**Introduction**

A Social Media is a kind of platform for establishing a virtual connection between people with similar interests, backgrounds, and activities. A Social Media is used for all kinds of activity like data sharing, finding friends, expressing thoughts, advertisement, media work, communication and many more work. Social Media is a platform which provides business opportunities, alliances, career opportunity, friendship, relationship, developing social skill, online communication, virtual community and many more. Communication and data sharing is very important aspects where users are able to share their interests, videos, photos, activities, and many more. In recent years, Social Media such as Facebook, Twitter, LinkedIn, Instagram, and Snapchat have become desired media of communication for billions of online users. These services combine user-created profiles with a communication mechanism that enables users to be connected with their friends, families, and colleagues. The prominence of these services is due to the fact that users can update their personal information, interact with other users, and browse other member’s profiles. Social Media is very beneficial for users because they shrink economic and geographical borders. In addition, they can be utilized for achieving goals related to job searching, entertainment, education, publishing online news etc. through subscribing the corresponding page. Fig. 1 contains some of the popular Social Media.

![Social Media](Fig_1.png)

Fig 1 - Social Media
There are many kinds of services are provided by Social Media. All these services are sorted based on their usages: Services for Publishing with (WordPress, Blogger, TypePad, Medium, Wix, Weebly, Ghost, SquareSpace…, wikis (Wikipedia, Wikia…), hybrid publishing / sharing services like Tumblr MySpace, and even make room for new decentralized platform Mastodon. Services for Sharing platforms for multimedia objects (YouTube, Vimeo, Dailymotion), live videos (Twitch, Periscope), documents (SlideShare, Scribd…), data (data.world), photos (Instagram, Flickr, Imgur, Giphy, 500px…), inspirations (Pinterest, Behance, Dribbble…), and music (Spotify, Deezer, Pandora, SoundCloud). Services for messaging in PDA (WhatsApp, Facebook Messenger, SnapChat, iMessage, BBM, Android Message, Allo, Duo, Telegram, Signal, Skype, Kik, Viber, Tango…), visual messaging (Tribe, TapTalk) and classic messaging – webmails – which still gather hundreds of millions of users (Gmail, Outlook, Yahoo Mail). Discussing platforms (Github, Reddit, Facebook, Groups, 4chan, Tapatalk), comment systems (Disqus, Muut, Discourse, GraphComment…), and collaborating FAQ (Quora, StackExchange, Ask…). Professional messaging (Slack, HipChat, Chime, TalkSpirit, Facebook Workplace, Hangouts Chat, Meet, Microsoft Teams) and collaboration platforms (Yammer, Chatter, Dropbox, Evernote…). (LinkedIn, Viadeo, Xing, Plaxo…), dating services (Ning, Nextdoor, Houzz…) and meeting services (Meetup, Eventbrite).

Social media are basically electronic communication forms through which users can build online communities to share ideas, opinions, information, messages, and other content types in different formats, including text, pictures, and videos [1]. In the last few years, we have been witnessing an explosive growth in information being generated and shared in social media. The speed at which social media has proliferated is unprecedented in the history of technological revolution. The continuous progress in social media and related technologies and platforms has led to an ecosystem where users with different cultural backgrounds and making use of various devices (e.g., desktops, tablets, laptops, smartphones) on various social platforms (e.g., Facebook, Twitter, Google+) interact with a variety of products, services, and ideas for various functions including publishing (e.g., tumblr, Quora, Wikia), sharing (e.g., YouTube, Instagram, Pinterest),
playing (e.g., Zynga, Playfish, Playdom), net-working (e.g., LinkedIn, Myspace, Tagged), buying (e.g., tripadvisor, Boosket, hunch), and localization (e.g., Foursquare, yelp, Path)[21]. Corcoran [22] has divided the social media ecosystem into three types: owned media (monitored by the founder/marketers such as a company website or blogs), paid media (purchased by the founder/marketer, such as sponsorships or advertisement).

Fig 2 - Social Media Ecosystem

A couple of years only have been sufficient, for example, for Facebook, Twitter, LinkedIn, and many others to reach each more than half million users worldwide. These numbers are reflecting an immense acceptance, but are also having a deep impact on customers’ behaviors during
information seeking or when making purchase decisions [2]. Social media producers are currently having a fierce competition worldwide to increase their revenues. To achieve this goal, they are investigating alternative ways to attract more users, generate new user activities, and collect valuable data for personalizing contents and services. Nowadays, the cyber-security media are very concerned about people being exposed to all sorts of abuse on Social Media Platforms (SMPs). The malicious intent of humans deceiving other humans constitutes a cyber threat that is one of the most difficult to contend. More importantly, these cyber threats are aggravated by the sheer number of vulnerabilities present in SMPs, the number of available and different types of SMPs (Chaffey, 2016 ), the poor design and construction of SMPs ( Haimson and Hoffmann, 2016 ), the large volumes of unstructured content ( Assunção et al., 2015 ), and the opportunities that SMPs provide to humans acting in malicious ways ( Fire et al., 2014 ).

Cyber threats are widespread, with SMPs being an enabler for cyber attacks ( Khandpur et al., 2017 ). SMPs are vulnerable to cyber threats as they breed trust between individuals without any authority validating or verifying the participants. Cyber crime can potentially have severe consequences. For example, a 14-year-old boy from the UK was groomed online and later killed (Camber, 2014), having been promised “great wealth”. DePaulo et al. (1996) profess that humans are known to lie, for instance about their gender or their age (Drouin et al., 2016). When humans lie about attributes that distinguish them from other humans, it is known as identity deception (Wang et al., 2006).

According to [33], as of November 2018, total worldwide population is 7.6 billion , the internet has 4.2 billion users, there are 3.03 billion active social media users, On average, people have 5.54 social media accounts, the average daily time spent on social is 116 minutes a day, 91% of retail brands use 2 or more social media channels, 81% of all small and medium businesses use some kind of social platform, Internet users have an average of 7.6 social media accounts. Social media users grew by 121 million between Q2 2017 and Q3 2017 [41]. In every 15 seconds a new social media user account is created. Facebook, WhatsApp, Twitter, LinkedIn, Instagram are more popular social media 31].

According to [50], Facebook adds 500,000 new users every day; 6 new profiles every second, 76% of Facebook users check it every day, The average user spends 35 minutes on Facebook a day, There are an estimated 270 million fake Facebook profiles, There are 60 million active
business pages on Facebook, Facebook has 5 million active advertisers on the platform, Facebook accounts for 53.1% of social logins made by consumers to sign into the apps and websites of publishers and brands. WhatsApp have 900 million users. Facebook Messenger and WhatsApp handle 60 billion messages in a day [24].

There is a total of 1.3 billion accounts on Twitter, but only 328 million are active. There are 500 million Tweets sent by user’s each day and 6,000 Tweets every second [51]. LinkedIn is a completely professional network used for networking, looking up for jobs, research work and more. LinkedIn has 500 million user over 200 countries. Out of 500 million users, 250 million users access the site monthly basis and 40 percent access daily. 2 new members join LinkedIn per second. More than 1 million members have published contents on it. 10 million jobs are actively listed on LinkedIn and 122 million people received an interview from LinkedIn profile. 40 million students and fresh graduates are on LinkedIn. There are 57% of male users and 44% female users on LinkedIn [34].

Instagram has 800 million monthly active users where 500 million are daily active users. There are 4.2 billion likes per day, around 95 million photos are uploaded each day and more than 40 billion photos have been shared so far. There are 32 percent of all internet users are on Instagram, 68 percent Instagram users are female and 90 percent of Instagram users are younger than 35 years. Instagram has 15 million registered business account, 80 percent of users follow at least one business on Instagram [35]. Snapchat has 178 million daily active users and on an average, 3 billion snaps are sent every day. There are 54% of Snapchat users log in at least once in a day, 55% of Snapchat users follow business on it. More than 400 million Snapchat stories are created per day and More than 20,000 photos are shared every second. The average daily user of Snapchat creates more than 20 messages, or “snaps,” per day [39]. There are many more social media platform are popular like Google+, Pinterest etc. While the popularity and usefulness of Social Media creates a high risk for their users in terms of data security. Data starts when you sign up for Social Media. It gains steam as you use the Social Media more. When you sign up for a Social Media account, you’re required to share: name, gender, date of birth, email or mobile number etc. [29]. Social Media gathers and stores more personal data, which can be used to target users with ads, including what users share and add, and their likes and clicks. Social Media tracks and stores data about: Every ad users
click on, Any additional personal information added to the profile including schools, maiden name, hometown and current city, employment, other social networks like political clubs, groups, and alumni associations (current and former), every IP address that the user used when logging into the Social Media account, every friend in the network, including friends that have been deleted, all of the user’s activity—ever. Social Media like Facebook describes its activity log as “a list of your posts and activity, from today back to the very beginning. You will also see stories and photos you have been tagged in, as well as the connections you have made – like when you liked a page or added someone as a friend.” That means every “like,” every status change, and every search of another person on Facebook [30].

Hackers targets the large amount of data shared by users on Social Media. Hackers can steel sensitive personal data from Social Media. Many kinds of attacks such as spam, malware, socialbots, and identity theft can be applied using following hacking technique-ClickJacking Attacks, Virus or Trojan, Phishing, Eavesdropping (Passive Attacks), Fake WAP, Waterhole attacks, Denial of Service (DoS\DDoS), Keylogger etc. A hacker can know about your personal unauthorized information which you might not want to reveal. Knowing about these common hacking techniques like phishing, DDoS, clickjacking etc. could come handy for your personal safety[40].

While hacking is illegal. Getting unauthorized information by modifying a system’s features and exploiting its loopholes comes under cybercrime. In this world where most of the things happen online, hacking provides wider opportunities for the hackers to gain unauthorized access to the crucial information like credit card details, bank account details, email account details, and other personal information [47].

**Motivations of the attacks on social media**

Attacker, also known as hackers, carry out attacks on social media with wide range of motivations. These include revenge/emotions, financial gains, entertainment, hacktivism, espionage and cyber warfare-

Revenge/Emotions- Dissatisfied or displeased users or even an organization employee can attempt a cyber-attack on social media due to their anger, disagreement or any kind of revenge.
These type of hackers aim to destroy the reputation of the victim organization by blocking their services and leaving the legitimate users disgruntled. Due to such kind of attacks victim organization may incur great financial loss [44].

Financial gains- This is the most important and common reason for attack on social media. Cyber criminals gain the sensitive information regarding the bank account of the users and maliciously access their account to acquire the financial gain. It may include stealing the business related information to gain the profit by another rival company [25].

Entertainment-Some hackers enjoy the thrilling experience of hacking on social media. They perform attack to gain recognition of their hacking abilities or notoriety among fellow hackers. They do it for their entertainment without expecting any financial or political gain. As some say, some men just want to watch the world burn [49].

Expertise for job- Most of the IT experts do not have cybersecurity and hacking background, thus there is a very high demand for expertise in these fields. The employment domain for these jobs is very fervent these days. Hiring hackers and cybersecurity specialists can help the organizations evaluate their security in a better way and tackle the cyber criminals easily, it is easy to beat acriminal if we have a person on our side, who can think and operate in the same way as him/her.

Hacktivism- Hacktivism is use of computers and computer networks to promote political ends, chiefly free speech, human rights and information ethics. This also includes the publishing aims and views of a political community or religion, to stage protests supporting their political/religious beliefs. It also includes vandalism of the various websites with political/religious messages [45].

Cyber espionage- This is also one of the important motivations that leads to the theft of confidential information on social media. It includes obtaining private information without permission of owner of the information from individuals, competitors, or even other country. These attacks are done with the help of various hacking techniques and malicious software[48].
Cyber warfare- These are politically motivated Internet-based attacks on information and information systems using social media. The target of these attacks mainly includes government websites to cripple down their communication, financial stability and many other things that mainly focus on improper functioning of the government of other country. It is basically a war that is fought by sitting inside the room, than going on the front. [37]

**Various attacks on social media**

The various types of Social media platforms invite a variety of attacks towards them, which tend to steal users’ identity or threaten then privacy and trust over the network. In this section, we present the some attacks which are prominent over the social media these days.

Identity theft - This refers to the real time impersonation of legitimate user, the attacker takes control the target profile and is able to successfully other genuine user that the profile belongs to him. Here the attacker misuses the profile in any way possible which could have severe impact on the user whose identity it was once.

Spam attack - Here, the attacker somehow obtains communication details about the user and are able to send spam or junk data. The communication details are not that hard to obtain, they can be extracted by the profiles of the legitimate user. The spam emails send in bulk cause network congestion and cost of sending emails falls mostly upon the service providers and sometimes on the user.

Malware attacks - They are becoming very common among social networking sites these. The attackers send malware injected scripts to the legitimate user. On clicking the malicious URL a malware might be installed on the attackers devices or it can lead to a fake website which attempts to steal some personal information from the target user.

Sybil attacks - Fake profiles are the foundation for Sybil attacks, which can be harm the proper functioning of the social media platform, they can be used for the distribution of junk information or even malware over the network. To prevent these attacks the authentication mechanisms while user registration should be stronger.
Social phishing- It refers to the attack where the attacker aims to obtain sensitive information from a target user via some fake website which appears to be real or by impersonating someone the target is acquainted with. These attacks can be significantly reduced if the users are aware and should examine the data they receive carefully beforehand.

Impersonation- Here the aim of the attacker is to create fake profile in order to successfully impersonate a real-world person. This attack highly depend on the authentication techniques that are faced by the users while registration to make new account. These attacks can do serious damage to the target which is being impersonated.

Hijacking - It refers to acquiring control over someone else’s profile. The attacker is successful in hijacking a legitimate profile if they are able to crack login password of the account. Weak passwords are thus a poor choice as they increase the threat of hijacking such passwords can be obtained by dictionary attacks. Strong passwords and changing them frequently is good practice.

Fake requests - The attacker sends fake request with their own profile, so as to enlarge their network. If the users accept fake request it gives the attacker more privileges and they are able to more information from the victim profiles. The prevention of fake requests is not possible, thus, the user should be more responsible over the social media.

Image retrieval and analysis - The attacker here uses various face and image recognition software to find more information about the target and its linked profiles. It not only affects the target but also his/her friends and family. This attacks aims to gather images videos etc. from the target.

Bait and switch hacking technique- The attacker can buy advertising spaces on the websites. Later, when a user clicks on the ad, he might get directed to a page that’s infected with malware. This way, they can further install malware or adware on your computer. The ads and download links shown in this technique are very attractive and users are expected to end up clicking on the same.

Cookie theft attack- The cookies of a browser keep our personal data such as browsing history, username, and passwords for different sites that we access. Once the hacker gets the access to
your cookie, he can even authenticate himself as you on a browser. A popular method to carry out this attack is to encourage a user’s IP packets to pass through attacker’s machine.

Clickjacking attack- The hacker hides the actual user interface where the victim is supposed to click. This behavior is very common in app download, movie streaming, and torrent websites. While they mostly employ this technique to earn advertising dollars, others can use it to steal your personal information.

Virus or trojans attack- They use malicious software programs which get installed into the victim’s system and keeps sending the victims data to the hacker. They can also lock your files, serve fraud advertisement, divert traffic, sniff your data, or spread on all the computer connected to your network.

Eavesdropping- This attack is a passive attack, in this attack hacker just monitors the computer systems and networks to gain some unwanted information. The motive behind eavesdropping is not to harm the system but to get some information without being identified. These types of hackers can target email, instant messaging services, phone calls, web browsing, and other methods of communication.

Fake WAP - Using fake WAP technique, a hacker can use software to fake a wireless access point. This WAP connects to a public place WAP. Once you get connect to a fake WAP, a hacker can steal your data.

Waterhole attack - Hackers target the most accessed location like coffee shop or cafeteria etc. Once hackers are aware of your timings, they might create a fake Wi-Fi access point on that particular time and modify your most visited website to redirect them to you to get your personal information. As this attack collects information on a user from a specific place, detecting the attacker is even harder. To protect from such kind of hacker, update your software/operating system on regular interval and follow the basic security practice.

Denial of Service attack - Attackers target the site or server which is unable to process the request in the real time because of heavy traffic. The attacker floods the targeted machine with tons of
requests to overwhelm the resources, which, in turn, restrict the actual requests from being fulfilled.

Keylogger - It is a simple software that records the key sequence and strokes of your keyboard into a log file on your machine. These log files might even contain your personal email IDs and passwords. It can be either software or hardware. While software-based keyloggers target the programs installed on a computer, hardware devices target keyboards, electromagnetic emissions, smartphone sensors, etc. To avoiding the keylogger, banks provide the virtual keyboard.

Apart from these traditional hacking technique others techniques are multimedia content threat. All social media provides data sharing feature where users used to share images, video, activities etc. These multimedia data attackers can used to get users sensitive information. Using multimedia retrieval techniques, such as location estimation, face recognition, web searches, and geotagging, can increase the chances of these items being illegally utilized. Under this category there are many other threats come like multimedia content exposure, shared ownership, manipulation of multimedia content, steganography, metadata, shared links to multimedia content, static links, transparency of data centers, video conference, tagging, and unauthorized data disclosure. In Multimedia content exposure,

Users are cautious to upload their id and home address. However, they are not as aware when it comes to posting multimedia data, which also discloses an enormous amount of sensitive information. For example, if a user posts pictures of his or her home, an intruder can find the user’s home address by using these data.

Problem Statement: “Social Media Profiling – A Step Ahead to Provide Social Media Security”