IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Security And Privacy Of Social Media: Modeling And Solutions

Taran Singh Bharati

Department of Computer Science
Jamia Millia Islamia,
New Delhi, India

**Abstract**

**Social networking has become the important part of the society. Almost all celebrities, politicians, businessmen, students, social activist, sportsmen, etc. have their accounts on social media. In the social media people can express their views which may be seen and analyzed by the general public. Millions of views, tweets, post are posted by people. What users express and discuss, there is no much control on them. Peoples' profiles' data is visible and can be misused by the eavesdroppers. As social media has no boundary therefore lot of challenges are there, i.e. storage management, security, privacy, etc. prevail. This paper focuses on the security and privacy concerns and proposes a security and privacy model along with solutions to uphold them**.

Keywords: **Social Sites; Blogs; Groups; Privacy; Security.**

## I. INTRODUCTION

Social media now has become new way of spreading the awareness because it is mostly un-regulated in many countries. On Social media, celebrities, politicians, ordinary people, students, office workers, sportsmen, businessman, Governments, NGOs, and other renowned people are available, who are followed by millions of followers. It is has become a convenient tool to spread your agenda very rapidly. When almost everybody is connected to these social sites specially when main stream media does not show interest to cover the events. The social sites helped people to reunite the childhood friends or old school or college mates. Social media like Facebook, Twitter, Instagram, Orkut, etc. Now any citizen of the country can open the account and join any group. In social media one can make groups of people for a cause and information can be shared within the group. People can make and write their individual Blog to express their thoughts and ideas. Social sites have vast applications that they are used by health professional to consult the remote patient, to consult or discuss the senior doctors to better diagnose the disease of the patient. Social media is nowadays start using in Government offices also for making communications for smoothly running government and following tags are associated with message; identity, authority, relevance, professionalism, openness, compliance, and privacy. In case of disaster data from social media pages of the people are collected like posts, tags, comments etc. are analyzed to get the conclusive information [1].

Social networks work in the way that there are people who create, delete, and update their digital profile and they are enabled to create the relationships to other users of common interest. Every user having its profile and relationships is denoted by digital user's social space. Users may use the social graph to model the users' relationships having different labels [4]. Users communicate and search in text, audio, video, etc. in their space on the same social site directly, or through trusted third party globally, or privately. These sites operate in two aspects client-server architecture where everything is done at server and it its disadvantages is of single point failure, congestion, and load at server. Another is peer to peer architecture which is distributed system where the server's responsibility is shared among peer nodes which itself is a challenge.

Huge amount of data is produced by social sites which are sold at very high price, and the same in turn is analyzed to predict the behavior, trend, demand, nature, etc. of the society and accordingly the policies can be framed for a businessmen, government or individuals. Data can be requested from the data source of the social sites to analyze. Since data is very high in volume, heterogeneous in nature, diverse, rapid therefore specialized data analytic tools are needed. For the same simulators, machine learning, and data mining tools are available such as SPSS, MATLAB, Python, Classifiers, etc.

## II. ARCHITECTURE OF SOCIAL MEDIA NETWORKING SITES

For authorization FOAL (friend a friend) is used to access the personal information of user's portal and TAAS (ticket base authorization system) is used to access the resources. There are two parts of the architecture, access control and ticket service. Ticket service provides the creation, transfer, storage, encryption and decryption, and synchronization. Access control provides refines the users requests to the client and it manages the interface resources of the system. Access controls works in four phases, i.e. data layer, resource management, access control management system, access control engine. The influencing architecture of social sites is proposed in [2], [16].

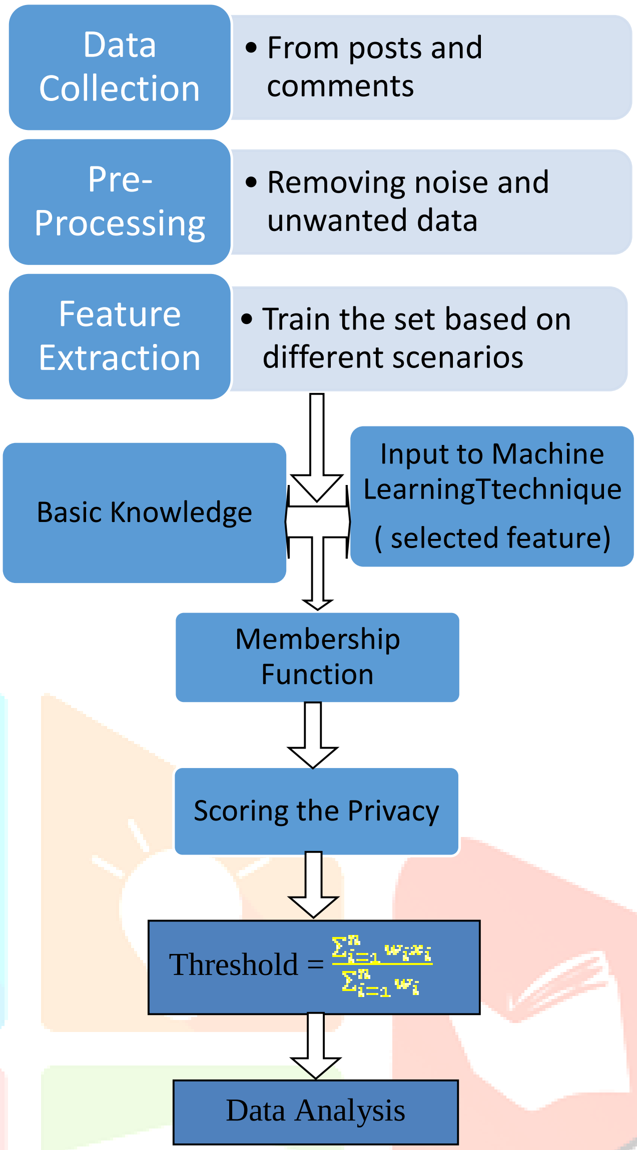
Data Collection
• From posts and comments
Pre-Processing
• Removing noise and unwanted data
Feature Extraction
• Train the set based on different scenarios
Basic Knowledge
Input to Machine LearningTtechnique
( selected feature)
Membership Function
Scoring the Privacy
Threshold = $\frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}$
Data Analysis

Fig. 1: Privacy Process

i) **Data Collection:** Data is requested from the social site such as twitter, Facebook, etc. regarding advertisement, shopping, call date, etc. for research purposes.

ii) **Data Preprocessing:** Data is tuned to be processed further by reducing the noise, removing unwanted data.

iii) **Feature Extraction**: From the users, visible information on site, the model takes the feature space. This model derives information of the user's privacy preferences.

iv) **Data Analysis:** Data analyzing parameters are measured to be used in finding the conclusive information.

For business organization, the proposed architecture [15] is meant for professional networking, professional communication, professional knowledge base, and for professional collaboration:

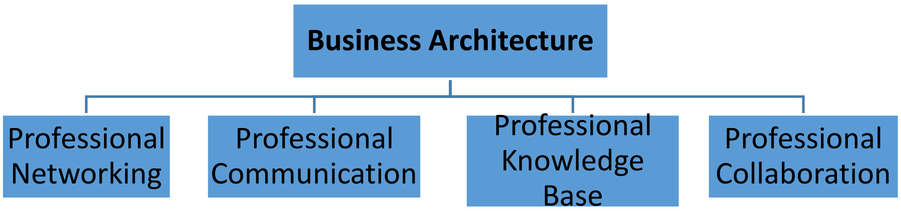
Business Architecture
Professional Networking
Professional Communication
Professional Knowledge Base
Professional Collaboration

Fig. 2: Business Architecture

A model to simulate and observe the behavior of the system and performance is analyzed for the observed behavior [17], [18]:

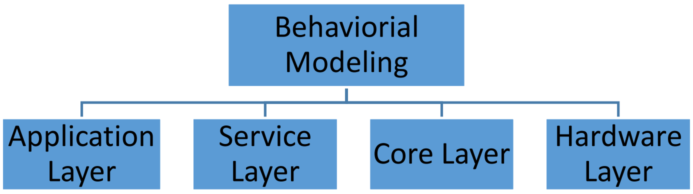

Fig. 3: Behavior Model

i) **Application Layer:** This enables to sharing, games, etc. the message, data, among the users, game sharing events are supported such as special events i.e. sports, cultural, or any other meeting details for gathering.
ii) **Service Layer:** For community connectivity managers and to deal fairness based incentives.
iii) **Core Layer:** It is main layers for dealing in routing, sensing, localizing, the events in users groups.
iv) **Hardware Layer:** It is made of many sensors, camera, microphone, etc. along with wireless technologies for making communities.

## III. SECURITY AND PRIVACY OF ONLINE SOCIAL NETWORKING

### 3.1 Privacy Breaches

Privacy and security of the online social networking is seen in two ways. First the confidentiality of the user's identity must be protected. On the social sites, the identities are not protected because they ask other public identities to verify the user. Second, the user's personal space must also be protected what user communicates to what people. Third is the visibility of the user's profile in public is also a privacy breach. People can get the information about the friends etc. This needs access control in fine graded manner so that private or secret information can be managed properly. There are various privacy attacks to breach the user's personal data, i.e. name, age, address, SSN, date of births, card numbers, etc. because, lot of personal data is floated in communication, among the parties [3], [6].

**Re-identification and De-anonymization:** Anonymized information is advertized or published to be used by researcher for research. But some companies de-identify the personal information from the social network. These attacks can be countered by involving more difficulty in data.

**Service providers' Breach**: Social sites work on client server based architecture. User has to register be a trustworthy with the service provider. Personal information of the users is stored in the server available at service providers' ends. Service providers can sell this data to advertising companies to earn revenue

**Unauthorized Breach:** If service provider provides the unauthorized access to un-confirmed users, it will definitely breach the privacy of the users' personal information.

**Breaches from Third Party**: Third parties are trusted parties; if it starts malfunctioning, personal information of the users is divulged. Re-identification and De-identification of information can be done even when users communicate anonymously.

### 3.2 Security

### 3.3 Attacks on Network Structure

**Attack**: Data is stores in terms of social graph of the users and relationships (links). Any deviation from the model is called attack. There are two types of attacks. One, attack on the identity of the users and second is the attack on the links apart from the other attacks such as availability and accountability. As time is passing social media attacks are increasing rapidly. Broadly attackers can be an insider, a legitimate user snoops in unauthorized areas and or outsiders can attack the infrastructure of the networking sites [5], [7], [12], [19], [21], [22], [23].

i) **Viral Marketing:** People using social networks are naïve and they are sometimes not aware of the virus, worm, and malwares, etc. Therefore security attacks are easily launched on online line social networking. Many people unknowingly open the alluring links and get infected. Spams consume more system resources unnecessarily. Therefore in order to control unwanted malwares defense mechanisms are devised; means good antivirus, anti-spam, software, etc., are needed.
ii) **Anonymization:** Spreading the information so as to make very difficult to be guessed.
iii) **Neighborhood Attack:** Some neighbors may have some private information about the neighbors that may be breached.
iv) **Sybil Attack**: This attack is launched by attacker by impersonating multiple identities. Its counter measures are the trusted users who have certificates will be allowed to join the network only. Privacy model is proposed [14]:
v) **Protection from the Phishing Attacks:** First of all users must check the social site platform, say Facebook platform whether it is correct or not, closely look in to URLs and ensure that they are using the legitimate websites, see some other crucial exclusive information for verification, and keep updating the browsers for new security update [10].
vi) **Keyloggers:** For keyloggers we need to protect our accounts, be cautious before opening the attachments, and try to deploy two level of authentication before signing. Stealers attack the stored passwords into browser history that we should thwart. Session hijacking can be managed by keeping the DNS update, refer only trusted sources to transfer.
vii) **Man in the Middle Attack**: Man in the middle attack can be prevented at server or client side by using the strong encryption techniques. Botnets help infect your system with the help of the other outsider systems and they can be protected by security update and watching the behavior of the users (watchfulness).

Some anti-Botnet tools are available for protection. In Twitter do not let third party to use or access account to avoid phishing and set private and public security settings. Linkedln is a better platform to share and connect professionals. For Skype, we must verify the website before put secret date and the same can be handled from website to control the fraud, spam, and viruses. Phishing is a security concern for Skype. Be alert when some emails prompt you to click or open the links. We must be alert and should update, keep strong passwords, and be extra cautious in sharing, for protection. Cyber Crimes in social media, i.e. Facebook, Cyberspace, Twitter, and Linkedln [9].

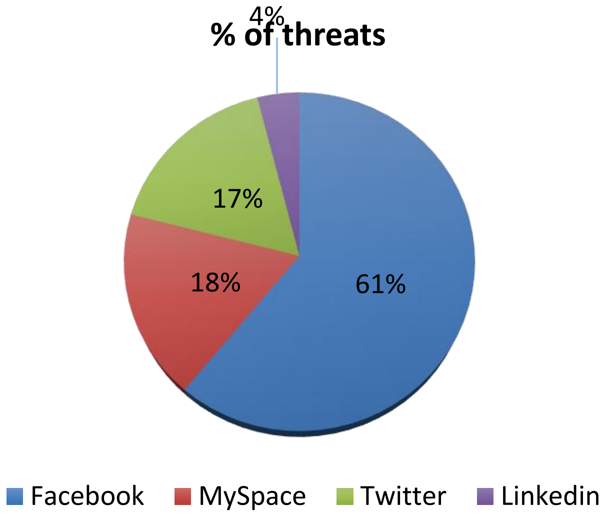

Fig. 4: Behavior Model

### 3.4 Solutions to Security and Privacy

Following are some of the propose solutions [21], [22]:

i) **Anonymitization of Identity in Social Media:** Any person can find the personal information of any other person in the group. For controlling it some solutions are proposed to allow users some restricted access of information. Only authorized users must be made capable to access the sensitive information. For this authorization is achieved through a trusted third party called identity server which keeps the identifying information of all active users in the group. Within a group all users know the identity of each other so they allow sharing their information. But what when an outsider try to masquerade into group. So this outsider first of all must get registered into the identity server for identity and, this identity is assigned for a limited time period. Once it gets identity it would be allowed to share within the group like other genuine group member.

ii) De-anonymity and neighborhood attacks are launched by attackers when they map the personal information from the anonymized information. Sometimes neighbor of the persons whose information is anonymized can re (de)-identify the people because neighbors know personal information of these people [8].

iii) **Cloning the User's Identity:** Some notorious people thief the identity of some naïve people and get personal information by sending threatening requests to friends of intended person.

iv) **Users Profile and Personal Information:** Many users retain default security setting and offer the personal information which in turn maps to identification of the people as a result their personal information is attacked by the attackers and some user's use third party software which also causes the information leakage. Sometimes this profile stealing can be a cross site also. By stealing information from one site, a fake identity is created on another social site to impersonate the people. Some strategies are proposed to control the threats [9] that users must not share their extra personal information because it is risky to be misused. Users must have some knowledge about the cybercrimes and their defense for protection for proper authentication and access control. There must be proper regulations and policies to set in system. If by any reasons, despite of taking all measure system is compromised, some counter tools to get rid of them, must be available to be used. And guidelines are suggested to enhance the security of the users, i.e. strong passwords, limited disclosure, updating of security policies, settings, passwords, don't entertaining the un-trusted information.

v) **Phishing Attacks**: These attacks are launched by fake users by creating fake websites to acquire the sensitive data, i.e. passwords, personal identification, etc.

vi) **Spam Attacks:** This is launched with the help of emails' broadcasting. Context aware Spams take already posted posts to fool the friends of intended users.

vii) **Man-in-the –Middle Attack:** It is made by hijacking the session of https protocol of the website.

viii) **Malwares:** They are created by attackers to get the IDs and send the fake messages on the behalf of intended users. Third party APIs cause the information leakage. Many times these attacks are launched through advertisement whenever users click on these links, (s) he is directed to malicious code. Some links are hidden or shortened and are not visible to naïve users; as a result they also get infected by malicious software as some web applications can also be vulnerable. For examples-Koobface and Twitter worm (profile spy worm and Google worm) are the malware software which was spread across the social media.

ix) **Physical Threats:** Sometimes there can be some physical threats which can harm the employees, office, and infrastructures where websites are maintained.

## IV. PROPOSED SOCIAL MEDIA HANDLING MODEL

Following is the proposed model to navigate and monitor the social media along with the working and functions of its each component:

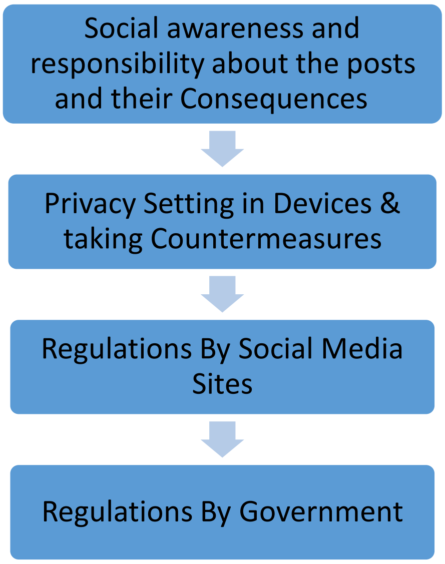
Social awareness and responsibility about the posts and their Consequences
Privacy Setting in Devices & taking Countermeasures
Regulations By Social Media Sites
Regulations By Government

Fig. 5: Proposed Model for Navigation, Monitoring, and Regulating

i) **Social awareness and responsibility about the posts and their consequences**: The awareness about the responsibilities and duties of the citizens, drives about the sensitivity of information regarding privacy issues, national security related issues, and freedom of speech must be disseminated so that people themselves can understand and take corrective measure before posting comments, liking, disliking, etc. [11], [13]. Users are expected to follow the following:

a) Is it really needed to post the post right now? Wouldn't it distort the social harmony?
b) Isn't an intrusion into once constitutional rights, i.e. right to freedom of speech, right to privacy , right to live with dignity, etc..
c) Before forwarding any post people must have some sense of its authenticity about its correctness and source verification. May be the post would be a fabricated post for different intentions.
d) Society must be aware of about what personal information to post and what not to post
e) Does the post not favoring or harming some people?
f) Isn't it influenced by authority or political party?

ii) Privacy and Security Setting and taking the countermeasures: everyone should always configure the best security and privacy settings for thwarting the attacks on device. People must install good quality anti-spam, antivirus, and install the firewalls to protect themselves on social media [20].

iii) **Some Regulations by Social Media Sites:** Particular social media is also expected to employ some checks to see the authenticity of the posts to before they are allowed to upload on social media. For this social media can have a department for dealing all such issues in terms issuing guidelines for the same in public platforms and every user willing to post must be asked to adhere these guideline. Once this department gives clearance, then only user's final post must be uploaded. Social sites are expected to employ the following:

a) A department for checking all issues regarding privacy and security of posts.
b) Users should be allowed to join or open the account with verifiable authentic ids so that they can be traced latter when needed.
c) There must be regular KYUs (Know Your Users) as KYCs is updated in Banks.
d) It should publish its guidelines and instruction for the users to be followed.
e) Social media must check and verify the source and authenticity of the post.
f) Users must be protected in the sense of identity and locations.
g) Users personal data must be protected and must not misused and mishandled.
h) It should block the unverified or un-authentic posts or can flash warning messages so that people can avoid further forwarding these posts.
i) This checking must be so sound that no unverified or unauthentic post should be posted on social site.
j) Some warning should be issued for violations before finally removing the users from the social sites and reporting their case to local administration or local government for any action if any.

iv) **Regulations by the Government:** Apart from the social media government or local administration should also have department or authority see the contents or the severity and the consequences of the post to be uploaded by the users. This authority would scan and see its all aspects, once it clears then only user should be allowed to upload the posts. Government of authority is expected to do the following:

a) Ask social cites to make framework or system to report at regular interval of time.
b) Appoint a liaising officer to deal social media issues.
c) Ensure that users' data must not be misused or mishandled.
d) Can ask the details of the policy violating users from social sites.

e) Can ask social sites to block or unblock some users' accounts.
f) Can demand the track record of some users in the interest of national security in the light of local constitution of the country.
g) Can ask social site to put their servers into country so that local rules can be applied on the users' data.

## V. RESULTS AND DISCUSSIONS

Social media being an important part of our life style, people are connected to it for doing business, making connections, sharing information, etc. People knowingly or unknowingly publish or post their sensitive data and sometimes their publicly published or posted data may map leading to their sensitive personal data. This causes the intrusion into ones privacy. This paper suggested what and how much information is to publish publicly so as to protect ones privacy and to deal with the various attacks, malicious software and counter them. This paper proposes a model to enhance the privacy, security, monitoring, and regulating social media users for its various stale holders.

## VI. CONCLUSIONS

This paper discusses the behavior, weaknesses, privacy, security, and regulatory aspects. Also this paper o proposes the architecture, modeling of proposed solutions and their mitigations.

## VII. ACKNOWLEDGEMENT

In this paper all contributions are made by author only, and this project did not receive any fund from any agency within country or outside.

## VIII. CONFLICT OF INTEREST

This paper is written by the author and this paper does not involve any financial and non-financial interest of any one.

## REFERENCES

[1] Kim J, Hastak M. Social network analysis: Characteristics of online social networks after a disaster. International Journal of Information Management. 2018 Feb 1; 38(1), pp. 86-96.
[2] Zhihan L, Quan Y, Lu L. Decentralized mobile SNS architecture and its personal information management mechanism. China Communications. 2016 Feb 12; 13(2), pp. 189- 199.
[3] Gao H, Hu J, Huang T, Wang J, Chen Y. Security issues in online social networks. IEEE Internet Computing. 2011 Apr 5; 15 (4), pp. 56-63.
[4] Zhang C, Sun J, Zhu X, Fang Y. Privacy and security for online social networks: challenges and opportunities. IEEE network. 2010 Jul 19; 24 (4), pp. 13-18.
[5] Joshi P, Kuo CC. Security and privacy in online social networks: A survey. In 2011 IEEE international conference on multimedia and Expo 2011 Jul 11, pp. 1-6, IEEE.
[6] Ahn GJ, Shehab M, Squicciarini A. Security and privacy in social networks. IEEE Internet Computing. 2011 Apr 25; 15(3), pp. 10-12.
[7] Beach A, Gartrell M, Han R. Solutions to security and privacy issues in mobile social networking. In2009 International Conference on Computational Science and Engineering 2009 Aug 29 (Vol. 4, pp. 1036-1042. IEEE.
[8] Gunatilaka D. A survey of privacy and security issues in social networks. CSE571S: Network Security. 2011 Nov, pp. 1-12.
[9] Gharibi W, Shaabi M. Cyber threats in social networking websites. arXiv preprint arXiv:1202.2420. 2012 Feb 11.
[10] Sushama C, Kumar MS, Neelima P. Privacy and security issues in the future: A social media. Materials Today: Proceedings. 2021 Jan 7.
[11] Trepte S. The social media privacy model: Privacy and communication in the light of social media affordances. Communication Theory. 2021 Nov; 31(4), pp. 549-570.
[12] Beigi G, Liu H. Privacy in social media: Identification, mitigation and applications. arXiv preprint arXiv:1808.02191. 2018 Aug 7.
[13] Nyoni P, Velempini M. Privacy and user awareness on Facebook. South African Journal of Science. 2018 Jun; 114(5-6), pp. 1-5.
[14] Aghasian E, Garg S, Montgomery J. An automated model to score the privacy of unstructured information—Social media case. Computers & Security. 2020 May 1; 92:101778.
[15] Fortino A, Nayak A. An architecture for applying social networking to business. In 2010 IEEE Long Island Systems, Applications and Technology Conference 2010 May 7, pp. 1-6, IEEE.
[16] Peng S, Wang G, Xie D. Social influence analysis in social networking big data: Opportunities and challenges. IEEE network. 2016 Nov 3; 31(1), pp. 11- 17.
[17] Wang Y, Vasilakos AV, Jin Q, Ma J. Survey on mobile social networking in proximity (MSNP): approaches, challenges and architecture. Wireless networks. 2014 Aug; 20(6), pp. 1295-1311.
[18] Nguyen H, Nguyen ML. A deep neural architecture for sentence-level sentiment classification in twitter social networking. International Conference of the Pacific Association for Computational Linguistics 2017 Aug 16, pp. 15-27, Springer, Singapore.

[19] Albulayhi MS, El Khediri S. A Comprehensive Study on Privacy and Security on Social Media. International Journal of Interactive Mobile Technologies. 2022 Jan 1; 16(1), pp. 20-29.

[20] Kumar, R., Kumar, P., & Kumar, V. Design and implementation of privacy and security system in social media. International Journal of Advanced Networking and Applications, 2022, 13(4), pp. 5081-5088.

[21] Bharati T. S., Challenges, issues, security and privacy of big data. International Journal of Scientific & Technology Research. 2020; 9(2), pp.1482-1486.

[22] Bharati T. S., Security Enhancement and Privacy Preserving of Big Data. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, vol.8 issue 10, pp 1754-1758.

[23] Kumar C, Bharati T.S., Prakash S. Online social network security: a comparative review using machine learning and deep learning. Neural Processing Letters. 2021, Feb; 53: pp. 843-861.

## Author's Brief Profile

Currently author is working as Associate Professor in the Department of Computer Science, Jamia Millia Islamia (A Central University), New Delhi. He earned B. Tech, M.E., and PhD in computer Science. He has more than 22 years of teaching and research experience and he has served in many reputed Engineering institutes at various capacities. His area of interests includes Cyber Security, Machine Learning, AI, Databases, IoT & Big data, Theoretical Computer Science, etc.