the victim of the attack. Fake Requests: User has the attack of fake requests that are being sent by the attacker repeatedly with aim to screw the privacy of the user. If user accepts the request, the attacker will have the chance to view personal information, networks and sometimes other contacts too. So opening room, for further attacks, by fake requests and effect the privacy and security of the users. Image Retrieval and analysts is advanced attack that enables the attacker to use various kinds of software for face recognition and image recognition, speech recognition and processing. Images could be collected from the target and then use them for various unethical causes that badly affect the privacy of the user as well as poor impact on social circle too. Data of each usage of social media is directly related to the vulnerability of threat. That's the reason it is really important to know that what are popular usage among social media and what I is trend in last years. This is represented in following Fig.3.

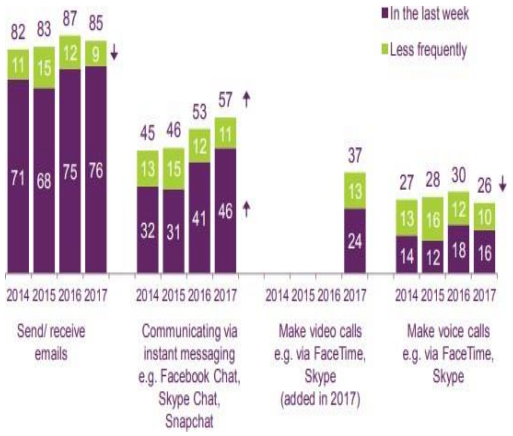

FIGURE 3. Data of social media usage (Data is collected from Research Report 2017 of Com)

2. BACKGROUND

Ali Dorri [8] has well-elaborated security of smart homes by taking one mechanism of BLOCK chain that work in IoT. This is a continuation of previous work of the authors on Blockchain and IoT. For designing BC smart home, complete process is being explained in terms of initialization, handing of transactions through miner and shared overlay Three main demanding aspects of smart homes are discussed; security, privacy and performance that we are also targeting in this paper and implementing it on social media. For any system to secure it must accomplish confidentiality, integrity and availability [9]. Block chain is one way to implement security to secure digital data. In [10], focus is on security of IoT and to implement it, concept of consumer security index is being introduced. This is the work of the project where requirements have been gathered using Study approaches. Four Study methods have been conducted and for each Study, aim, used methods/design, analysis are well elaborated. This introduces new idea to implement any security measure on digital data through study approaches, same as discussed in [10]. MAC layer attack can be at wireless interface, hardware, software, on sensor input

and on infrastructure. Jamming attack is very common that can cause denial of service. Node targeted flooding can happen. Data could be manipulated at sensor input to mislead the readings. It can lead to random number generation tempering. Replay messages can be generated. It can lead to spoofing, man in middle and timing attack as well. DoS and sensor input data is being targeted the most under MAC layer attack. It causes bandwidth consumption too to produce latency. Overall confidentiality, integrity, authenticity, and network availability is being compromised as result of MAC layer attacks [11]. Router is a device that works in layer 3 of OSI model and its main job is routing. Attacks at routing layer can affect routing by intrusion of wrong information of paths and misguiding in packet forwarding. Attacks at this layer can be denial of service, denial of node, man in the middle to create falsified information, spoofing, emerging spam messages, and attack on reading of sensor input data, jamming, malware, blackhole, greyhole, wormhole, replay, timing, unauthorized access and change in information of data [12]. It main targets at hardware, software level by either by spoofing or by intrusion of malicious entity either as a node or as outside attacker to create wrong information about route, drop any packet, act of malicious node like the original node, replay to the old messages, controlling the routing and effecting the network by any mean. This can cause consumption of bandwidth, congestion of data pockets and even could fail the complete network as well as routing is one of the basic functions of wireless networks [13]. Security is being implemented using three approaches: using security infrastructure, with security architecture and with the help of security standards. All three measures complement each other as infrastructure will help to design architecture and architecture will have set of standards to implement. [14] For security infrastructure, concept of PKI exists that work with certificate authority CA to implement security. Based on PKI, many security architectures are being adopted by various originations to deal with security issues within their scope. ETSI has introduced security for ITS communication using ETS architectural layers [15]. NHTSA has introduced security architecture using basic safety messages and security information messages based on bootstrap functions and pseudonym functions. This architecture appears more secure as compared to others. Without standards and protocols, security cannot be implemented at all and more research is proceeding in this area to come up with more secure algorithms, standards and practices for network [16]. Support of cryptographic algorithm, routing protocol and certification authority together set the security of the network along with other optional security measures like data verification, detection rates, and involvement of specific authority, formal group formation, and location, architecture and individual access rights of a node within the network. So whatever security approach is used, focus is to avoid attack by targeting vulnerable threats available in the network and don't leave any loop hole for the attacker to intrude in the network and harm it with his malicious efforts, activities and actions [17]. Attacks are categorized into four sections in [18]; vulnerability of attack using wireless interface, attacks because of hardware or software, attack on

Category	Attack	Description
Using wireless interface	Location Tracking	Attacker locates the location of the user.
	Denial of Service	Attacker attacks to make services unavailable for the user.
	Distributed Denial of Service	Attack like DoS but in distributed way; from different locations.
	Sybil	Using same identity, multiple accounts will be created.
	Malware	Attacker consumes network bandwidth by sending spam messages.
	Spam	Spam messages are sent in the network to consume bandwidth.
	Man in Middle	Middle malicious node has access to the communication in between two devices.
	Brute Force	Attacker uses trial and error approach to get access to password, identity or any protected data.
Using hardware or software	Spoofing & Forgery	Injection of wrong emergency warning messages for the user.
	GPS Spoofing	Attacks to the GPS to mislead the network by wrong locations.
	Message change	Attacker either drops the packet or changes the contents of the packet.
	Replay	Reply to the old messages to mislead the network.
	Message injection	Attacker injects intentionally false information.
	Tampering hardware	Attacker tries to tamper the hardware.
	Routing	Attacker disturbs the routing by targeting network layer.

TABLE 3:

	Timing	Play with the time to delay the message so that should be received in the network when it is no more required.
Attack to sensor input	Illusion	Attack on the sensors to read wrong sensor readings.
	Jamming	Attacker attacks on radio frequencies to create jam.
Infrastructure attacks	unauthorized access	Unauthorized access deals with malicious access to any node, service or network by any mean. During session hijack, attacker takes control of the session after authentication and controls the session in its own way.
	repudiation	During Repudiation, event traceability is loosed that leads to denial of node in the network.

CATEGORIES OF ATTACKS WITH ATTACK TYPE AND DESCRIPTION

sensor input and attack on infrastructure. Each attack has further subcategories and is targeting any particular feature(s) depending upon the user's vulnerability as mentioned in table below:

3. ANALYSIS

As per all the attacks discussed in section 2, here we will propose different security measures that we need while using social media. Security can be implemented on:

- Images
- Text
- Passwords
- Location
- General measures

Image Security: First we will start with different options to secure images that we do share on social media. Images can be misused, with or without editing. Watermarking: Digital watermarking is the most wide used approach to protect the image authorization, identity and integrity. [19] Image can be watermarked as copyright or with user's name or any other statement that can prevent its modification by any other user. [20] Digital watermarking fulfills robustness, resistance, security, modification, and imperceptibility. Also multiple watermarks could be inserted to make the security stronger and complex so that any other common user can't break it [21, 22]. Stangeography and watermark encoding: Images used for high secure communication uses stangeography and encryption techniques. These techniques are not used by common man, but mainly by government and military agencies. Stangeography is used to hide any information under the image layers and with advanced image processing tools; it is complex mechanism to break its security. Different filters, pixels, coordinates are modified using gray scale as well as on colored images using image processing software like Matlab. This makes not only the image secure but also ensures confidentiality of the message hidden inside it [23]. Watermark can be encoded using same techniques that we use for encoding text. If water mark is having text along with digital signature attached to it, this is the most successful security implication on the image. That approach too should be used where high security of images is required. Signature verification will assure that image has arrived from the same sender and is not being altered too. It means integrity, confidentiality and authorization are ensured [24].Text security: Text security for simple user is to only follow official accounts, trust only the membershe knows and don' share private information with anyone. For high security, messages can be encrypted using cipher, with any key, with hash code, message authentication code and signature. Digital signature is the most secure method in all. Digital signature: One can deny the signature on a hard document but denying digital signature is impossible. For any text to be digitally signed there should be strong communication channel to share private key as the text will be signed using private key of the sender. Then the same text could be decrypted using public key corresponding to the sender's private key. There is involvement of public key infrastructure too which ensures the successful completion of the process [25]. Passwords protection: Passwords should be secure enough to implement user's security on social media. Here this feature lacks in social media websites as there is not any measure to make the password strong which will make efforts of the attacker harder to break it. We strongly recommend implementing security features on the password so that user should use different combination of text, numbers, and alphabets to set the passwords. Also passwords should be long enough that it should resist brute force attack. Most of us use easy to remember passwords that contain some personal or family information like name, age, phone number etc. This should be strongly avoided. Passwords should not be easily guessable, and we need to be smart while choosing any password. Also we should not use same password for all social media accounts. This also, opens door for the attacker, to easily guess the password. Location: Showing location every time to the public is not suitable approach; each social media

website has implementation of global positioning system to show location of the user. This is beneficial if you have set the privacy in your account or make your account private. It means you will share with only those people who you do trust. Being a public account, location sharing is not advisable for common user as it can lead to hardware, software and wireless interface attacks on the user application. General measures: As a general user, we need to be careful while suing social media. First privacy is being set at account setting itself, so we need to restrict our circle as much as possible to add only those people who are trustworthy. Password should be strong and should not be publically informed to friend's circle. Accounts should not be opened from different machines as they will save the authorization details through cookies and could be used by attacker to misuse account details. Messages, mails and requests from unknown sender should not be opened. If any message contains attachment, it must go through security scan which is already being provided by social media websites. These are small steps, but together implementing them can make you safe and secure in social media.

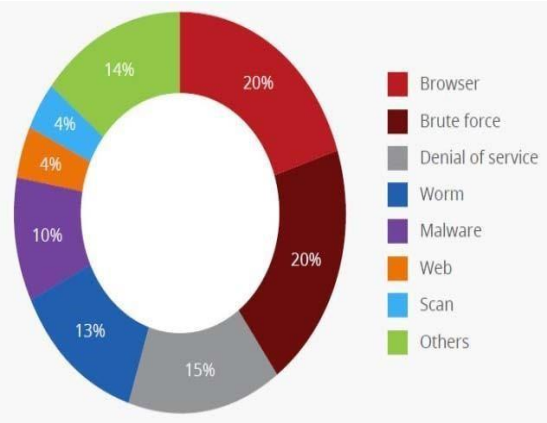

Fig.4. Data of Social media attacks (Data obtained by Mcfee lab 2017)

4. DISCUSSION AND CONCLUSION

Social media is used by diverse age groups, but it is more commonly used by adults and females. In social networking, main concern is to protect user's security and privacy. This can be achieved by awareness to the common user about privacy options, with use of counter measures and adapting various security tools. Also be aware of your circle of the network, user should not trust everyone and put his identity in danger. User should be careful about what he is sharing. If anything needs to be labeled by his own name or identity, then various technologies like digital watermark and digital sign should be used with un- editable format so that any attacker could not miss use it. Being in a social network is making you socially connected. So this drives the privacy settings of each network too that how information, passwords, identities and profiles can be socially protected. For passwords strength, still various social networks re not having strong policies and we recommend that it should be implemented to force the user to choose stronger password that should not be easily guessed or broken by brute force approach. Strong passwords strengthen the security and could prevent many of the discussed attacks on social media. Also, user has to be careful about browser, device, network and interconnected devices. Strong anti- malware software could protect digital security by detecting the threat in social network. Still ultimate responsibility is of the user. This paper is contributing to make user aware about various security threats on digital data, and how they can be tackled by various security measures. Users other than computer background too can be benefitted by the proposed counter measures and implementing them as being an active participant of the social network.

Acknowledgment: The authors would like to thank King Khalid University of Saudi Arabia for supporting this research under the grant number R.G.P.2/7/38.

REFERENCE

[1]. A. Doha, N. Elnahla, and L. McShane, "Social commerce as social networking," J. Retail. Consum. Serv., vol. 47, pp. 307–321, Mar. 2019.

[2]. Weaver, A.C, Social Networking, Computer (Long Beach, Calif.) ISSN: 0018-9162 Date: 02/01/2008 Volume: 41, Issue:

[3]. 2, Page: 97-100, DOI: 10.1109/ MC.2008.61, IEEE Enterprise

[4]. Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," Futur. Gener. Comput. Syst., vol. 86, pp. 914–925, Sep. 2018.

[5]. W. F. Hsieh and P. Y. Lin, "Analyze the digital watermarking security demands for the facebook website," in Proceedings - 2012 6th International Conference on Genetic and Evolutionary Computing, ICGEC 2012, 2012.

[6]. R. Grimm, (2005). "A security analysis of business models for

[7]. Digital products," INDICARE. Retrieved from http://www.indicare.org/tiki-download_file.php?fileId=76, October 22, 2011.

[8]. S. H. Han, and Chu, C. H, "Content-based image authentication: Current status, issues, and challenges," International Journal of Information Security, vol. 9, pp. 19- 32, 2010.

[9]. P. Y. Lin, J. S. Lee, and C. C. Chang, "Dual digital watermarking for internet media based on hybrid strategies," Circuits and Systems for Video Technology, vol. 19, pp. 1169- 1177, 2009.

[10]. Ali Dorri_, Salil S. Kanhere _, Raja Jurdaky and Praveen

[11]. Gauravaramz, Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,, Conference Paper · March 2017 DOI: 10.1109/PERCOMW.2017.7917634

[12]. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[13]. J M Blythe*, SDJohnson*, The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices, March 2018, https://www.researchgate.net/publication/324088630.

[14]. R.Rajadurai, N.Jayalakshmi, "Vehicular network: properties, structure, challenges, attacks, solution for improving scalability and security", International Journal of Advance Research, IJOAR .org,Volume 1, Issue 3, March 2013.

[15]. N.K. Chauley, "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study", International Journal of Security and Its Applications vol.10, No.5 pp.261- 274, 2016.

[16]. H. Hasrouny, C. Bassil, A. Samhat, A. Laouiti, "Security Risk Analysis of a Trust model fzor Secure Group Leader-based communication in VANET", Second International Workshop on Vehicular Adhoc Networks for Smart Cities, IWVSC'2016.

[17]. R. Raiya, Sh. Gandhi, "Survey of Various Security Techniques in VANET", International Journal of Advanced Research in in computer Science and Software Engineering, Volume 4, Issue 6, June 2014 ETSI TS 102 867 V1.1.1- Security-Mapping for IEEE 1609.2

[18]. P. Caballero-Gil, "Security issues in VANET", available: http://cdn.intechopen.com/pdfs-wm/12879.pdf, 2011.

[19]. A.M. Malla, R.K. Sahu, "A Review on Vehicle to Vehicle Communication Protocols in VANETs", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[20]. H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," Veh. Commun., vol. 7, pp. 7–20, Jan. 2017.

[21]. D. R. Nicholson and C. S. Librarian, "Digital rights management and access to information: A developing country's perspective," Library and Information Science Research Electronic Journal, vol. 19, pp. 1-17, 2009.

[22]. C. K. Ramaiah, S. Foo, and H. P. Choo, (2006). "Trends in Electronic publishing." In H. S. Ching, P. W. T. Poon, & C. McNaught (Eds.), e-Learning and digital publishing, pp. 111- 131, Retrieved from SpringerLink database, October 18, 2011.

[23]. X. Y. Wang and H. Zhao, "A novel synchronization invariant Audio watermarking scheme based on DWT and DCT," IEEE Transactions on Signal Processing, vol. 54, pp. 4835-4840, 2006.

[24]. Z. Zhang, Q. Pei, J. Ma and L. Yang, "Security and trust in digital Rights management: A survey," International Journal of Network Security, vol. 9, pp. 247-263, 2009.

[25]. Analyze the Digital Watermarking Security Demands for the Facebook Website, Wei-Fan Hsieh, Pei-Yu Lin, 2012 Sixth International Conference on Genetic and Evolutionary Computing, 978-0-7695-4763-3/12 $26.00 © 2012 IEEE DOI 10.1109/ICGEC.2012.62, IEEE Computing Society

[26]. M. A. Qadir and I. Ahmad, "Digital text watermarking: Secure content delivery and data hiding in digital documents," IEEE Aerosp. Electron. Syst. Mag., 2006.

[27]. Junling Zhang, A Study on Application of Digital Signature Technology, 2010 International Conference on Networking and Digital Society, 978-1-4244-5161-6 ©20 1 0 IEEE

