American Journal of Electronics & Communication

Prerana Kundu et. al., American Journal of Electronics & Communication, Vol. II (3), 20-29

ANALYSIS OF SECURITY AND PRIVACY IN SOCIAL MEDIA PLATFORMS

Prerana Kundu[1],Pabitra Kundu[1], Sohini Mallik[1] ,
SrimoyeeBhowmick[1], Pratim Mandal[1], Hritam Banerjee[1],
Sudipta Basu Pal[2*[0000-0001-6993-5902]]

[1]Computer Science Engineering Department,
University of Engineering and Management Kolkata, India.

[2]CST & CSIT Department,
University of Engineering and Management Kolkata, India.

Communication Mail: sudipta_basu68@yahoo.com

***ABSTRACT*---**

With advancements in fields of science and technology, communication has become quite faster and more efficient. As the popularity of several social media apps continues to grow among the population of both young and old, telephonic communication is being gradually replaced by these powerful social apps. Apart from standard communication, these apps are also utilized for sharing news, academic scriptures, images, files, music, movies, etc. In conclusion, we might state that our lives have got linked with these apps in massive amounts. Social media platforms contain numerous information about us, in certain cases, even more than we can figure. These apps have emerged to access a certain amount of power and control upon us. So, this massive amount of information needs to be protected, for the breach of the same could harm the basic privacy and security rights of any human being. In this paper, we will try to make a thorough study on different threats and issues regarding our privacy and security and analyze certain precautionary measures.

***Keywords*---- OSNs, security, classic security and privacy threats, moderns threats, TOS.**

I. INTRODUCTION

The internet , nowadays , is known for it's wide applications .Impacting the thoughts , and changing people's lifestyle all throughout . The internet has become a place for gathering and exchanging services, goods and information with this growing usage of the Internet and the development of the same , comes various security and privacy issues that one needs to be aware of . If not cautious enough , one might face the inevitable risk of getting their private information leaked on the internet unknowingly . In worse scenarios, people sometimes end up losing large amounts of money by disclosing their private information to online scammers, falling prey to the various online scams that exist on the internet. This easy, frees of cost gathering of information makes this issue more serious.

This has made the customers voice their concerns regarding privacy and security threats; they might face in their daily online lives. Since every country has their own laws for Cyber security. It is essential to spread awareness and educate the people on how privacy protection could be established globally, have made it possible for people from all over the world to connect with each other.

Every social networking sites' privacy systems makes the users believe, that they have total authority of their own data . While, actually the Social Network Service Provider, practices total authority over private data, of millions of users. Most Social Networking Sites has some license to share its users' posts which it normally mentions on its Terms Of Services. For example, Facebook's Terms of Services stated that it has the license to use it's users posts and blog for promotional reasons till November 2013 . While Facebook's current TOS till retains "non-exclusive, transferable , royalty-free , worldwide license to use any IP content that you post"

Spreading awareness, among all the social network users regarding the security, privacy issues faced on the internet is a must.

Fig. 1 Privacy and Security online

II. LITERATURE REVIEW:

A. *From Privacy Concerns to Uses of Social Network Sites: A Cultural Comparison via UserSurvey.*

This study was conducted by Ho Keung Tsoi and Li Chen from the department of Computer Science at Hong Kong Baptist University in 2011. In this study, Tsoi and Chen (2011) examined the effect of cultural variables on users' privacy concerns and trust in SNSs, and how this affected users' motivation to use such sites, their actual usage, their attitudes and likely future behaviour. The paper focused on the differences between Hong Kong and French SNS users with respect to a number of measures. The purpose of the survey was to identify whether the two cultural groups had different levels of privacy concerns with regard to SNS use. In addition, Tsoi and Chen investigated whether the two groups' differences regarding privacy would influence their trust in SNSs and their motivation regarding SNS use. For instance, if an SNS user is very concerned about the possibility that their personal information will be used by the site owners for purposes other than merely displaying the information, will that user be less likely to trust the site and thus less motivated to share information? Finally, the researchers wanted to see whether users' privacy concerns, trust and motivation would influence their actual usage of SNSs, their overall attitudes, and any other future behavioural intentions. The researchers applied the Theory of Planned Behaviour in the SNS context to identify associations between the variables. This theory is a predictive and persuasive type, where the subjective norm (in the case of this research, trust, privacy, and enjoyability), is connected to individual behaviours such as attitude and behavior intentions.An online survey was used to collect the data: the researchers obtained 154 participants. The survey was distributed through French and Hong Kong public messaging boards and popular forums. Gender, age, educational background and profession were used to classify the survey participants. The survey's main focus was on privacy and trust concerns. The results were analysed using multivariate analysis of covariance. According to Tsoi and Chen, this tool was used because of its ability to adjust mean values and because it is able to identify any differences that can be attributed to nationality or other

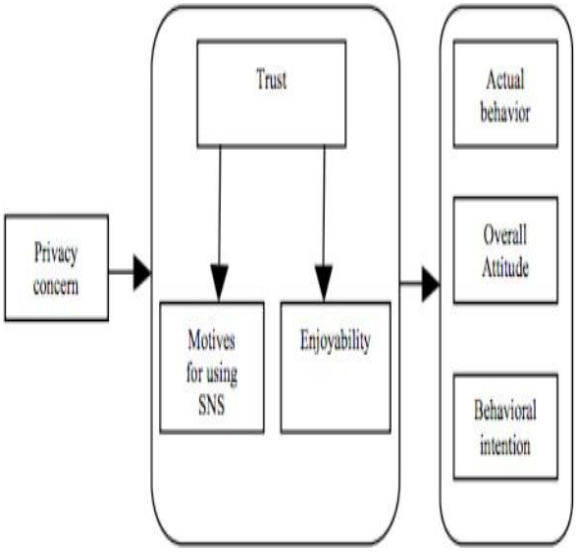

Fig 2. The relationship between measured

possible factors such as gender. The survey used a 5-point Likert scaling method, for instance, some questions had answers that ranged from 'very seldom' to 'very often.' The survey was composed of three sections. The first section contained questions associated with privacy and disclosure of personal information; the degree of comfort the users felt when giving personal information in their SNSs profile; their control over their profile when specifying/updating information; and the overall privacy protection that the user perceived for the SNS. Tsoi and Chen (2011) also asked questions about users' general privacy concerns when using the Internet; their specific and current privacy settings in SNSs; the types of personal information that users provided in their profiles; and the type of posts that they often posted on the site. The second section had questions relating to users' level of trust in SNSs; their main motives for using SNSs; and the degree of enjoyment they got from using SNSs. The third section contained questions about SNS users' overall attitudes towards SNSs, such as, whether they considered the use of SNSs to be a part of their everyday activity. The third also contained questions about users' behavioural intentions; for instance, measuring the level of intention to keep using SNSs more frequently and on a regular basis, and intention to invite friends to use and join them in the network. The privacy questions were used as dependent variables, whereas nationality and gender were used as two covariates. The results showed that nationality had a significant effect on the differences, but gender did not have a significant statistical effect. After determining how the survey participants perceived their SNS privacy, Tsoi and Chen evaluated the kind of personal information that was disclosed in user SNS profiles of French and Hong Kong (HK) participants to determine the differences. The results showed the HK users tended to share more identifying information than the French users. Further results, combined with users' privacy concerns, implied that French SNS users' higher privacy worries probably resulted in a lower level of disclosure of personal information. The lower sharing rate also indicated that they were having a less enjoyable experience, resulting in less motivation to share. Multiple regression analyses were conducted in order to correlate users' privacy concerns with trust, motives, and enjoyability. The latter factors were correlated to users' actual SNS usage, overall attitudes when using SNSs, and behavioural intentions. The results showed a difference in causal factors between the two cultural groups. The French users' results showed the three privacy factors all had effects on one or more of their motives. For HK users, the only factor that played a significant role in influencing the users' motives was their degree of control in updating their profiles. The results also showed that French users' visiting frequency, attitudes, and intentions to using SNSs were genuinely affected by privacy factors. Tsoi and Chen concluded that the French users' higher privacy concerns affected their use of SNSs differently to those of HK users, who were more active due to their lower privacy concerns.

B. A Survey of the degree of online self-disclosure(DOSD)

In this research, conducted in China, Ge et al. (2014) studied privacy leakage issues in Pengyou, one of the most widely used SNSs in China. They explored how users responded to friendship invitations from strangers and therefore their willingness to give access to private information and lists of friends. The researchers created eight fake user profiles, each of which then gained a number of online friends by sending daily friend requests to random strangers. They gained access to 2761 profiles. They then proceeded to quantitatively analyse and examine the degree of online self-disclosure (DOSD), the age distribution of the fake users' friends, and photographic information leakage from the fake user's friends. The researchers used field leakage and DOSD to quantify user's tendency to disclose their own personal information.

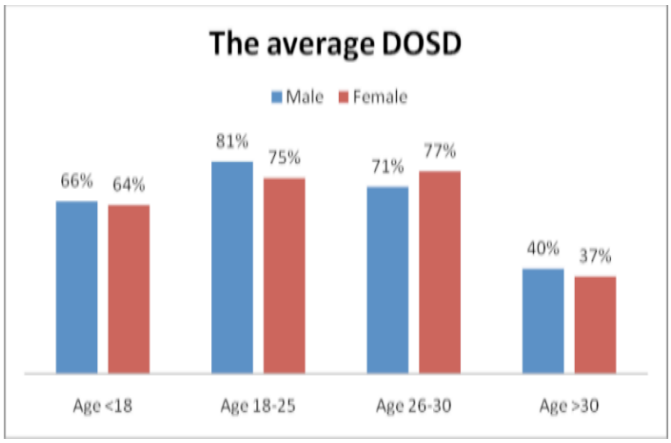

FIG 3. The average DOSD bygender and age.
Source: Ge et al.(2014)

The calculation used four formulae, wwhich are listed in the paper. However, Ge et al. (2014) did not explain how they derived the mathematical formulae. Personal information was analysed based on occupation, residential address, education, email address, hobbies, birthday information, mailing address, and telephone.
In figure 3 the average DOSD by gender and age clearly depicted[]. The survey results revealed some serious privacy threats for SNS users, particularly for minors and young people. The groups most willing to disclose their personal information in that particular SNS were men (81%) aged 18-25 and women (77%) in the same age group.

C. A CASE STUDE: CAMBRIDGE ANALYTICA DATA SCANDAL

Aleksandr Kogan, a data scientist at the University of Cambridge, was hired by Cambridge Analytica , an offshoot of SCL Group, to develop an app called "This Is Your Digital Life" (sometimes stylized as "this is your digital life"). Cambridge Analytica then arranged an informed consent process for research in which several hundred thousand Facebook users would agree to complete a survey for payment that was only for academic use. However, Facebook allowed this app not only to collect personal information from survey respondents but also from respondents' Facebook friends. In this way, Cambridge Analytica acquired data from millions of Facebook users.

The collection of personal data by Cambridge Analytica was first reported in December 2015 by Harry Davies, a journalist for The Guardian. He reported that Cambridge Analytica was working for United States Senator Ted Cruz using data harvested from millions of people's Facebook accounts without their consent. Further reports followed in November 2016 by McKenzie Funk for the New York Times Sunday Review, December 2016 by Hannes Grasseger and Mikael Krogerus for the Swiss publication Das Magazin (later translated and published by Vice), in February 2017 by Carole Cadwalladr for The Guardian (starting in February 2017), and in March 2017 by Mattathias Schwartz for The Intercept. According to PolitiFact, in his 2016 presidential campaign, Trump paid Cambridge Analytica in September, October, and November for data on Americans and their political preferences.

Information on the data breach came to a head in March 2018 with the emergence of a whistleblower, an ex- Cambridge Analytica employee Christopher Wylie. He had been an anonymous source for an article in 2017 in The Observer by Cadwalladr,headlined "The Great British Brexit Robbery". Cadwalladr worked with Wylie for a year to coax him to come forward as a whistleblower. She later brought in Channel 4 News in the UK and The New York Times due to legal threats against The Guardian and The Observer by Cambridge Analytica.Kogan's name change to Aleksandr Spectre, which resulted in the ominous "Dr. Spectre", added to the intrigue and popular appeal of the story.

The Guardian and The New York Times published articles simultaneously on March 17, 2018. More than $100 billion was knocked off Facebook's market capitalization in days and politicians in the US and UK demanded answers from Facebook CEO Mark Zuckerberg. The negative public response to the media coverage eventually led to him agreeing to testify in front of the United States Congress. Meghan McCain drew an equivalence between the use of data by Cambridge Analytica and Barack Obama's 2012 presidential campaign; PolitiFact, however, alleged that this data was not used in an unethical way, since Obama's campaign used this data to "have their supporters contact their most persuadable friends" rather than using this data for highly targeted digital ads on websites such as Facebook.

III. Problem Statement.

Various online threats and scams have been increasing with each passing day , as social media runs on internet , which is a public domain and contains ample amount of personal information of an individual. Some types of social networking attacks are as follows :

1. Identity theft:
As the name suggests, the attacker collects personal information of the victim and tries to impersonate him/her to get some benefit or to harm the victim. Attackers use different methods to launch identity theft like phishing, Collecting information from users who have had shared personal details . Users fall into this trap by visiting harmful sites, having low privacy setting etc.

- Click jacking:

In click jacking, the attacker intends to make the victim click

on something which is different from what the victim aimed to click on. OSN users are often manipulated and they share spam posts on their timelines in order to get 'likes' to links , which is malicious and they are unaware about it. In click jacking , the attacker can even access the hardware devices of the victim to track her/his activities.

Phishing is one of the most common methods to initiate an identity theft attack. Here , the attacker aims to access the personal information of the victim like credit card number , bank details , etc by impersonating themselves as a trustworthy organisations like banks.
Spear phishing is a special type of phishing where the attacker targets a particular group of people having a high profile and extracts their personal details. This type of attack mostly get initiated by the fact that the attacker has some discrete information about the victim (like email) , or has some familiarity with the target user . For example, the attacker sends an email which looks genuine but actually aims at extracting personal information of the victim like credit card details, atm pin etc.

2. Spamming attacks: A spammer sends numerous amounts of emails (or messages) not only to advertise or sell their products but also they aim at extracting sensitive information of the users like their password, credit card information etc. The attackers often create fake profiles and try to steal information of some targeted users.

3. Malware issues: Malware is basically a malicious software which is specially designed to damage a computer system or to take control over the system in order to extract some sensitive information. As the OSN connects huge number of people , the malware gets multiplied easily and more number of users falls into this trap and compromise their security.

4. Cross-Site Scripting: Cross site scripting or XXS is a dangerous attack on web based applications. A malicious code is injected on the platform where the user and the application interact and as a result the victim compromises her/his data , loses data or datas get stored in form of cookies.

5. Internet fraud: Investors often use Social networking platforms as a source of information for making financial transaction. Malicious users take this opportunity and targets the weaknesses and try to manipulate the information and commit fraud to get some monetary benefits.

6. Data mining : Researchers use data mining as a tool to extract valuable knowledge which help them to study the data patterns primarily used in different machine learning algorithms. Gathering data from OSN helps them to improvise the service but again attackers use this technique to gather information that hampers the user's privacy.

IV. Pproblem Solution

Social networks are based on the internet which is a public resource, so online social media can introduce new threats for their users because of the potential for accessing a vast amount of personal information which can be a target of several types of attacks. Some of them are:

A. .Protecting user data from the OSN:

The "notice-and-consent" approach to online privacy is the status-quo forpractically all online services, OSNs included. This approach informs the user of the privacy practices of the service and provides the user a choice whether to engage in the service or not. The limitations of this approach have been acknowledged for long. First, the long and abstruse privacy policies offered for reading are virtually impossible to understand, even if the user is willing to invest the time for reading them. For example, on May 2017, we found 3048 words on Instagram's privacy policies and 3806 words on Twitter's privacy policies. Second, such policies always leave room for future modifications; therefore, the user is expected to read them repeatedly in order to practice informed consent. And third, long as they are, these privacy policies tend to be incomplete [93], as they often cannot include all the parties to which user's private information will be allowed to flow (such as advertisers). Consequently, generally people do not read the Terms of Service and when they do, they do not understand them[30].A second serious deterrent for users protecting their online privacy is the "take-it-or-leave-it" "choice" the users are offered.

1. Protection by information hiding

This line of work is empirically supported by the Acquisti and Gross's study [72] that shows that while 60% of users trust their friends completely with their private and personal information, only 18% of users trust Facebook to the same degree.
The general approach for hiding information from the OSN is based on the observation that OSNs can run on fake data. If the operations that OSNs perform on the fake data are mapped back to original data, users can still use the OSNs without providing them real information. Fake data could be ciphertext (encrypted) or obtained by substituting the original data with pre-mapped data from a dictionary. Encrypted data can be stored on a user's trusted device (including third-party servers or a friend's computer). Access controls are provided by allowing authorized users (e.g.,friends) to get the original data from the fake data. Example: Persona [95] hides user data from the OSN by combining attribute-based encryption (ABE) and public key cryptography. The core functionalities of current OSNs such as profiles, walls, notes, etc., are implemented in Persona

as applications. Persona uses an application "Storage" to enable users to store personal information, and share them with others through an API. Persona application in Facebook is similar to any third-party Facebook application, where users log-in by authenticating to the browser extension. The browser extension translates Persona's special markup language. User information is stored in Persona storage services rather than on Facebook and other Persona users can access the data given that they have the necessary keys and access rights. Similar to the fly- By Night, Persona's operation depends on the OSN, as core functionalities are implemented as applications.

2. Protection viade centralization

An alternative to obfuscate information from the OSN is to mi- grate to another service that is especially designed for user privacy protection. Research in this area explored the design space of decentralized (peer-to-peer) architectures for managing user information, thus avoiding the centralized service with a global view of the entire user population. The typical overlay used in most of these solutions is based on distributed hash tables, preferred over unstructured overlays for their performance guarantees. In addition, data is encrypted and only authorized users get access to the plain text. In this section, we discuss decentralized solutions for OSNs. There are three dimensions that differentiate the solutions: (1) how the distributed hash table has been implemented (e.g., Open DHT, Free Pastry, LikirDHT)
(2) where to store users' content (e.g., nodes run by the user, by the friends or cloud infrastructures)?
(3) How to manage encryption keys for access controls (e.g., public-key infrastructure, out-of-band) Example: LotusNet [104] is a framework for the implementation of aP2Pbased OSN on a Likir DHT [105]. It binds a user identity to both overlay nodes and published resources for robustness of the over- lay network and secures identity based resource retrieval. Users' information is encrypted and stored in the Likir DHT. Access control responsibility is assigned to over lay index-nodes. Users issue signed grants to other users for accessing their data. DHT returns the stored data to the requestor only if the requestor can provide a proper grant, signed by the data owner.

B. Mitigating attacks from large scale crawlers

OSNs enhance social browsing experience by allowing users to view public profiles of others. This way a user meets others, gets a chance to know strangers and eventually befriends some of them. Unfortunately, attackers are there in the vast landscape of OSNs, who exploit this functionality. Users' social data are always invaluable to marketers. Professional data aggregators build databases using public views of profiles and social links and sale the databases to insurance companies, background-check agencies and credit-ratings agencies [31]. For example, crawling 100 million public profiles from Facebook created news recently [109]. Some- times crawling is a violation of terms of service. Facebook states that someone should not collect "...users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior per- mission" [110].One solution of the problem could be the removal of the public profile view functionality. But removal of the public profile view functionality is against the business model of OSNs. Services like search and targeted advertisements bring new users and ultimately revenues to OSNs, but openly accessible contents are necessary for their operation. Moreover, removal of the public view functionality will undermine user experience, as it makes a connection, communication and sharing easy with unknown people in thenetwork.OSN operators such as Facebook and Twitter attempt to de- fend large-scale crawling by limiting the number of user profiles a user can see from an IP address in a time window [111]. However, tracking users with low level network identifiers (e.g., IP address, TCP port numbers or SSL session IDs) is fundamentally flawed as a solution of this problem [112]. Aggressive attackers may gather a large vector of those identifiers by creating a large number of fake user accounts, gaining access to compromised accounts, virtualizing in a cloud, employing botnets, and forwarding requests to proxies. Until now, researchers have leveraged encryption based technique [112] and crawler's observational behaviour [113] to com- bat the problem.

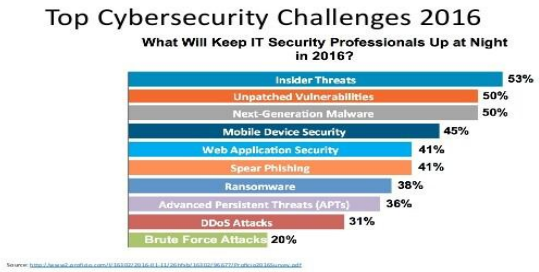

FIG 4. Graph of Top Security Challenges of 2016

V. Result Analysis

A. Countermeasures Against PhishingAttacks:-

There are several factors that contribute to the success of a phishing attack. The main issue is that users may not be able to easily and accurately verify the identity of the sender of email messages. Another problem is that users cannot always differentiate between legitimate and illegitimate contents correctly. It is also possible that the user is not familiar with the meaning of the Secure Sockets Layer (SSL) lock icon, SSL

certificates, absence of security indicators, or the difference between genuine security indicators and fake indicators. Additionally, users usually do not pay enough attention to the location bar at every transaction, and they may not be knowledgeable about the structure of domain names and URLs. In brief, a phishing attack is typically the result of the user's reliance on a particular website, logo, and any other trust indicators [5].There are different classes of phishing attacks—including malware attacks, deceptive attacks, and DNS-based attacks (pharming)—whose common purpose is to steal confidential information from the users. On the other hand, there are several steps that can be taken to equip the users against phishing attack. One solution is to use signature-based anti-spam filters that are able to identify phishing messages and block them before the users access them. Anti-phishing toolbars and browser plug-ins, such as Netcraft or SpoofStick, are used to warn users about phishing sites. Message authentication is an alternative solution against phishing attacks that provides assurance to users that messages sent to them are from trusted parties.Personalized visual information is used as a technique to reduce the likelihood of phishing attacks. An example of this method is using personalized images to transfer online messages or selecting a secret image to log into a website. By applying this technique, attackers cannot send deceptive emails since they do not know what personalized information the target user has chosen. For instance, if the secret image is not displayed to the user while logging into his account, it means that he is not on the trusted website and he should not enter his confidential information. Another countermeasure against phishing attacks is to draw the user's attention to the fact that a message may contain misleading information by using a clear language to explain where a certain link may lead. For instance, if a webpage contains deceptive links, the content will be rendered or highlighted in such a way that the user can visually realize that the embedded URL is suspicious and points to a page that could be malicious.

B. Countermeasures Against Spamming:-

Several solutions have been proposed to address spamming. One of the most common techniques to detect spam is to use statistical or keyword filtering of messages. In keyword spam filtering, the filter looks for suspicious words in the messages using a list of criteria to determine whether the message is spam. On the other hand, statistical spam filters—like Bayesian spam filters—compute statistics on how many times tokens, which can be words or other elements of a message, appear in both spam and non-spam messages and then calculate a statistical probability to decide if an email is spam or not by looking at the tokens in it. Video spamming is also common in video sharing social networks like YouTube. In this case, a malicious user responds to videos posted by legitimate users with unrelated videos with the sole purpose of advertising products or services, distributing pornography, etc. The techniques used to identify spam in text messages cannot be easily used for video spam. Additionally, users must watch at least a part of the posted video to find out if it is spam or not, which will waste system bandwidth and other resources. Some algorithms based on machine learning have been proposed to detect spam in online social networks. For instance, Benevenuto et al. suggested an algorithm to detect video spammers (rather than video spams) by evaluating users' profiles, social behaviour, and posted videos.

C. The Role of OSN Users:-

As explained in previous sections, users of OSNs deal with various types of privacy and security risks. In this section, we offer simple guidelines that can help OSN users to enhance security and privacy and protect themselves against different types of attacks:

- Users must not share too much personal information in OSNs. Sharing unneeded private information within a large network can provide malicious users with opportunities to gather or infer personal information about OSN users, putting their privacy and security at risk.
- Users must not take the risk of accepting friend requests from unknown people, since such requests are likely to come from malicious users.
- Reading the Terms of Use and Privacy Policies of the online social network is recommended to users before registration.
- Since the default privacy settings of OSNs are often inadequate, users are advised to modify their settings after joining an OSN so that the information they share in their profile is not visible to unknown people. For instance, friends only are typically the best option among available levels of privacy settings and permits only friends of the user to gain access to the information shared in a user'sprofile.
- Installing Internet security software is recommended to protect users' personal information while surfing through OSNs. Another suggestion is to remove unnecessary third-party applications that can potentially gather personal information about theusers.
- OSN users must be cautious about location-based applications provided by social networks since they can reveal a user's location and trace any movement. Also, it is a good practice that users do not share their contact information, like email

addresses, schedules, and routines with others, which might allow malicious users to stalk them.

- Since children are more vulnerable to computer crimes, their parents must monitor their online activities. They must also educate their children about the inherent dangers of cyber crimes and teach them the basic rules to follow while surfing through the Internet in general and OSNs in particular.
- Users must report any concern they might have about their privacy and security, like spam,cyberbullying, or identity theft. They should consider contacting the OSN provider and local enforcement agencies or consulting knowledgeable attorneys if they think that they are the victims of cybercrime.

In summary, users must be aware of the fact that once their personal information is disclosed online, there is no guarantee that this information can be removed, since it may have been collected by search engines or copied by other users.

D. Legal and Regulatory Landscape: -

As the number of people using online social networks increases, OSNs are becoming a prime target for cyber criminals. Therefore, several laws and regulations have been introduced to protect OSN users from malicious users trying to take advantage of existing weaknesses and vulnerabilities. For instance, some laws exist against identity theft. Any activity aimed at collecting personal information with the goal of assuming someone else's identity is considered identity theft, including but not limited to:

- Collecting someone else's identity information or photo to create a fake online social account
- Logging into someone else's email or online social account without his permission
- Deceiving someone to release key personal information like his credit card number using fake emails and websites.

There are several centres and organizations that have been established to combat cyber-attacks. For instance, the Department of Homeland Security in cooperation with public and private partners has established the Multi-State Information Sharing and Analysis Centre (MS-ISAC) and the National Association of State Chief Information Officers (NASCIO) to enhance public awareness about cyber security threats.2 MS-ISAC was established for identification and mitigation of cyber threat vulnerabilities and incident response, whereas NASCIO's main focus is to find advanced solutions for public sector IT challenges and cyber security attacks. The US Secret Service has established a network of Electronic Crimes Task Forces (ECTFs) to track and capture malicious activities nationwide. Additionally, the Secret Service has established the National Computer Forensics Institute to provide law enforcement agencies with the resources to fight cyber crimes.3 The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS)—which is working with private sectors, institutions, and other government agencies and foreign counterparts—is another organization that is responsible for fighting cyber crimes. Specifically, CCIPS is responsible for protecting intellectual property (IP)—including any material protected under copyright, trade secret, or trademark laws—against cyber attacks.4 The Federal Bureau of Investigation (FBI) is another government agency that is in charge of dealing with cyber crimes, including cyber-based terrorism and cyber frauds. Indeed, they usually take the first steps to gather information about fraudulent activities and share it with other agencies worldwide. Last but not least, the International Criminal Police Organization (Interpol)is taking steps against cyber crimes since most computer crimes take place trans nationally. Malicious users are now hiring individuals from other countries without diplomatic ties to accomplish their fraudulent activities, including identity theft,phishing, and scamming, with very little chances of being tracked.

VI. Future Scope

The future of the internet is heavily dependent on user data, thus safeguarding this data, and hence, retaining the trust of the users has become the need of the hour. For ages yet to arrive, we face the grave challenge of protecting our digital footprints. Personal information must only be shared with the entities we choose to share them with, and we must also have a way to control the duration and the extent to which our digital footprints are being shared with these entities. With advancements in computer vision,

biometrics, big data, and cloud computing, our digital assets will expand. Therefore, to create safer developments in cyber security, it is essential.

VII. Conclusion

Data collected essentially showed that as much as a more significant percentage of respondents are concerned about their privacy when using social networking sites, there is very little that they can do to guarantee such privacy. This is because of how open the system of most social networking sites isis, allowing people who are neither friends nor followers to view other people's profiles. Even though there is the option made by social networking sites such as Facebook for users to limit people that can view their profile, the respondents said blocking their personal information from the general public was like going hiding from the public, and that would kill the essence and idea of social media networking. A good number of respondents confessed to having looked at the profiles of other people they did not know for curiosity purposes. These findings confirm that, indeed, the issue of privacy remains one that continues to pose a challenge with the use of social media networks. This is because even with a few provisions made by the site hosts to promote identity privacy, not many people are using these as they find them contrary to the whole idea of social networking. Based on the findings, it can be concluded that people have different attitudes towards the use of social media networks, with the younger age mainly focused on the need to make as many friends and followers who will know about what happens in their daily lives as possible. Because of this attitude to social media networks, very little concern is shown towards privacy issues. A conclusion that the risk with privacy will continue to be felt by most users, especially younger people below the age of 30, will be a valid conclusion. Also, secondary data suggests that social network hosts are using their sites as a powerful marketing platform through the sale of critical user data. Then the conclusion is that a user's refusal to be personally concerned about privacy would mean an automatic exposure to privacy risk. It can also be validated until such a time that users will take their privacy into their hands and ensure that no sensitive private data are made available on social media networks as part of building a social profile. Then only very little can be done by the hosts to guarantee safety with privacy, especially as the works of hackers remain uncontrolled.

REFERENCES

[1] Zephoria, The Top 20 Valuable Facebook Statistics, Zephoria2017, URL: https://zephoria.com/top-15-valuable-facebook-statistics/.

[2] Twitter, Twitter Usage/Company Facts, Twitter2017, URL: https://about. twitter.com/company.

[3] E. Protalinski, 56% of employers check applicants' Facebook, LinkedIn, Twitter, 2012,URL:http://www.zdnet.com/article/56-of-employers-check-applicants- facebook-linkedin-twitter/.

[4] H. Kelly, Police embrace social media as crime-fighting tool, 2012, URL: http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media.

[5] G. Lotan, E. Graeff, M. Ananny, D. Gaffney, I. Pearce, et al., The arab spring—the revolutions were tweeted:Information flows during the 2011 tunisianand egyptian revolutions, Int. J. Commun. 5 (2011) 31.(2011) 32–48.

[6] W.B. Dam, School teacher suspended for Facebook gun photo, 2009, URL:http://www.foxnews.com/story/2009/02/05/schoolteacher-suspended-for-facebook-gun-photo/.

[7] D. Mail, Bank worker fired for Facebook post comparing her 7-an- hourwageto Lloyds boss's 4000-an-hour salary, 2011, URL: http://dailym.ai/fjRTlC.

[8] C. Dwyer, Privacy in the age of Google and Facebook, IEEE Technol. Soc.Mag.30 (3) (2011) 58–63.

[9] B. Krishnamurthy, C.E. Wills, Characterizing privacy in online social networks,in: Proceedings of the First Workshop on Online Social Networks, 2008,pp. 37–42.

[10] A. Simpson, On the need for user-defined fine-grained access control policiesfor social networking applications, in: Proceedings of the 2008 Workshop on Security in Opportunistic and SOCial Networks, ACM, 2008, pp. 1:1–1:8.

[11] S. Kruk, FOAM-Realm: control your friends access to the resource, in: Proceedings of the First Workshop on Friend of a Friend,2004.

[12] H.C. Choi, S.R. Kruk, S. Grzonkowski, K. Stankiewicz,B.Davis, J. Breslin, Trustmodels for community aware identity management, in: Proceedings of the 2006 Identity, Reference and Web Workshop, in Conjunction with WWW, 2006, pp. 140–154.

[13] B. Carminati, E. Ferrari, A. Perego,

Rule-based access control for social networks, in: Proceedings of the 2006 International Conference on On the Moveto Meaningful Internet Systems, 2006, pp. 1734–1744.
[14] N. Elahi, MChowdhury, J. Noll, Semantic access control in web based communities, in: Proceedings of the Third International Multi-Conference onComputing in the Global Information Technology, 2008, pp. 131–136.
[15] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu,B.Thuraisingham, Asemantic web based framework for social network access control, in: Proceedings of the Fourteenth ACM Symposium on Access Control Models andTechnologies, SACMAT '09, 2009.
[16] A. Masoumzadeh, J. Joshi, Ontology-based access control for socialnetworksystems., IJIPSI 1 (1) (2011) 59–78.
[17] R. Engelmore (Ed.), Readings from the AI Magazine, American AssociationforArtificial Intelligence, Menlo Park, CA, USA, 1988.
[18] P.W. Fong, Relationship-based access control: protection model and policylanguage, in: Proceedings of the First ACM Conference on Data and Application Security and Privacy, 2011, pp. 191–202.
[19] F. Giunchiglia, R. Zhang, B. Crispo, RelBAC: relation based access control,in:Proceedings of the Fourth International Conference on Semantics, Knowledge and Grid, 2008, pp. 3–11.
[20] Boyd, D.M.; Ellison, N.B. Social network sites: Definition, history, and scholarship. J. Comput.-Mediat. Commun. 2007, 13, 210–230. [CrossRef]
[21] Obar, J.A.; Wildman, S. Social media definition and thegovernance challenge: An introduction to the special issue. Telecommun. Policy 2015, 39, 745–750. [CrossRef]Kaplan, A.M.; Haenlein, M.Users of the world, unite! The challenges and opportunities of Social Media. Bus. Horiz. 2010, 53, 59–68. [CrossRef]
[22] Shozi, N.A.; Mtsweni, J. Big data privacy in social media sites. In Proceedings of the 2017 IST-Africa WeekConference (IST-Africa), Windhoek, Namibia, Southern Africa, 30 May–2 June 2017; pp.1–6.
[23] Nissenbaum, H. Privacy as Contextual Integrity. Wash. L. Rev. 2004, 79,101–139.
[24] Davison, H.K.; Maraist, C.C.; Hamilton, R.; Bing, M.N. To Screen or Not to Screen? Using the Internet for Selection Decisions. Empl. Responsib. Rights J. 2012, 24, 1–21.[CrossRef]
[25] Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. J. Comput.-Mediat. Commun. 2014, 19, 248–273. [CrossRef]
[26] Marwick, A.E.; Boyd, D. Networked privacy: How teenagers negotiate context in social media. New Media Soci. 2014, 16, 1051–1067. [CrossRef]
[27] Ashtari, S. I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy. J. Inf. Priv. Secur. 2013, 9, 80–82. [CrossRef]
[28] Fire, M.; Goldschmidt, R.;Elovici,Y. Online social networks: Threats and solutions. IEEE Commun. Surv. Tutor.2014, 16, 2019–2036.[CrossRef]
[29] Heymann, P.; Koutrika, G.; Garcia-Molina, H. Fighting spam on social web sites: A survey of approaches and futurechallenges.IEEE Internet Comput. 2007, 11, 36–45. [CrossRef]
[30] Everett, C. Social media: Opportunity or risk? Comput. Fraud Secur. 2010, 2010, 8–10.[CrossRef