

# Research Journal of Pharmaceutical, Biological and Chemical Sciences

## Risk Factors Analysis of Social Media Networks.

Bala Sundara Ganapathy N\*, and Mohana Prasad K.

Department of Computer Science Engineering, Sathyabama University, Tamil Nadu, India

### ABSTRACT

Most of the popular social networks provide access in various languages so that the users can interact with their acquaintances around the world irrespective of the boundaries based on geographical, cultural, political or economic factors. It has been recently estimated that the number of social networks users are roughly around two billion; moreover, it is anticipated that this number would significantly raise in value due to the increasing use of cell phones, which in turn results in the increasing use of mobile social networks. As the use expands, we ought to be mindful about their upsides and downsides. This paper dissects about the hazard elements of social media network. The point of this investigation is to make the attention to the social media networking and think about what to do and what don't? We have raised with a grouping of social issues and proposed a portion of the relief strategy to fathom them. The investigation comes about that we ought to painstakingly handle the social media websites so that our protection can be saved and it shouldn't be abused. We have considered the most Popular Social Networking Sites and Apps for our examination.

**Keywords:** risk factors, social networks, mobile social networks, social issues

*\*Corresponding author*



## INTRODUCTION

All Internet clients now interface with Social Media somehow. A few of us contribute new substance while others like to just peruse it and once in a while post remarks, surveys or bookmark their most loved substance for some other time. Whatever the case, Social Media has hugely affected the way we utilize the Internet to mingle, teach ourselves, work together, thus considerably more.

As indicated by research completed by Forrester Research [1], there are 6 distinct sorts of online web-based social networking clients: Creators, Critics, Collectors, Joiners, Spectators and Inactives.

**The Creator:** This is the individual who makes online networking for the world to see. This kind of client will distribute blog entries or site pages, transfer recordings/pictures/sound and share content on the web.

**The Critic:** The individual who reacts to content posted by others. Posts evaluations and surveys of items and administrations, remarks on online journals and gatherings and adds to articles in a wiki.

**The Collector:** The individual who arranges content for themselves or others utilizing RSS channels, social bookmarking (ex: Digg) and photograph or page labeling.

**The Joiner:** The kind of individual who joins informal communication sites like Facebook and Twitter and keeps up various profiles.

**The Spectator:** This sort is likely the most widely recognized – The individual who peruses sites, sees client created recordings (ex: YouTube), peruses online forums, listens to podcasts and as often as possible hunt down client audits and appraisals.

**The Inactive:** The individual who is on the web yet not the slightest bit takes part in any type of web-based social networking. Doesn't post anything or read anything which is client produced content. This sort is getting to be rarer as more sites coordinate components of online networking into their site.

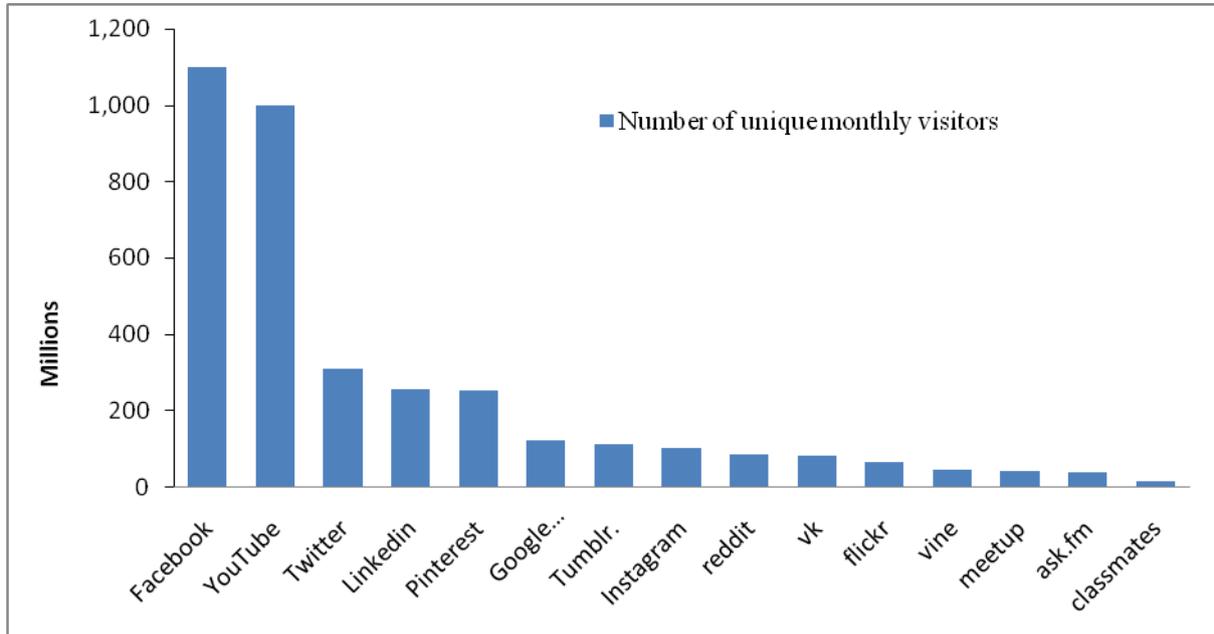
Among these clients, joiner and spectators part is high among the youthful teenagers and high at youth and youthful grown-ups. Joiner and spectators are being staged loads of issues taking care of the web-based social networking system either straightforwardly or in a roundabout way. In this manner it is our duty to give upsides and downsides of web-based social networking system, so that the more youthful eras handle the net in more secured way.

## POPULAR SOCIAL NETWORKING SITES

There are huge Social media systems accessible for fulfilling various types of clients for various purposes. For instance web-based social networking systems are especially useful to the businessmen. Web-based social networking systems are a noteworthy asset for both little and huge organizations that are hoping to advance their brands on the Internet. The stages are anything but difficult to utilize and some of them even have paid publicizing choices for organizations that need to achieve new groups of onlookers. Nonetheless, in light of the fact that our business should be on these stages doesn't imply that it must be on each other online networking website. To appropriately use the force of online networking we have to know the most well known web-based social networking locales and distinguish the ones that work best for our business to abstain from spreading our self too thin. To make this simple for us, we profiled 15 most famous online networking sites so we can now settle on educated showcasing choices.

This measurement gives data on the most mainstream systems worldwide as of April 2016, positioned by number of dynamic records. Showcase pioneer Facebook was the principal informal community to outperform 1 billion enlisted accounts and presently sits at 1.59 billion month to month dynamic clients. Eighth-positioned photograph sharing application Instagram had more than 400 million month to month dynamic records. In the interim, blogging administration Tumblr had more than 555 million dynamic blog clients on their website.

The bar graph given in figure 1 are the main 15 Most Popular Social Networking Sites as got from eBizMBA Rank which is a consistently overhauled normal of every site's Alexa Global Traffic Rank, and U.S. Activity Rank from both Compete and Quantcast[2].



**figure 1: number of unique monthly visitors as on december 1, 2016**

### Social Media Issues

#### Social Media Addiction

Social media networks are hugely addictive. A great many people we know check and associate on social media websites continually for the duration of the day. What's more, they have no clue how much genuine time they spend via web-based networking media. In case you're a web-based social networking junkie, and your dependence is deteriorating, there's an explanation behind that: Most of the significant social media network companies, and also social substance makers, are buckling down each day to make their systems so addictive that we can't avoid them.

#### Facebook

Cornell Information Science distributed research [3] [11] not long ago that took a gander at (in addition to other things) the trouble a few people have in stopping Facebook and other social media networks. They even have a name for the inability to stop: "web-based social networking inversion." The study utilized information from a website called 99DaysofFreedom.com, which urges individuals to quit utilizing Facebook for 99 days. The site and study are fascinating on the grounds that they uncovered the trouble individuals have stopping Facebook due to addiction. Members planned to stop, needed to stop and trusted they could stop (for 99 days), however many couldn't make more than a couple days.

The addictive part of long range interpersonal communication is connected with FOMO - fear of missing out. Everybody is on Facebook. They're posting things, sharing news and substance and conversing with each other every minute of every day.

The system impact itself is addicting, according to Hochmuth and craftsman and PC researcher Jonathan Harris made a web encounter called Network Effect. The site recreates the experience of perusing through online networking by giving you an encourage of individuals connecting with on different exercises. At



that point, following a couple of minutes, the site won't give you a chance to observe any longer (for 24 hours) so you can encounter the unpretentious withdrawal side effects.

In the realm of social media networking, Facebook benefits most from system impact. Facebook happened to be the top social media networking when long range interpersonal communication broke out as a standard movement. Presently, everyone's on Facebook on the grounds that everyone's on Facebook. What's more, even individuals who don't care for the interpersonal organization utilize it in any case, since that is the place their family, companions and associates are - and due to addiction. The commitment of system impact to the addictive nature of sites is unplanned. Be that as it may, social destinations are additionally addictive by outline.

#### **Notification number:**

One trap informal communities utilize is a notification number, demonstrating to you the quantity of individuals initially who have said or tailed you. Notification numbers show up on the application symbol to attract you, then on the top or base menu to attract you assist. They play the same mental trap on you that click bait features do - they let you know that there's data you truly need to know, yet they don't let you know enough to fulfill. Notice numbers work simply like that. Seeing a red "5" on the Facebook notices bar resemble a click bait feature: "You will have a hard time believing what three individuals have said in regards to you." You must snap or tap. It's urgent. Furthermore, after some time, it gets to be addictive.

The greatest apparatus in the online networking expansion tool stash is algorithmic separating. Destinations like Facebook, Google+ and, soon, Twitter, change their calculations, then screen the reaction of clients to check whether those changes kept them on the site longer or expanded their engagement. We're all guinea pigs in a goliath, worldwide analysis. The utilization of algorithms for making social streams progressively addictive clarifies a considerable measure. It clarifies why Facebook now gets more than a billion clients a day. It clarifies why Google never let you kill algorithmic stream separating the distance. What's more, it discloses why Twitter needs to algorithmically channel nourishes, in spite of the general complaint of clients. The tweaking of algorithmic channels for habit implies that in principle social destinations get more addictive consistently, and that the locales are in a war for survival where just the most addictive destinations will survive. Then, our intrinsic human capacity to oppose this fixation doesn't advance.

#### **YouTube**

YouTube is addictive, as well, particularly for individuals less than 20 years old or something like that, who utilize YouTube as their principle wellspring of stimulation [12]. Serial YouTube video clicking is likened to the impulse to TV channel-surf. You flip through the channels interminably in light of the fact that definitely something better should be on right at this point. YouTube resemble TV, however with a billion channels. What frequent youthful YouTubers are viewing is a vital component to understanding why it's addictive for them. The vast majority of this viewing includes recordings where YouTube stars converse with the camera. For instance,

<https://www.youtube.com/watch?v=NWUnf8xr0oo>,

post about My Brand New Car has 1,023,590 viewers up to November, 2016. Demonstrates like these traps the human cerebrum into feeling like the YouTuber star is talking straightforwardly to the viewer, and makes the viewer feel like they have an individual association with the individual before the camera.

In the interim, there's another Darwinian challenge occurring. YouTube stars have figured out how to talk in a way that snatches and holds the consideration of the viewer. They've figured out how to make their own on-screen identities addictive. It joins the natural human fascination for social association with a Darwinian challenge among stars to ace the craft of consideration snatching appeal in addition to the channel-surfing impulse in addition to an addictive interpersonal interaction component in the remarks segments.

### **Cyber stalking and location disclosure**

With the production of social sites like Facebook, many individuals are giving their own data out on the web [13]. Most clients don't know that they can change the protection settings and unless they alter them, their data is open to the public. Social media web sites, for example, Facebook and Twitter have become well known by communicating notices including individual data, for example, location. A few applications verge on "cyberstalking." This has reclassified the part of Internet protection as covering with that of security.

A few applications are unequivocally focused on "cyberstalking." An application named "Creepy" can track a man's location on a map utilizing photographs transferred to Twitter or Flickr. At the point when a man transfers photographs to a social media web site, others can track their latest location. Some advanced mobile phones can implant the longitude and latitude coordinates into the photograph and naturally send this data to the application. Anyone utilizing the application can hunt down a particular individual and after that locate their current location. This stances numerous potential dangers to clients who impart their data to a vast gathering of followers.[4]

"Facebook Places" is a service, which broadcasts client location data to the social media networking community. Clients are permitted to "check-in" at different areas including retail locations, comfort stores, and eateries. Additionally, clients can make their own "place," revealing individual data onto the Internet. This type of location tracking is robotized and must be killed physically. The Federal Trade Commission has gotten two grievances as to Facebook's "unjustifiable and tricky" exchange rehearses, which are utilized to target promoting segments of the online group. "Places" tracks client area data and is utilized principally to advertise purposes. Every area followed permits outsider sponsors to redo notices that suit one's interests. At present, the Federal Trade Commissioner alongside the Electronic Privacy Information Center are revealing insight into the issues of area information following on interpersonal interaction sites.[5]

### **Privacy Agreements**

Another security issue with social media networks is the privacy agreement. The privacy agreement expresses that the social media network possesses the greater part of the substance that clients transfer. This incorporates pictures, recordings, and messages are altogether put away in the social media networks database regardless of the possibility that the client chooses to end his or her account.[6]

Privacy agreement in many cases says that they can track a client's location and action in light of the gadget utilized for the site. For instance, the protection assentment for Facebook states that "all gadgets that a man uses to get to Facebook are recorded, for example, IP addresses, phone numbers, operating system and even GPS locations".[7] One principle worry about privacy agreement are the length, since they set aside a considerable measure of opportunity to completely read and get it. Most security assentments express the most critical data toward the end since it is expected that individuals won't read it totally.

### **Privacy Settings**

Most social media users don't know that they can adjust the protection settings and unless they alter them, their data is interested in people in general. On Facebook security settings can be gotten to by means of the drop down menu under record in the upper right corner. There clients can change who can see their profile and what data can be shown on their profile.[6] In many cases profiles are interested in either "all my system and companions" or "the greater part of my companions." Also, data that shows on a client's profile, for example, birthday, religious perspectives, and relationship status can be expelled by means of the security settings.[8] If a client is under 13 years of age they are not ready to make a Facebook or a MySpace account, in any case, this is not regulated.[9]

### **Law Enforcement Prowling the Networks**

The FBI has devoted covert specialists on Facebook, Twitter, MySpace, LinkedIn. The standards and rules to the security issue is inward to the Justice Department and subtle elements aren't discharged to general society. Specialists can imitate a companion, a missing relative, even a mate and youngster. This raises



main problems with respect to security. In spite of the fact that individuals who utilize Facebook, Twitter, and other social media networking sites know about some level of security will dependably be traded off, in any case, nobody could ever presume that the companion welcome may be from a government specialist whose sole reason for the companion demand was to snoop around. Besides, Facebook, Twitter, and MySpace have individual data and past presents logged for up on one year; even erased profiles, and with a warrant, can give up our individual information's.

### **TrueCaller**

The TrueCaller application gives an exhaustive telephone index of individuals, both locally and universally. Client can discover subtle elements of obscure portable or landline telephone numbers. These subtle elements may incorporate name, address and area of the guest. TrueCaller can likewise piece undesirable calls and fill subtle elements in your phonebook utilizing web-based social networking profiles of contacts. It right away lets you know who's ringing before you pick the call. It gathers and keeps up the contact subtle elements of the considerable number of clients who install the application. At the point when installing the application, it requests that consent get to every one of our subtle elements including contact. On acknowledge the terms and conditions it recover all our contact subtle elements and store it in their database, through which the application gives caller data to us. Here our security is deficient.

### **Twitter**

Twitter permits individuals to impart data to their supporters. Any messages that are not changed from the default protection setting are open, and accordingly can be seen by anybody with a Twitter account. Despite Twitter's earnest attempts to ensure their clients security, individual data can in any case be hazardous to share. There have been episodes of spilled tweets on Twitter. Spilled tweets will be tweets that have been distributed from a private record yet have been made open. This happens when companions of somebody with a private record re-tweet, or duplicate and glue, that individual's tweet et cetera until the tweet is made open. This can make private data open, and could be dangerous.[10] Another issue including security on Twitter manages clients unconsciously unveiling their data through tweets. Twitter has area administrations appended to tweets, which a few clients don't know are empowered. Numerous clients tweet about being at home and join their area to their tweet, uncovering their own personal residence.

### **To Be Safe In Social Media Network**

Web-based social networking addiction is genuine, and it can harm vocations, corrupt life and even damage connections. For a large portion of us, however, we're essentially being controlled by the social media sites and content makers to squander substantially a lot of time in a way that advantages them, not us. The best arrangement is to visit social media networking sites once every day. Plan it. What's more, monitor how much time you're spending there. Attempt it. Also, on the off chance that you succeed, you're en route to beating habit without going immediately. Furthermore, in the event that you can't adhere to your once-a-day propensity, well, it sounds like you have a habit issue.

You can relieve the irritating stuff effortlessly enough:

- Hide notices from companions who don't present anything that intriguing on you.
- Keep a littler number of contacts. Your news sustain will be significantly less messed in case you're not seeing announcements from scores of individuals you scarcely know.
- Change your settings so your contacts can't perceive what number of companions you have, in case you're inclined to agonizing over whether individuals will judge over your number of contacts.
- Hide future announcements from amusements, applications, tests. Nowadays Facebook is better about doing this consequently, fortunately.
- Turn your protection settings up to the most extreme and by and large be discrete and saving about what data you uncover about yourself. In case you're just on the site to stay aware of your companions you don't need to add a cluster of interests to your profile and give Facebook Inc. additional promoting information.

- Maybe take an all the more accommodating perspective of what individuals do on Facebook. Possibly that one individual isn't a consideration addict, and she just likes going out with her companions and after that snickering about the recollections and pictures a while later. A few people may jump at the chance to hear that their one companion experimented with another treat formula, or that they went on a lovely walk. Perhaps they believe it's a pleasant little insight about how they spent their day. What's more, it's alright if some social trades are somewhat pointless. It doesn't need to be profound and important throughout the day, consistently.
- Different settings must be turned off and controlled all together for the client to guarantee protection. As indicated by epic.org, Facebook clients are prescribed to: (1) debilitate "Companions can register me with Places," (2) alter "Places I Check In," (3) incapacitate "Individuals Here Now," and (4) uncheck "Places I've Visited."
- Users should familiarize themselves with various privacy settings so that they can ensure privacy to the maximum possible extent. Since most of the default settings reveals their personal details, users should manually change the settings as needed. It is a good idea to follow the following recommendations of epic.org, in relation to the Facebook access: (1)disable "Friends can check me in to Places," (2)customize "Places I Check In," (3)disable "People Here Now," and (4) uncheck "Places I've Visited."

### CONCLUSION

This paper analyze about various risk factors which affects our privacy in social media network. It also suggests various mitigation techniques to overcome the above said risk. In future we have planned to develop a new framework to handle the above discussed issues.

### REFERENCES

- [1] <http://www.ondigitalmarketing.com/learn/odm/research/social-media-users>
- [2] <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users>
- [3] <http://infosci.cornell.edu/news/cornell-research-these-factors-might-explain-why-we-can-or-cant-quit-facebook>, 10 December 2015
- [4] Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case). [Online]. Available at: <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>[Accessed 24 April 2011].
- [5] Kelly, S. Identity 'at risk' on Facebook. BBC News. [online]. Available at:[http://news.bbc.co.uk/1/hi/programmes/click\\_online/7375772.stm](http://news.bbc.co.uk/1/hi/programmes/click_online/7375772.stm)[Accessed 25 April 2011].
- [6] Merritt, Grace E. (February 16, 2007). "My God. What Do I Do?". Hartford Courant. Retrieved 20 May 2015.
- [7] "Vancouver riots 2011: Crown to look at potential charges". Global News. 2011-06-20. Archived from the original on 2011-10-04.
- [8] Gross, R. and Acquisti, A. 2005. Information Revelation and Privacy in Online Social Networking Sites (The Facebook Case).[online]. p. 8. Available at: <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf> [Accessed 24 April 2011].
- [9] Randall, D. and Richards, V. Facebook can ruin your life. And so can Myspace, Bebo. The Independent [online]. Available at: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html>. [Accessed 24 April 2011]
- [10] <http://www.beyondidentitytheft.com/dangers-of-social-networking.html>
- [11] K. Mohana Prasad, Dr. R. Sabitha "Meta Physical Algorithmic Representation for Flawless Clustering" Journal of Theoretical and Applied Information Technology (JATIT), ISSN : 1992-8645, Volume 76, NO 1,PP 82-87.
- [12] -k.mohana prasad, Dr. R. Sabitha "Evolution Of An Algorithm For Formulating Efficient Clusters To Eliminate Limitations" International Journal of Applied Engineering Research (IJAER), ISSN 0973 – 4562, Volume 9, Issue 23, pp. 20111-20118.
- [13] - K. Mohana Prasad, Dr. R. Sabitha," Yoking of Algorithms for Effective Clustering", Indian Journal of Science and Technology,ISSN: 0974-6846 Vol 8(22), IPL0269, September 2015,pp 1-4.