IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 2, April 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Survey on Security Framework to Protect Against Social Network Threats

[1] V Divya; [2] Dr. Radhika K R

[1] Dept. of Information Science and Engineering, B.M.S. College of Engineering, Bengaluru, Karnataka, India

[2] Dept. of Information Science and Engineering, B.M.S. College of Engineering, Bengaluru, Karnataka, India

Abstract - We all can see that social media at present has developed very popularly everywhere. These social networking sites allow zillions of people to communicate with their friends located in different states and countries without any barriers. Confidentiality and safety on the online social network has become their main concern over the recent years. All though we have all the security strategies, awareness strategies, standards, and devices at present, people still face some unusual kind of risks or danger whenever sensitive information is shared online. The sudden boom in the Social media applications by its abundant users, has bought the attackers a different method of invasion opportunities for disclosing all the private information, for the virus management strategy facilities like firewall, Intrusion methods for Prevention, antimalware, and Data leakage methods of prevention. As its result, this paper tells us about the safety framework to shield the users by securing them by providing knowledge to counterattack the threats occurring due to Social networking sites. We will also be discussing about all the different kinds of crimes on the social media and provide methods and strategies to diminish the risks faced by the social media users.

Keywords - *Intrusion Prevention System, Social Networks Services ,Intrusion Prevention System, Personal Digital Assistants, Firewall, online social network*

1. Introduction

There are different network services like social media site where they set up a digital relation between the users who have the same kind of interests, history or lifestyles. A social networking site lets the users to discover new friends and grow their group of friends. One of the main features of Social Media is Data sharing where they can upload videotapes, images, events, different interests, and other multimedia content. The great volume of private data that people upload online creates a weak mission for the attackers. They get all the private subtle information about an individual, and for the employees who use business network to interact, interface, combine, and data access all their critical business documents is being spread into a bigger outer environment that is more dangerous and tough to guard. Due to the rise in smart mobiles and Private virtual Assistants and its outcome is the borderline within the company i.e. inside or outside the premises/company has been developed. People presently are seen working in cabs, café's and everywhere, wherever there is availability of internet connection, which is normal and common these days. Therefore all the company's private information can spread over an unprotected network and lose to protect equipment and private data. There are many dangerous cases and mistakes caused by staff members, while working outside the office environment like using illegal codes, abuse of company computers, unapproved OS layer access, abuse of users passwords and relocate private data between company's workstation and own computers when they are doing work from home. The Social Network provides facilities within the network and lets people to upload, innovative ideas, marketing, events, fest happening and other ideas of their interest. However the overall belief that we have on Facebook, Instagram, Twitter, LinkedIn, etc. provides a medium to commit a variety of illegal offensive attacks, such as violate into an organization system and information is leaked due to this act [23]. Firewall is a process of securing one network from another unprotected network; they are divided as categories, different substitution, examination or a mixture of them.

Prevention methods due to unusual interruption are like a network system security mechanism, where it observers system and network activities from harmful or unnecessary behavior and can be applied in real-time, to avoid such things without any disturbance. These Network prevention system works to observe jam in any

network for malignant nodes as well. Once any cyber-attack is noticed, it can leave the malignant data when its still allowing all other traffic to pass. These Online Social Networks are means where they let people to post or publish multimedia contents or other personal details about the user and to connect and communicate with other users of the same circle with same enthusiasm and activities through links. Lately, the popularity of social network is increasing undoubtedly.

For example, Twitter now says to have beyond 34 million active everyday users. Data that is shared on social media can be used against the user to launch various cyber-attacks as soon as he/she posts their details on social networking sites, which is not private anymore. As there is rise in the quantity of shared data of an individual which would boost the ways of data outbreak risks of an user. Cyber criminals are always one level above the crime police expert and internet police [24].

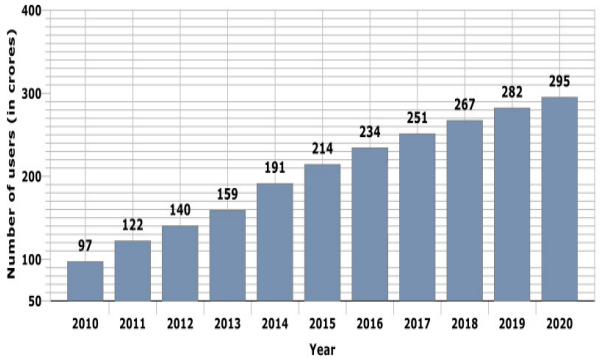

Fig 1: Number of social network users worldwide from 2010 to 2020

2. Security Threats in Social Network

Attacker always mistreats human exposure to execute different social engineering crimes. Here, they mislead the social network user by pretending to be from an authorized medium and gain from those attacks. Further we would be discussing about different threats that's been popularly happening over the social networking site for its users.

2.1 2.1 Traditional Threats

- **Phishing:** Starting off with Phishing invasion is an attack, here what happens is that the site appears to be like an authorized site but it's actually a fraud link and mails to trick the victim who would be revealing all sensitive information of the user. In this kind of cyber-attack the invader tries to dupe the original authorized page in such a way that the unauthenticated page appears as similar as a legitimate one. For example, what these attackers do to create the fake website is they copy the format and options on the bank website and next they paste in the editor tool and create the same fake bank link and link to the required address of login form, to his mentioned endpoint which is nothing but the attacker page gets all full details like the username and password and stores it.. These attacks are usually done through spam emails "sign in" pages, for example using Gmail, Facebook, twitter login pages.

- **Click-stealing:** Click-stealing is a threat that is been recently budding over the internet, here these attackers mask up the malignant unsafe tools in the background using users sensitive interfaces or they plan to press, these buttons as used by the users to rob the clicks of them for the attacker's wicked goals. Click-stealing is diverse, but the most popular in public eye currently are Like-stealing and Cursor stealing. In Like stealing, here invader partners with malicious code and test plans with Instagram's "Like" emoji, which displays on his/her profile feed. Cursor-stealing/cursor-fooling uses he users interlink between and reforms the process Cursor stealing where it modifies the current place of the cursor, where the intruder switches with an original real arrow with a fake cursor to reroute the user to a malignant link or site.

- **Replica of existing account*:*** In this cloning attack, the attacker creates a duplicate profile on an already created active user profile either in the same Social media site or on any another sites. With the help of this duplicate profile, the intruder would be sending a friend/follow requests to the other users of the official authenticated account and develop a trustworthy relationship with the victim's friends. The intruder may completely use this to collect private and delicate data about the victim's friends or plan various kinds of online fraud, such as cyber mistreatment, threats and cyber following,. The revengers clone the account and use the pictures of them and recreate the attacker's profile.

2.2 Multimedia content threats

- **Multimedia subject revelation:** Social media account holders are habitually precautious while disclosing textual information on social media. Hence, some people sync their personal details and house location. Although, they are not so while

uploading Hypermedia files data, they reveal a huge number of delicate instances, where an operator uploads images of his house, the attacker will discover the operator's house location because of their carelessness and lack of knowledge. Another example is when an individual updates his own status which is also referred to as 'story' these days on Social media platforms representing as the owner/victim is away from his house (for instance; a party, on a retreat, at a pub or a show), which indirectly tells that the house is empty and safe for the invader to launch an attack. A uploaded image from a latest update can show the current region or area of the home and till what time there will be out. All this info is guessed by them by seeing their activities and are ready to attack. People from their side should also be careful that attacker may be waiting to examine updated images for expensive properties/substances. Thus, precious details displayed or recorded in a videotape, pictures can mark for an unwanted attention for the attacker to notice. The other way of data exposure is when the user uploads or updates the images that consist of other friend or colleague irrespective to their consent, this may disturb their confidentiality. There are plenty of latest upgraded methods, like expression and dialogue identification, or left behind proofs which can disclose information about numerous folks without their knowledge.

- **Shared ownership:** Distributed photos and videos and other sensitive data onto Social network sites may connect to several users. For example, two folks might take a picture together at an occasion and either of them could share the pictures on the Social media without their confidentiality account/system set up and also without the permission or consent of the person looped which will disclose the secrecy of other pal such as an image of both of them. As they are only single user and they make a decision upon their preferred confidentiality settings for the mixed media files that are of many operators, which could be uploaded with the desired confidential framework that are chosen by the operator.

- **Metadata:** This is a kind of information that comprises and carries data about other files. In social networking sites, multimedia substance behaves as metadata. This data may or may not consist of a huge sum of precious private information, such as authentic details of a person and region of address. As this may be treasured by the owner, it may disclose the user to intrude, if it is exposed. One kind of multimedia metadata that could disclose owners'/ operator's area is one of the recent phone handsets introduced by the Global Positioning System in the mobile phones and manages in) the uploaded or photos clicked and posted, by this mobile reveals the area where he stays and other information of the person in the clicked image. This information of the user could also disclose the data about them, such as religious or ethical beliefs, health status or condition etc. Besides, location-tagged images may leak private information, for example, the Facebook eliminates all metadata beforehand sharing the photos, whereas Google+ holds all metadata other than the live location. Instagram reveals the GPS coordinates in a picture and evades displaying the photos of another person at the similar address.
- **Video conference:** In the present time, many social networking sites equally help in conferencing in text and live call facilities, as video conferencing can offer more interaction between the users. Due to this video calling, these extra unwanted details can be leaked. A malignant operator can interface the live video happening this can be misused with all the potential weaknesses. Also, the members of the live meeting in the conference or chat can effortlessly document to threaten them to deform the confidential information. The malignant operator can randomly use the webcam of the sufferer with the help of hacking they take benefits of these weaknesses attack through these means.

- **Linking futile with Tags – linking in social media sites: In** Social media one of the main feature is tagging your friends by sharing meme or trolls online. Due to this tagging facility online and also when a picture, video or audio is uploaded to collaborate with other social media users and to allow extra hunt skills. An uploader online can tag you in those videotape or image. They think it is connected to you and link you with malicious node along with this some extra information is also revealed. However this feature could lead to few confidential risks. There are some users who wouldn't like to share or upload image of their own on any Social media (Facebook, Instagram) site. Although, somebody in their friends circle can reveal or leak their photos through tagging and recognize them. The problem is that this can associate somebody who do have any account on

those social networking site and who usual don't prefer to share picture in public online. Similarly, a spammer online tag's huge number of inappropriate or targeted users in one post, like in a spam photo, adult video, to spread to huge number of victim, using this malignant content for its viewers with minimal struggle.

2.3 Social Threats

Cyberbullying and cyber-grooming
Cyberbullying: In this attack the threat is occurred intentionally and recurred as days go on here harassing users, abusing them through social Medias In Cyber-grooming the attacker tries to develop an emotional, friendly bond with a user, child or an adolescent to mistreat them sexually. Younger generations are extremely vulnerable to these kinds of hunters and outbreak due to the defenceless attitude, this can lead to misery in youngster. Attackers may try to trap a youngster by showing some pity, affection, attention, concern or by devoting time by communicating and presenting them presents online, money, etc. Many online safety experts think that attackers have tried to fraud on several of school children all around the map. A similar case, where it is one of most critical crime filed was of a young girl case, which led the girl committing suicide.

- **Corporate espionage***:* In this attack what they do is using social engineering through Social network. A social engineer can collect prized details of the staff, things like a staff's status inside an organization, addresses of the employees like home address and mail ID, Surnames along with first and second name, etc. instead of using social engineering methods we can use social network for getting into organization details. The writers presented the workers data within the targeted company through from network which will be deliberately misused for using social engineering trick.
- **Virtual Pestering***:* virtual pestering is where an Social network user can reveal their private information for example their mobile contact number, education, college/company, interests, many other location details of where they stay ,etc. by means of their Social media account. Using these data it could be misused and attacked for the purpose of cyberstalking crime. For example, an attacker can threat their target by calling them or texting through online (chatting). Besides, they regularly disclose address, regional details using their picture and intruders can collect these details and misuse to plan these hazardous attacks.
- **Financial Threats***:* One of the most frequent and recurring threat that's happening every other day is the financial threat on social network and different platforms, here the hackers gain the bank details of the victim, and misuses it by accessing there bank details and withdrawing cash which is financial gain . this attack is done for the opposing company/organization as well, by stealing all the details associated data to gain financial benefit by opposing organization to create loss for them.

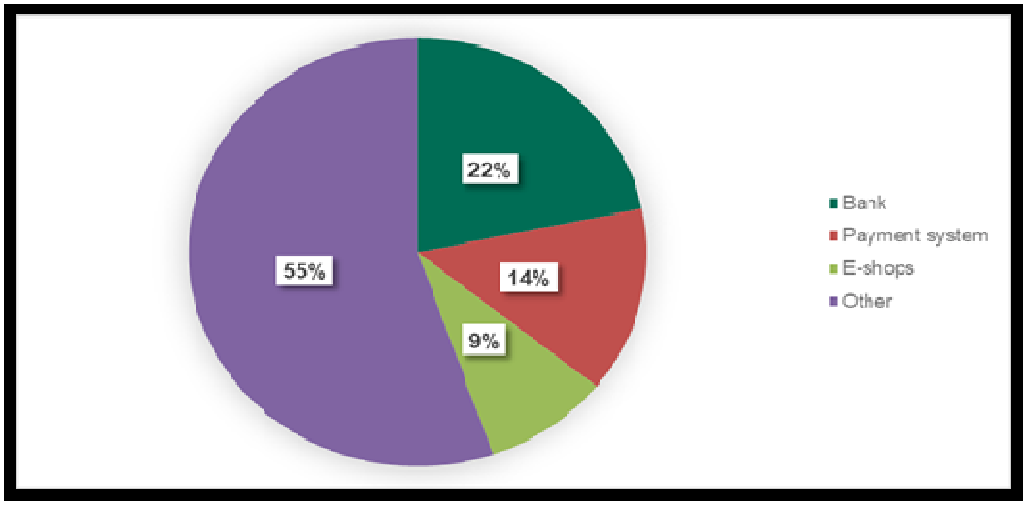

Fig 2: Financial threats statistics in India

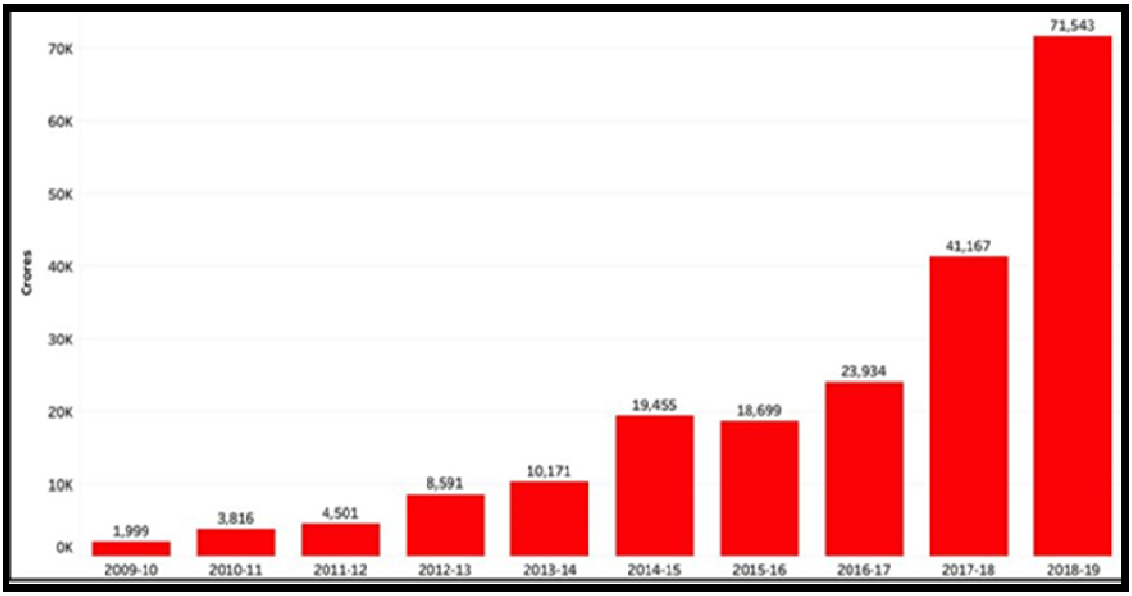

Fig 2.1 Graphical representation of Financial threats in India till 2019

3. Study of Social Network Security Solutions

Table 1: Social network security solutions, description, key methods and relate studies

Solution	Description	Key methods
Storage encryption	Storage encryption allows SNSs users to efficiently store and recover their data on SNSs without exposing any data to the third party service provider Such as cloud service providers.	Cryptographic techniques, Various encryption schemes for cloud storage such as attribute-based encryption, proxy re-encryption. Various techniques for Encryption of multimedia data.
Metadata removal and security	This solution provides various approaches for metadata removal and for mitigating the metadata privacy leakage in SNSs.	Various methods for editing metadata in multimedia file, Encryption of multimedia metadata, Anonymous messaging platform.
Malware detection	Malware detection includes various mechanisms to detect malware propagation in SNSs.	Identification of graph parameters, Machine learning technique, Maximum coverage algorithm, Various server-oriented and user-oriented defense mechanisms, Several Malware prevention rules.
Sybil defense and fake profile detection	Recently, many security researchers have developed tools and techniques to detect fake profiles and defense against Sybil attacks. Most of the techniques either rely on performing a limited amount of arbitrary walks within the social graphs or the concept of random routes.	Network topology analysis, Sybil Defender, Sybil Frame, Sybil Limit, Sybil Guard, Gate Keeper Sybil Infer, Bayesian inference method.
Phishing detection	It includes various anti-phishing methods to detect and prevent phishing attacks in SNSs.	Machine learning technique, PhishAri technique, Warning Bird system, Two-phase Unsupervised learning algorithm.

Table1.1: Social network security and its relate research

Solution	Description	Key methods
Spammer detection	The fundamental concept of the existing approaches for spammer detection in SNSs is to extract a feature set that separate spam users from legitimate ones and supply that feature set into different machine learning classifier models for identifying inappropriate activities.	Machine learning technique, Social honeypot based approach, Data-mining based technique, General activity detection clustering algorithm, Supervised matrix factorization technique, Latent dirichlet allocation model.
Commercial solutions	Commercial solutions include various security products which have been developed by several security companies to protect SNSs users Against security threats.	FB phishing protector, Social guard privacy scan, Net nanny social, Minor monitor, Web security software, Social protection application.
Built-in SNS security solutions	Many SNSs provide various in-built security solutions such as user privacy settings, authorization mechanisms, Report abusive content.	Multi-factor authentication, Photos-of-friends identification, CAPTCHA, Two Factor authentication, Facebook immune System.
Profile cloning detection	Many SNSs such as Facebook are currently developing a feature that automatically detects cloned profile and notifies their users about such Profile.	Face recognition technology, Clone Spotte system.

- **Different commercial classification for Social network security**

Table 1.3: Various commercial Solution for Social network security

Manufacturer	Product	Key features	Pricing	Platform
Diego Casorran	FB Phishing Protector	Uses as Firefox add-on to protect Facebook users against phishing attacks.	Free	Firefox add-on
Check Point	Social Guard Privacy Scan	Identifies privacy concerns in Facebook user's profile by scanning recent activities of the user's profile.	Free	Facebook application
Net Nanny	Net Nanny Social	Helps parents to protect their children from SNSs risks such as online predators, cyber bullying, and Pornography.	Paid software	Personal computer and smart phone
Info glide	Minor Monitor	Provides parents an easy and quick dashboard view of Facebook Activities of their kids.	Free	Web service
Several security corporations such as Symantec, McAfee, Panda, Kaspersky	Web Security Software	Involves firewall, IDS, anti-virus and other protection software which help SNSs users in protecting their personal computer against risks such as phishing, clickjacking, and Malware.	Free for trail period and paid for licensing	Personal computer
McAfee	Social Protection Application	Helps Facebook users to manage and Control the privacy of their photos.	Free	Android device

4. Social Network Protection Mechanism

As Social Network is a main source for Data loss, it is doubtful to provide complete safety in any sort of strategies. It would be significant or very important to discuss and ask them to be aware of social network. Also these account holders need to be given some knowledge about it and how to keep the information safely without letting it out by themselves.
Organize public gathering for discussing about awareness program is very important attempt for reducing crime. All these planned techniques should eventually benefit the users.

4.1 Data Loss Prevention System

In this prevention system we will be discussing about the protection for data theft. As we know information is lost in many ways, say like the customer details, Protocols and other strategies are all transferred to the competitor then usually this happens deliberately it is very rare that happens accidently, this can be happened by the employees or another staff members of the accidents which consist of private information copyrights, intellectual property or the project information and its strategies are all leaked. This is actually an act of violation of the organization rules and regulation.

The main three paths of the data loss in an organization are as follows
• Moving Information between the networks via internet like when they upload any information on social network

• Resting Information or the data that stays is stored in the database in storage platform

• End traces of Information within the network inside the MP3 player, devices, and drives/disc

Organization should classify them only for sorting out which data should be put out and which should be saved safely using the policies of the company.
The below figure describes the prevention methods to gear up and control the files that are moving outside.

4.2 Protection Strategies

Lately many information security protocols are examined and inform them by giving awareness program through social network by snooping in the users personal data.

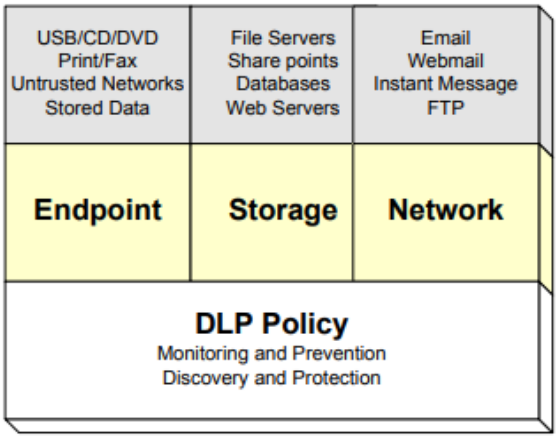

Fig 3: Data Loss Prevention system model

Encryption can be used to protect communication networks in a much unsophisticated method, this means that the conversation among the users and the social network uses encipher method, for instance Hypertext Transfer Protocol Secure to secure against snooping. Although, this is from a technical perspective simple, comfortably applicable and willingly available secure instrument is not broadly used by most of the Social networking site.

- For security, Information can be split by dividing the amount of information stored at the social media. All publicly accessible data can be saved at the Social networking sites, while personal and sensitive data could be saved at a mediator, for instance, the computer of the operator, a loyal third party, or an untrusted third party. To secure the data at the distrusted third party, encryption can be used to allow secretive or well grained access controls.

- Fake data, giving fake data online instead or your real details can be an added level of security against curious social networking users or peripheral adversaries. The social network only examines the false data, while maybe verified and sensitive data is saved encrypted on a third party server. As a source for fake data either predefined dictionary or dynamic content from the Internet may be used. This secures naive attempts for identifying the fake data.

- Stenography is generally where it is attempted by inserting the photo or video which consists of sensitive/private information is hidden or keeps it invisible this way the data is protected from leakage

5. Framework

In order to tackle the crime that's occurring in these days through social network using protocols, designs are all well examined and they are registered to be safe and accepted to be accurate. Hence lets focus on the crime happening and how to deal with it in spite of being active on social network.

Organization Assessment: Starting of the framework with the Business assessment where the design is necessary, and it also necessary to the situation of the organization internal and external situation what can meaningfully lead the agenda. Let me begin with internal framework ,it consists but then not constrained to the protocols, values, principals, morals, data system, data movements, result formulation procedure and other source and information are available. Company values are a usual approaches and policies, principles at a joint stage having knowledge and understand the performance.

Next coming to the external situation consists it but not retrained to I values, governmental, research, interviews, lawful, rules and regulation, investigate, experimenting using the apparatus to comprehend the company's situation these two play a crucial roles in the model of framework.

Safety Rule: The safety strategy should touch all the problems associated with Social network seeing precise rules such, Data which authenticates users identity shouldn't be uploaded to Facebook, Instagram and other social media websites, which includes house location, birthdays and DL,. Similarly, information of mission to be done or published online to any journal or conference shouldn't be submitted to other websites or other unauthenticated sites as these files consist of private details, holiday spots they visited, and other plans which have been implemented. All the data categorisation protocols is basically a perfect process to deliver procedure for the staffs to know all the delicate information and familiarize and be very familiar to those data to safeguard them. One of the important form to support the framework is improvement towards it, though It's not mandatory.

Social media sites research: Knowing staff's choice and behaviour in the Social network is the most accomplishing feature for making the framework successful. All these awareness plans and study of the media research can be done through internet, VPN, or through "any desk" application by providing knowledge to them through these means by filling the forms to participate in it.

Duties and Supply: The person assigned in the office for this job must clearly explain the complete process like

"When, Where, What, Who", for example, all HR in the organization is accountable of alertness procedure. In this process we must take suitable employees like who are talented, skilled, educated, experienced, good in budget maintenance lacking these qualities in any staff is a very big risk and dangerous step for following the framework.

Alertness Plan: As mentioned above, all the techniques mentioned used to educate about data safety methods is required to provide knowledge to the staffs, the cyber-attacks happening and how to overcome them by tackling it, the study is a base to frame the alertness protocols to proceed. Agenda Involves matters like risk and methods to protect in social network One of the main plans to the protocol is the alertness plan which reduces drastic amount of crimes occurring all over the world.

Additional Organization procedure: In the entire Organisation a separate team for Data Security is necessary and they have to be implanted in all firewalls of the business plan which gives additional security which is very effective as well. This procedure must be the main part of the strategic plan in the security program and framework which stays on mark till the date and provides a better design for new programs of the business for recruiting new workers.

6. Conclusion

Within this survey paper we have studied and discussed about Social network and its threats and how they have impacted in all our lives by connecting zillions of users all over the world by which is a platform allowing users to explore ones interests, pictures, videotapes, video call , chat online with their digital friends without any distance barrier. Although, having all facilities would lead to dangerous cyber security risks. Moreover, we have discussed about all the major threats happing and divided the threats into three categories describing three classes of threats: Social media threats, Multimedia content threats, and Traditional threats, that, we examined and discussed about and current plans and protocols for providing safety for Social network operators. In this paper we provide kinds of threats, attack, prevention strategies, and other precautions while using social media. As we know the amount of attacks that is occurring worldwide is increasing day by day over the five years which needs to be controlled .We have also used methods of prevention system using

four subcategories which is discussed in the paper also Stenography may be used in mixture with any of the other subcategories, to further expand stealthiest. The suggested framework acknowledges the familiar and provides awareness about the threats which have not been identified and minimise the safety threats that ascend mixture of organization of Social network.

Future Work

The future work should be done to improve the present methods of prevention and provide more accurate results for the prevention mechanism in the field of Social network security and also investigate methods of automation in security for the companies or organization which can eventually lead automated security system to the social media as well, Additionally we can evaluate and reduce the effects of the information loss issue and its prevention mechanism for improvising it more accurately.

References

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

[2] Zhang , W. Xu , F, S. Zhu , Toward worm detection in online social networks, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACM, 2010, pp. 11–20

[3] IEEE,2012,pp.1–12,Rajadesingan.A Kumaraguru p ,Aggarwal A,PhishAri: automatic realtime phishing detection on twitter, in: eCrime

[4] Martino , P. Savla Content analysis of privacy policies for health social networks, in: Proceedings of the International Symposium on Policies for Distributed Systems and Networks (POLICY), IEEE, 2012, pp. 94–101

[5] ACM, 2013, pp. 75–88I. Spiro , M. Tierney , C.Bregler , L. Subramanian , Cryptogram: photo privacy for online social media, in: Proceedings of the first ACM conference on Online social networks,.

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

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

[7] (2016) 582–594 P. Kairouz , G. Fanti , S. Oh , K. Ramchandran , P. Viswanath , Metadata-conscious anonymous messaging, IEEE Trans. Signal Inf. Process. Netw. 2 (4)

[8] G. Fanti , P. Kairouz , S. Oh , K. Ramchandran , P. Viswanath , Metadata-conscious anonymous messaging, IEEE Trans. Signal Inf. Process. Netw. 2 (4) (2016) 582–594 .

[9] G. Yan , G. Chen , S. Eidenbenz , N. Li , Malware propagation in online social networks: nature, dynamics, and defense implications, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 196–206

[10] H. Zhu , C. Huang , H. Li , MPPM: Malware propagation and prevention model in online SNS, in: IEEE International Conference on Communications Workshops (ICC), IEEE, 2014, pp. 6 82–6 87

[11] G. Wang , F. Musau , S. Guo , M.B. Abdullahi , Neighbor similarity trust against sybil attack in P2P e-commerce, Trans. Parallel Distrib. Syst. 26 (3) (2015) 824–833

[12] Cao , Q. Li , Y. Ji , Y. He , D. Guo , Detection of forwarding-based malicious urls in online social networks, Int. J. Parallel Program 44 (1) (2016) 163–180

[13] A.Y. Varjani , M. Moghimi New rule-based phishing detection method, Expert Syst. Appl. 53 (2016) 231–242

[14] J. Kim , S. Lee ,Warningbird: a near real-time detection system for suspicious urls in twitter stream, IEEE Trans. Dependable Secure Comput. 10 (3) (2017) 183–195

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

[16] ,(https://www.facebook.com/games/sgprivacy/)Check Point Software, Social Guard Privacy Scan. Online; accessed 04 April 2017

[17] Infoglide, Minor monitor—Facebook Monitoring and Parental Control Software, (http://www.minormonitor.com/) . Online; accessed 04 April 2017

[18] Malavida, Facebook Phishing Protector, (http://facebook- phishing- protector.en.malavida.com/). Online; accessed 04 April 2017

[19] McAfe, Social Protection, (http://beta.mcafee.com/betamcafee/mspbeta _ lp.aspx?cookieCheck=true). Online; accessed 04 April 2017

[20] I. Polakis , G. Kontaxis S. Ioannidis , E.P. Markatos , Detecting social network profile cloning, in: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE, 2017, pp. 295–300

[21] (http://thehackernews.com/2016/03/fake-facebook-account. html R. Krishnan, Facebook's latest feature Alerts You if Someone Impersonates Your Profile, Online; accessed 04 April 2017

[22] J. Lv Z, Shan , H. Cao , J. Lv , C. Yan , A. Liu , Enhancing and identifying cloning attacks in online social networks, in: Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, ACM, 2017, pp. 59–65

[23] Social network security: Issues , challenges ,threats, and solutions Shailendra Rathorea, Pradip Kumar Sharmaa, Vincenzo Loiab, Young-SikJ eongc, JongHyuk Parka, **Information Sciences** • December 2017

[24] Net nanny , Social media safety & protection with net nanny

[25] R. Goldschmidt , M. Fire, Y. Elovici , Online social networks: threats and solutions, IEEE Common. Surv. Tut. 16 (4) (2017) 2019–2036

[26] B. Greschbach , G. Kreitz , S. Buchegger , The devil is in the metadata—new privacy challenges in decentralised online social networks, in: Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE, 2017, pp. 333–339

Divya V Currently is a Master's student at B.M.S College of Engineering, Information Science department. Divya received her Bachelor's degree in Telecommunication Engineering in 2018.. Her area of interest is in Network Security, Cloud security, Image Processing and Cyber Security system.

Radhika K R is a professor at B.M.S College of Engineering. She has an experience of 23 years in teaching a wide area of subjects in Information Science Department at BMSCE. She has 40+ publications in various reputed journal. She is a senior member of IEEE. Her area of interests is network security, data mining, cloud security.