Al-Rafidain Journal of Engineering Sciences

Journal homepage https://rjes.iq/index.php/rjes

ISSN 3005-3153 (Online)

Cybersecurity in Social Media

Saja Alaam Talib

Control and Systems Engineering Department / Computer Engineering Branch, University of Technology, Baghdad, Iraq

ARTICLE INFO

Article history:

Received	20 May 2025
Revised	16 June 2025
Accepted	12 July 2025
Available online	14 July 2025

Keywords:
Cyber Security
Social Media
Attack
Internet
Network

ABSTRACT

Online social networks have become an inherent part of our lives today. These networks connect millions of people to their friends and family where they can share information using various social media platforms. Many people struggle to manage multimedia files such as audios, videos, and photos because of the inherent threat to privacy and confidentiality associated with these files. Therefore, any personal or sensitive information has the potential to go viral the moment it leaks out. Content that is leaked out can within minutes become a topic of discussion for people around the globe thanks to social networking platforms. The rise in social media use has ushered in a new era of online threats and attacks. Internet bullying, data theft, identity fraud, and phishing scams are just some of the risks that are threatening both individuals and organizations. This report analyses the social media impacts on cybersecurity and their negative consequences as well as measures that should be taken to mitigate the effects. Also, we will explain why proper User Awareness and Education is fundamental for ensuring cyber security.

1. Introduction

Social Networking Services (SNS) provide an online space to meet people of different types whether they are interested in making a real connection with someone or have common interests.

The ease with which people can make new friends and enlarge their circles is unprecedented compared to what it was in the past. Friendship can now go beyond borders, all with the help of online platforms. One can share files as well as chat and even video call directly from their desks or while lounging in bed, using a few taps on a handheld gadget. IoT has the potential to SNS and encourages its development on an even further level.

A crucial aspect of SNS is its ability to enable users to share photos, videos, blogs, writings, and other files with one another.

As far as different SNS platforms are concerned, nowadays Facebook and twitter have the highest number of users as these two platforms experienced a greater level of acceptance due to ease of interaction between users. Over the past few years, billions of people have been using these platforms constantly, in addition to some other famous media apps like WhatsApp, Viber, Imo, Skype, etc. [1].

To become these service users, a profile needs to be created with which a person can interact with their loved ones. Users can verify and modify their information on their own when they deem necessary. Users can also view other users' profiles and even communicate with other users based on their individual preferences. Social networking services SNS allows for the elimination of the political and geographical economic borders [2].

SNSs can fulfils the needs of searching for entertainment or job opportunities, or even

Corresponding author E-mail address: sajaalaam@yahoo.com

https://doi.org/10.61268/zwxnbm29

education among other things. Even though SNSs have achieved heightened popularity and usage across the world, there are still notable dangers associated with it, as these sites have become common victims of cyber-attacks.

It is undeniable that often the attackers accomplish certain objectives by targeting the users' delicate personal information through certain methods, such as social bots spam, malware, identity theft, etc. These users use the platform to carry out some phishing attacks as well [3].

These SNS can sometimes provide attackers with exploitable cyber-attack doors. It also examined different SNS types of attacks like impersonation, malware attack, account or ID hacking, etc., and it shows that a well-orchestrated attack can pose a grave risk of destruction of a targeted enterprise networks and incite violence among the users. Figure 1 below shows different types of SNS users [4].

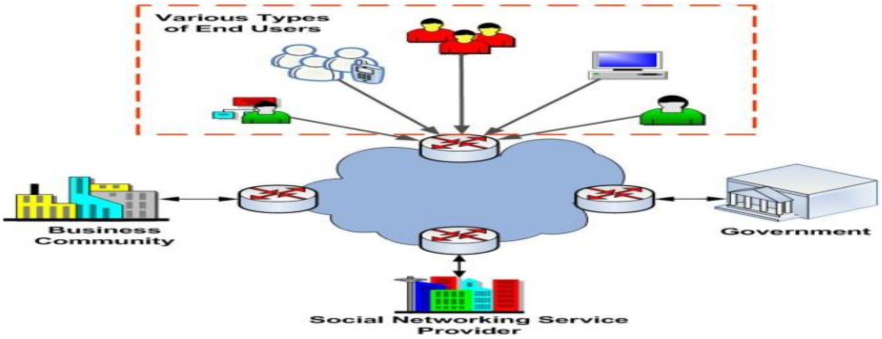

Figure 1. Various types of users use SNS.

These days, the attackers seem to focus on breaking into significant data repositories sites such as national security systems, official websites, banks and so on as these perpetrate serious cybercrimes.

Attackers looking for weak users to exploit will obtain the user's location or identity for use personally for nefarious deeds. Although many SNSs provide protection to users such as Twitter which disallows sensitive information to be released publicly, some users are allowed to disclose sensitive information daily which can ultimately be analysed by Wicked attackers. In fact, a user reveals many personal issues like choices and preferences when talking about their life. Routine problems need a drastic measure problem solver [5].

The growing realm of ordinary and advanced cyber threats posed by criminals who exploit multimedia content uploaded by people daily call for attention. That is the reason many security firms and several other researchers have come up with some rather fascinating solutions aimed at reducing these issues: Steganalysis, digital oblivion, and watermarking for the protection of the offenders and users who share multimedia content. Phishing and spam boots can also serve as traditional defence mechanisms against online cyber threats.

The SNS security issue can be addressed with the help of moderation tools that can actively enforce privacy policies, authentication provisions, and social protection systems like Monitor Minor. This work reveals an intensive examination of the issues outlined above and technological responses available in this area [6].

This paper looks at measures which individuals and organizations can undertake to protect themselves from online threats and attacks. It looks at the dangers that may be associated with the usage of social media. This research also examines how government and social media companies can enhance general awareness and practice of cybersecurity [7].

2. Aim of the work

The thesis will investigate privacy and security questions on social media by users today. These components will be explained in detail identifying workable solutions, legislative actions needed and what social media companies should do to protect the helpless social media user. It also seeks to educate social media users on the risks they face and enable them by showing them ways to address these risks.

3. Social media

Social media is a form of social interaction that allows users to create content and share it through online communities and networks. Different types of social media include websites and applications for forums, micro blogging, social networking, social bookmarking, social curation, and wikis [8].

There are Some Examples of Social Media Platforms [9]:

• Facebook: arguably the best platform to share instant photos and videos directly socializing with family and friends. Users can use Facebook to send messages, share posts, add locations, stream live videos, and much more, all at no charge.

• Twitter: another social networking platform which lets the user broadcast in the form of short calls Tweets that can be done on multiple devices and platforms.

• Google: an application which is also used as a virtual social platform that facilitates designing and sharing of information by users over the internet simultaneously.

• Instagram: is again a popular social networking application and ads can be viewed by millions of active users daily. Users can share edited media files and geotag them, which includes hash tagging and setting filters.

• YouTube: This is an application that everyone can access by Google, which was released in 2005. Users have the capability to view, upload, and share videos on YouTube.

• Linked in is the most popular professional social networking site used all over the world, especially by business communities. Figure 2 below shows the average of using social media sites in different places around the world.

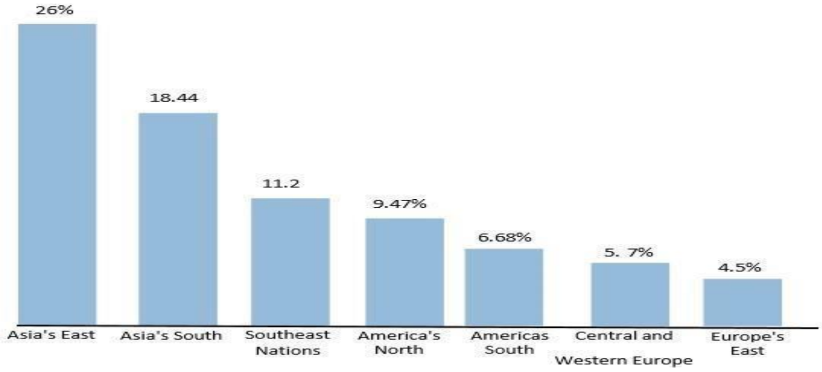

Figure 2. Distribution of social media users around the globe [10]

Social media is the most widely practiced form of social media. People still turn to Facebook, Twitter, and LinkedIn, even when they don’t have a specific purpose to connect with their peers, follow the news, or expand their professional circles. In addition, other short social networking services such as YouTube and TikTok are growing in popularity.

The number of global TikTok users was predicted to surpass a billion and a half in 2022 [11]. Figure 3 below shows the ration of people who using social media from 2017 to 2025 in billions, it clear that the usage of social media increases from 30.4 in 2013 to 168.6 in 2025.

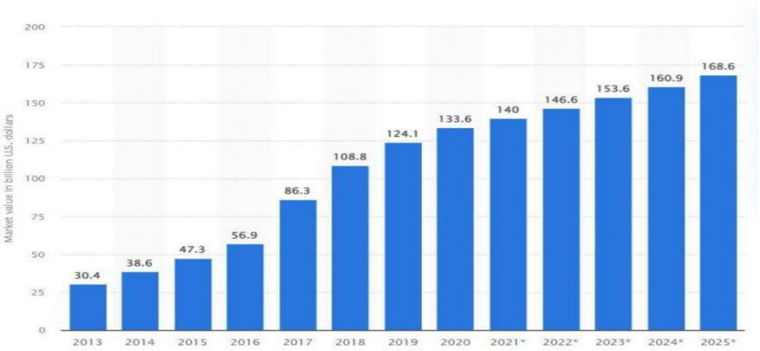

Figure 3. World social media users from 2017 to 202٥ in billions [10]

Figure 4 below shows different types of social media sites with their usage in millions of people all over the world. Facebook is most usage site in the world ،On the contrary of Pinterest Which shows the least used in the world.

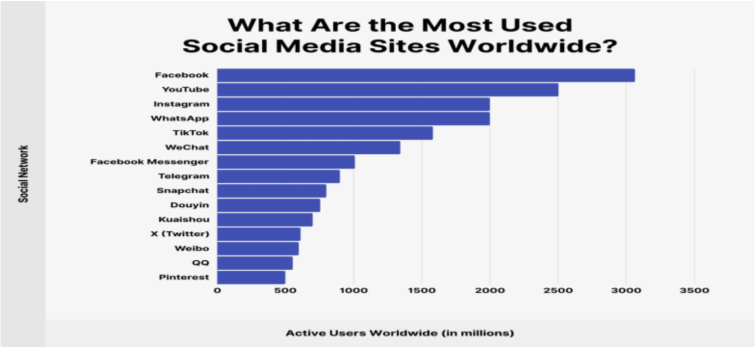

Figure 4. Social media networks with their global usage in millions [10]

Social media networks can be classified into four categories depending on the nature of their communication [12].

- Textual-based platform: Primarily utilized for sending and receiving social text messages. Excellent instances are the messaging platforms.
- Visual-based platforms: Used for social picture exchanges like sending and receiving pictures. The primary illustration is the flyer platform.
- Multimedia Platforms: Social activities that comprise of sending and receiving video data like YouTube. It is very popular.
- Hybrid based Platforms: Integrates features of several text, pictures and video platforms. Facebook is one such example.

Table 1 depicts summary and analysis of different categories of social media platforms in relation to their level of interactions support.

Table 1: Classification of social media platforms

Category	Usage
Email Service Providers	The first social networking site was built to support the Internet, allowing interpersonal interaction via email services such as Yahoo Mail and Microsoft Outlook.
Online platforms for social interaction and connection	Social networking platforms such as Facebook and Twitter are popular for connecting with friends, family, brands and potential clients.
Discussion Platforms	Reddit and Naira Land serve as discussion forums for serious academic and focused conversations for people of similar interests and views.
Blogging platforms	People can create and share articles such as reviews and essays through blogs, which are then shared via email, social networks, websites, and feeds.
instant Messenger Platforms	Social media instant messengers like Twitter (X) and Yahoo Messenger allow text chatting in real time, facilitating real communications.
Multimedia Platforms	Media such as YouTube serve as distribution channels for text, pictures, audio, and video for social media users and subscribers.
Auction Systems	Auction Platforms: Related to the buying and selling activities of goods and services like eBay.
Cooperate Social Platforms	Companies have started to add social elements to their online applications such as blogs to better reach their target audience with their products and services.
Educational/Professional Platforms	Platforms for education and work such as Meet, Zoom or LinkedIn connect people to share information through charts, files, live meetings, and even with social media professionals.
Gaming applications	Gaming applications give social media users a chance to entertain themselves through online gaming, including gambling, like King Bet.
An Engine search	Unlike the previous paragraph, where I concentrated on a single tool to socialize with others, this section will point out a double-edged tool which is Google, for it’s a search engine and social media platform all in one.

4. Social media and cybersecurity

Because of the high amount of sensitive data shared by users, a social media site is a primary target for cybercrime. This data can serve as a basis for conducting identity theft, phishing, malware, and social engineering attacks.

When identity theft happens, the person claiming to be a certain victim uses the victim’s sensitive information pulled out from the social media account. Phishing attacks refer to phone calls, emails, or messages purporting to be from trusted sources, aimed at obtaining sensitive information such as passwords and credit card details.

This type of attack also relates to malware because these attacks occur when transferred files containing unwanted and malign computer programs onto the device which can extract sensitive data or remotely access the user's device. Social engineering on the other hand, attempts to trick the public into giving out private details or clicking on some harmful sites [13]. Social media platforms are very popular and widely used across different audiences mainly due to their unique communication and interaction features. Unfortunately, users are regularly falling victim to fraud as private information is easily accessible by the public.

Cybercriminals as well as online fraudsters employ this information to launch multiple attacks such as phishing, creation of malware, and social engineering attempts. As social media websites operate in an ever-shifting world, the threats and dangers are evolving which makes social media an equally daunting task for cybersecurity experts [14]. Social media has increasingly become a target for hackers.

A wide range of personalized attacks, including phishing attempts, malware distribution, and even personal information theft, can be conducted through social media as personal data such as emails, phone numbers and geographical locations are readily available on these platforms. Cyber criminals harvest these details to craft communications that are extremely sophisticated and appear to originate from reputable contacts. Furthermore, social media is a breeding ground for impersonating accounts and profiles which can be leveraged for malware distribution and private information theft [15].

5. Social media associated risks

While social media is highly beneficial, it poses some risks that can affect individuals and

organizations differently. Here are some of the common risks that are associated with social media use [16]:
1. Social Media Fraud: Different social media platforms invariably ask users for personal details. Receiving fraud and identity theft crimes are all imaginable for hackers and cybercriminals.
2. Online Harassment: Bullying and harassment is rampant on social media and can be particularly damaging to the target of such malice.
3. Social media hacking accounts: One of the more common forms of hacking is hacking social media accounts where people can get private information and/or launch more hacking efforts.
4. Phishing attacks: It is known that hackers use social media channels to deploy phishing attacks by building web pages and email addresses to harvest information.

6. Common types of cyber attacks

A social media cyber-attack can occur in many types and scenarios. A pecuniary phishing attack happens when Cybercriminals use phone emails or messages to reconstruct the personal accounts of victims by tricking them into revealing personal details like passwords or credit card numbers.

Of the various malware attacks such as attempts to infect the user’s device through harmful software which is designed to harvest sensitive information or take control of the device, prominent ones are lower and higher chronic severe lead poisoning.

Social engineering attacks are tactics that use deception to manipulate people into divulging confidential information. Anyone with the intention of social media cyber-attack may be able to, therefore, it is imperative for the user to be vigilant against and take steps to safeguard against phishing scams [17].

7. Safeguarding digital threats and security breaches [18]

Both people and businesses must possess a proactive approach to cybersecurity to protect themselves from online threats and attacks. One possible method is multi-factor authentication (MFA) which offers a protective layer to user accounts barrier against unauthorized access. This may help in restricting access to private and sensitive information.

Another important measure which can help in minimizing problems cybercriminals can take advantage of is frequent updating of software and patches for security. User awareness and education are also a vital component of sustaining cybersecurity, together with technical measures.

Users ought to be trained on basic online security measures such as the avoidance of chances links or communications in addition to rotating passwords frequently to ensure that the most current security threats targeted towards them are dealt with; also, organizations can set up specialized security sessions for them.

An assortment of methods can be utilized by individuals and organizations to shield themselves from online threats and attacks like:

- Strong passwords: Users should set aside strong, unique passwords for each of their social media accounts.
- Two-factor authentication: Users have the scope to enable two-factor authentication on their accounts and this provides extra security by requiring a second step such as a code sent via text to a mobile phone.
- Cautious When Clicking on Links: Users need to exercise caution when clicking links because it can be damaging if they are not certain of the source. Malicious links can infest a user’s device with malware or redirect them onto a phishing website.
- Keep Software Updated: Software is essential on every device and should be updated consistently as it covers security holes. This includes operating systems, antivirus software, and web browsers.
- Limit Personal Information Sharing: Users should refrain from sharing an overabundance of personal content on social media profiles. Sensitive information such as home address, phone number or banking details should also be omitted.
- Privacy Settings: There are various settings in social media which can be adjusted to

control the level of privacy and protect users from cybercriminals.

- Stay Aware: Users must remain alert and need to flag any questionable behaviour or messages for the support team to investigate. They ought to track their accounts on a regular basis to identify any unusual access.

8. Functions of government institutions and social media companies

Because of the responsibility they have in ensuring cybersecurity, social media companies are supposed to undertake measures aimed at protecting their clients from attacks and threats on the internet. Below are some of the steps that social media businesses can take [19]:

- By enabling encryption on online social platforms, cybercriminals will find it harder to access the user's private information. It is easier for hackers to target users whose data is unprotected, so social media organizations can easily shield private data to users become less vulnerable.
- Users should be educated on the potential dangers and Cybersecurity threats on the internet, and the safe practices needed to protect themselves from it. Online social platforms can moderate lessons and guidelines on how users can protect themselves from a plethora of threats online.
- Social Media platforms require rules to be in place that ensure the safety of users from violent attacks and set high standards for dealing with online threats and attacks.

Social media companies must follow a set code of conduct and work under regulations to perform successfully on the business. Among various other actions, they can help maintain cybersecurity by doing this [20]:

- Supervision: the activities of the media companies in question will be investigated by the government and will be expected to meet the standards provided regarding Cybersecurity measures.
- Educating the General Public: As Nurmi and Weir (2018) argue, authorities can guide citizens on the dangers that lurk on the internet and provide with resources on preventative measures to guard themselves against such cyber means.
- Collaboration: Governments can partner with social media companies to formulate and implement cybersecurity strategies designed to protect users from cyber threats and attacks.

9. Recommendations

This section provides various measures that can be taken to ensure that the user's information is secure, including the following [21].

- A company should take the necessary steps to make sure that the e-mails are easily identifiable and not lost in a sea of spam or phishing attempts.
- Both individual users and companies need to invest in good quality anti-viruses so that they can effectively filter out and block malicious websites.
- Every website should perform some form of authentication to mitigate unauthorized access to sensitive personal information from attackers.
- Social networking websites that require user private information should ensure security using these techniques: group key exchange, data mining, and encryption to name a few.
- The government should initiate training and advertising seminars and other competitions to encourage people to actively educate themselves on cyber security. The government should conduct publicity campaigns and programs about cyberspace including seminars, contests, and exhibitions.
- Social networking sites that allow the user to modify the privacy security settings have features that assist in account protection. Such is the case with Facebook privacy settings where privacy basics are divided into subcategories.
    - Who can see my stuff is a setting on top of the list of priorities for Facebook users as it allows the person to restrict the audience that can access their posts.

Public posts can be misused for fraudulent activities.

  - Login-Alerts: With this option, users are informed whenever there is a log-in from a new/strange device or browser.
  - Third party authenticator- This new setting to Facebook allows a user to create Facebook security code that can be used to authenticate any third-party app.
  - How others who have access to a user's account can engage with the user: This is helpful in enabling users to control activities of other users that affect his or her profile. And manages tags, unfriend, or block options.
- web browser security settings:
  - Users must have respective browsers updated with the latest version and enable automatic updates for the browser.
  - Restrictions on plug-ins, pop-ups, and phishing websites should be imposed.
  - Browser settings should be optimized not to save passwords.
  - Third party cookies should be turned off.
  - Browser specific settings:
  - ❖ Firefox: No Script add-on should be installed.
  - ❖ Safari: Java should be turned off.
  - ❖ IE: Security zones should be configured.

10. Conclusion

Social media is now part and parcel of our lives, this becomes problematic regarding our cybersecurity. Social media contains a lot of personal information which is used by cybercriminals to easily launch a targeted attack and steal sensitive information. There is a need for everybody, both individuals and organizations, to adopt measures to prepare themselves against these threats' behavioural adjustments, along with implementing technological solutions to improve security online must be established. This will ensure that social media remains free from these issues.

Sneak-and-peek warrants, and primary use of social media has neatened things up for cybercrimes. Cyber Crime remains to be a global problem and imposes dangers to the economic and national Security of any country. Organizations in both private and public sectors from healthcare, education and telecommunications, defence, and banking are vulnerable.

Therefore, to eliminate cyberspace crime, organizations must implement adequate security steps and holder of personal details, usernames, passwords, etc. draw up a timid and only dissolve for identity tricking verifiable. The cyberspace is become a new battlefield for cyber criminals and terrorists. Hence, there is a need for countries to come together to tackle the growing cyber menace collectively.

References

[1] K. Thakur, T. Hayajneh and J. Tseng, "Cyber Security in Social Media: Challenges and the Way Forward," in IT Professional, vol. 21, no. 2, pp. 41-49, 2019https://doi.org/10.1109/MITP.2018.2881373

[2] R. P. Khandpur, T. Ji, et al, "Crowdsourcing cybersecurity: Cyber attack detection using social media, "In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, pp. 1049-1057, 2017. https://doi.org/10.1145/3132847.3132866

[3] E. Van der Walt, J. H. Eloff, and J. Grobler, "Cyber-security: Identity deception detection on social media platforms," Computers & Security, Vo.78, pp.76-89, 2018. https://doi.org/10.1016/j.cose.2018.05.015

[4] K. M. Carley, "Social cybersecurity: an emerging science," Computational and mathematical organization theory, Vo. 26, No.4, pp. 365-381, 2020.

[5] H. Zamir, "Cybersecurity and social media," In Cybersecurity for Information Professionals, pp. 153-171, 2020.

[6] D. R. Alqurashi, M. Alghizzawi, and A. Al-Hadrami, "The role of social media in raising awareness of cybersecurity risks," In Opportunities and Risks in AI for Business Development, Vol.1, pp. 365-376, 2024. https://doi.org/10.1007/978-3-031-65203-5_33

[7] M. Khan, and S. Haque, "Cyber Security and Ethics on Social Media," Journal of Modern Developments in Applied Engineering & Technology Research, Vol.1, No.2, pp.51-58, 2017.

[8] K. M. Carley, G. Cervone, et al," Social cyber-security," In International conference on social computing, behavioral-cultural modeling and prediction and behavior representation in modeling and simulation ,pp. 389-394, 2018. https://doi.org/10.1007/978-3-319-93372-6_42

[9] K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, "Cyber security challenges and its emerging trends on latest technologies," In IOP Conference Series: Materials Science and Engineering, Vol. 981, No. 2, p. 022062, 2020. https://doi.org/10.1088/1757-899X/981/2/022062

[10] L.K. Ahmed and R.D. Rashid, "Advanced security: The application of social media and their security," In ITM Web of Conferences,Vol. 64, p. 01006, 2024.

https://doi.org/10.1051/itmconf/20246401006

[11] S. Hendawi, S. AlZu'bi, Mughaid, et al, "Ensuring cybersecurity while leveraging social media as a data source for internet of things applications," In International Conference on Advances in Computing Research , pp. 587-604), 2023. https://doi.org/10.1007/978-3-031-33743-7_47

[12] N. Z. Khidzir, K. A. Mat Daud, et al, "Information security requirement: The relationship between cybersecurity risk confidentiality, integrity and availability in digital social media," In Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016) Theoretical and Applied Sciences , pp. 229-237, 2018. https://doi.org/10.1007/978-981-13-0074-5_21

[13] A. Hamid, M. Alam, et al, "Cyber security concerns in social networking service," International Journal of Communication Networks and Information Security, vol.12, No.2, pp.198-212, 2020.

[14] F. B. Salamah, M. A. Palomino, et al, "The importance of the job role in social media cybersecurity training," In 2022 IEEE European Symposium on Security and Privacy Workshops , pp. 454-462, 2022.
https://doi.org/10.1109/EuroSPW55150.2022.00054

[15] R. Goolsby, L. Shanley, and A. Lovell, "On cybersecurity, crowdsourcing, and social cyber-attack," Policy memo series, Vol.1, 2013.

[16] N. Kashmar, M. Adda, et al, "Access Control in Cybersecurity and social media," Cybersécurité Médias Sociaux, pp. 69-105,2021.

[17] S. Ahangama, "Relating social media diffusion, Education level and cybersecurity protection mechanisms to e-participation initiatives: Insights from a cross-country analysis," Information Systems Frontiers, Vol.25, No.5, pp.1695-1711, 2023. https://doi.org/10.1007/s10796-023-10385-7

[18] R. S. Kunwar, and P. Sharma, "Social media: A new vector for cyber attack," In 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring), pp. 1-5, 2016.
https://doi.org/10.1109/ICACCA.2016.7578896

[19] E. Ozkaya, "Cyber Security Challenges in Social Media, "2018.

[20] N. Ahmad, A. Arifin, et al, "Parental awareness on cyber threats using social media," Jurnal Komunikasi: Malaysian Journal of Communication, Vol.35, No.2, pp.485-498, 2019.

[21] M. Huda, L. Sutopo, et al, "Digital information transparency for cyber security: critical points in social media trends," In Future of Information and Communication Conference, pp. 814-831, 2022. https://doi.org/10.1007/978-3-030-98015-3_55