Advanced security: The application social media and their security

Lana Kemal Ahmed [1*], *Rasber* Dhahir Rashid[2]

[1,2] College of Science, Department of Computer science & information technology, Salahaddin university, Erbil, Iraq

Abstract. Social media networks are a vital platform for the virtual community, connecting billions of people for mutual interaction. However, hackers are aggressively exploiting these platforms for malicious intentions. Despite the implementation of preventive measures, hacker activity has surged, leading to the need for a social media intrusion detection system. Online social networks have provided users with conveniences but also pose significant threats to their security and privacy. Users' attempts to adjust their privacy settings are less than their efforts to implement other security measures. A significant proportion of individuals using social media platforms have limited technical expertise, resulting in less apprehension about the privacy implications of their personal content. To address privacy concerns, a comprehensive set of well- defined policies should be established, including robust passwords, periodic password changes, caution when sharing personal information, the importance of antivirus software, and proprietary software use. Machine learning algorithms can be employed to examine user sentiment, identify deceptive news, and combat child trafficking. Researchers are currently investigating the incorporation of improving cyber security of social media platforms by using artificial intelligence, focusing particularly on adversarial machine learning. The growing popularity of AI for Good project and the emphasis on Fair AI and Bias in AI highlight the need for further research on how these fields can be used in relation to the social media. This research provides a thorough analysis of the most recent advancements in social media security and dependability, presenting a groundbreaking approach to enhance security and dependability. Organizations must safeguard information broadcasted on social media due to frequent security breaches, which can hinder economic growth.

1 Introduction

Over a billion people use online social networks, or OSNs, as their main communication tool at the moment. On OSN, users may establish a profile that includes their name, age, location, interests, and other details. Social media obviously helps with this, but the main goal is still to unite individuals who have similar interests. An online social network was originally made

* Corresponding author: klanamantik@gmail.com

available on his Six Degrees website in 1997. Users may build profiles and communicate with friends using it. OSNs are commonly classified into two categories: specialized sites and general-purpose sites. Users may connect and exchange media, including photos, videos, and music, on websites like Facebook, Google+, and Myspace [1]. Social media networking sites offer a way to improve the efficiency of online sociability within the international community. Because of this, a growing number of social media users view these platforms as their virtual homes and save private information about them in their databases. Information security is becoming a serious problem due to the world's growing reliance on social media networks. Malicious acts and digital versions of the majority of traditional crimes are probably going to occur amid all these incredible advancements. when malicious individuals and hackers use social media sites to harm other people. A hacker is a cyber-criminal with expertise in virtual terrorism who employs a range of hacking techniques to target both the general online community and the authorized members of the Social Media Network His Platform (SMNP). Sites on social media and people are the main targets of this cybercrime. Given how easily private information is available on social media, some users might wish to keep it there. He employs a number of strategies to keep hackers off his social media network platform. Two succinct recommendations in relation to data warehouse databases, Competent hackers are coming up with new ways to sneak into social media networks despite intrusion detection systems [2]. Globally, there are 3.4 billion active social media profiles at the moment. Personal social network accounts are still more vulnerable, even with major advancements in information security measures. The reasons behind those sorts of instances include consumers' ignorance of the security measures put in place by firms for their personal accounts. Information security experts also suggest a few methods for protecting user accounts. Even though the aforementioned technologies greatly boost account security, social media does not automatically apply them [3]. However, little study has examined the potential impact that users' actual behavior on social networking sites may have on security. In this study, we investigate the correlation between users' real on-site activity and their perceptions of security risks on social media. Additionally, we recommend developing a system that can notify users of security threats and motivate them to employ recommended riskreduction techniques when utilizing social media. [5]. This study looks at social media security protocols and possible uses of artificial intelligence (AI) in this field. This piece examines a few of the current issues caused by resourceful hacking and the dissemination of false information on social media platforms. Specifically, machine learning techniques for retrieving pertinent data and assisting individuals will be showcased, in addition to utilizing AI to tackle the difficult task of identifying false information. We'll talk about issues like limiting access to the social-media platform, and other privacy concerns that can surface from examining social media data. One potential flaw in the machine learning methods used to analyses social-media data is [4].

2 Literature review

The technique used for the review paper on "Social Media Applications and Their Security Systems" included a meticulous examination of the most recent scholarly publications in this domain, with a specific emphasis on studies completed during the preceding three years. If there was a lack of comprehensive data on a particular issue over the last three years, we included pertinent studies from previous years throughout the data gathering phase. The paper selection process for this review was conducted with great care, with a strong focus on using reliable sources. The papers were obtained from credible scientific publications and reliable sources such as IEEE and Science Direct. This methodology guarantees that the material provided in the review is derived from trustworthy and current research discoveries in the realm of social- media apps and their corresponding security measures.

2.1 Application for social media

Social media platforms are web-based programmers designed to disseminate content created by users. A social media network is a website that facilitates online relationships between friends and admirers with similar interests. It deals with the sharing of information and multimedia files between users on related platforms via electronic networks, most notably the internet and cyberspace. This platform, which is also a fantastic instrument for a social and personal engagement, has grown geometrically to become a dynamic conduit for official and corporate communications. Hundreds of social media platforms are used today for a wide range of objectives; the most popular ones are listed below [2]:

i. Facebook application: provides a range of services, such as an online marketplace, voice and video chatting, video sharing and viewing, online advertising, voice calling, instant messaging, and virtual gifts for teenagers and adults. Facebook advertising has the potential to reach 14 billion people [2].

ii. (X)Twitter application: are brief communications composed of characters that users may write and read on the social media site Twitter. It centers on the idea that people who choose to follow another Twitter user may observe the tweets that user sends out as followers [2].

iii. Insta-gram application: lets users share media files that have been Geographically tagged, hash tagged, and subjected to filter editing. Insta-gram ads may reach billions of the million's daily viewers of Insta-gram stories and billions of active users [2].

iv. YouTube application: It's an application that anyone can use to see, upload, and share videos on YouTube, published by Google in [2].

v. LinkedIn: is a professional networking social media website. Professionals and job seekers can utilize this social networking service, which allows users to interact with both other users and non- users [2].

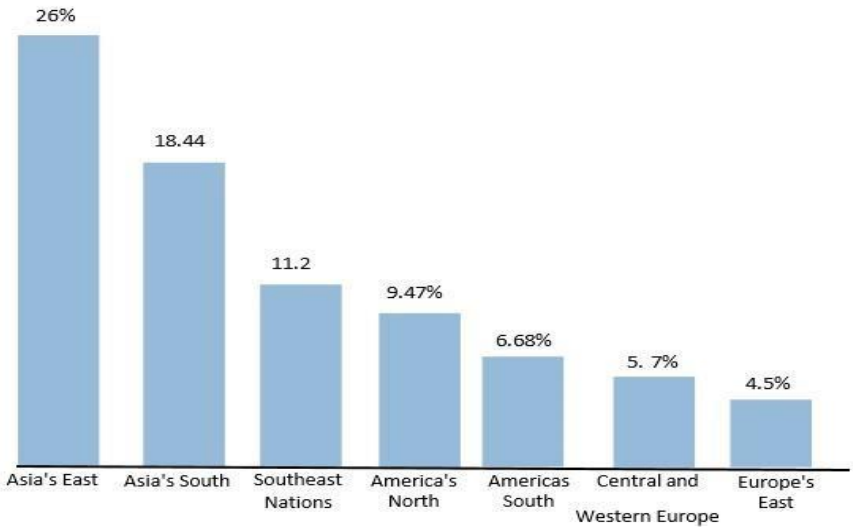

Fig. 1 The Regional breakdown of the global platform of social media users

Though there are many other kinds of social media, social networking is the most popular. Facebook, Twitter, and LinkedIn continue to draw people, regardless of their needs—to stay in touch with friends, keep up with current events, or grow their professional network.

Furthermore, among the popular social networking sites, social video platforms like YouTube and the short-form phenomenon Tik Tok have been making their mark. The global Tik Tok user count was predicted to reach over one and a half billion in 2022 [5].

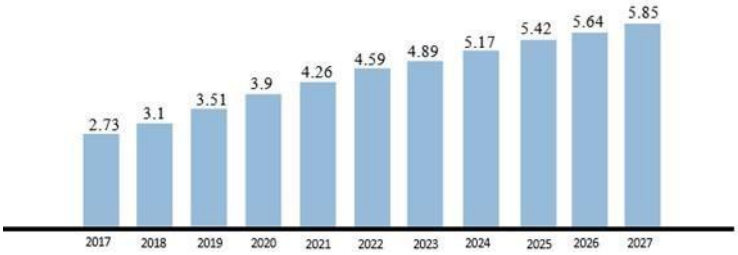

Fig. 2 Global social media user count from 2017 to 2027 (in billions)

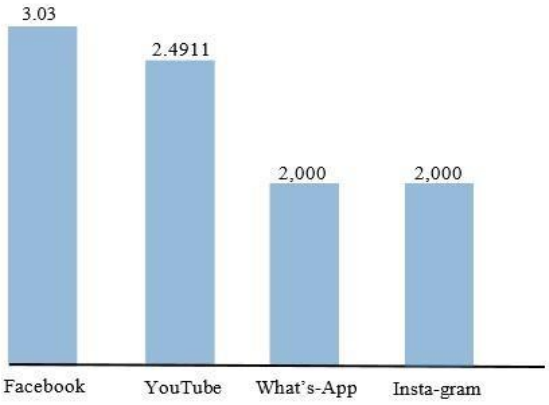

Fig. 3 The social media networks with the most global usage in 2023 (Number of users in billion) [5].

Social media networks may be divided into four categories based on the kind of data they exchange [2]:

i. Textual-based platform: used for social text messaging, including sending and receiving. The message platforms are excellent instances [2].
ii. Visual-based platforms: utilized for social exchanges including pictures, such as sending and receiving pictures. The flyer platform is a prime illustration [2]. iii. Platforms that use audio and visual elements: or social activities using videos, such as sending and receiving video data. A common illustration is the YouTube [2].
iv. Hybrid-based platforms: This platform combines characteristics from many textual, visual, and audio-visual platforms. Facebook exemplifies this [2].

Table 1 provides a concise overview of the various categories of social media platforms based on their level of support for social interactions.

Table 1. Classification of Social Media Platforms

Category	Usage
Email Service Providers	The initial social media network laid the foundation for the Internet, enabling interpersonal communication through electronic mail platforms like Yahoo Mail and Microsoft Outlook.
Online platforms for social interaction and connection	Social networking websites like Facebook and Twitter are commonly used to establish connections with friends, family, brands, and target customers.
Discussion Platforms	Discussion platforms like Reddit and Naira Land are designed for scholarly inquiry and focused discourse among individuals with similar interests and perspectives.
Blogging platforms	Authors can publish articles, opinions, or product evaluations on blogging platforms, which can be distributed through social networks, email, websites, feed syndications, and more.
instant Messenger Platforms	Instant Messenger platforms like Twitter (X) and Yahoo Messenger enable real-time text chats, enabling instant messaging and communication.
Multimedia Platforms	Media platforms such as YouTube facilitate the distribution of diverse forms of content, including text, images, audio, and video, to both social media users and subscribers.
Auction Systems	Auction Systems: Concerning the sale of goods and services, for example, eBay , etc.
Cooperate Social Platforms	Businesses are increasingly incorporating social components into their online applications, such as blogs, to effectively engage their target market with their products and services.
Educational/Professional Platforms	Academic and career-oriented platforms like Meet, Zoom, and LinkedIn enable information exchange through charts, resource uploading, live meetings, and connecting with specialists in the social media business.
Gaming applications	Gaming applications offer social media users, a platform to play games for entertainment, enjoyment, or gambling, such as King Bet.
An Engine search	Web search engines like Chrome and Google are essential tools for enhancing online social interaction, allowing users to easily locate a necessary material.

2.2 Attacks and threats on social media

Social media platforms are vulnerable to various attacks aimed at stealing users' identities, compromising privacy, and compromising trust, with several prevalent attacks currently targeting these platforms, some type of attack are:

i. Spam Attack: Attackers can transmit unsolicited data by acquiring user communication details, leading to network congestion and financial expenses for service providers and users [6].

ii. Malware assaults on social networking sites are increasing, with attackers sending scripts containing malware, potentially stealing personal information or redirecting users to fraudulent websites [6].

iii. Sybil attacks disrupt social media platforms, spreading malware and false information through fraudulent accounts. Enhanced authentication during user registration is crucial to prevent these attacks [6].

iv. Social-spoofing is a cyber-attack using psychological tactics to gain sensitive information or unauthorized access to systems or accounts. It involves impersonating a victim's friend or using fake websites. Vigilance and careful data examination can reduce attacks [6].

v. Impersonation: Assailants build counterfeit profiles to masquerade as authentic individuals, utilizing authentication techniques during account registration. Replicating these attacks can result in severe injuries [6].

vi. Hijacking involves assuming control over another person's profile, increasing the risk of hacker attacks. It's advisable to use secure passwords and regularly update them to prevent dictionary attacks [6].

vii. Adversaries use accounts to send fraudulent requests, enlarging networks and gaining privileges. Users must exercise responsibility on social media, as a complete prohibition is impossible [6].

viii. The assailant uses facial and image recognition algorithms to gather information about the target and associated profiles, including the victim's acquaintances and relatives, to collect media content [6].

ix. Malicious individuals target social networks' structural frameworks, primarily through DDoS attacks, aiming to prevent users from using services and quickly impacting their infrastructure [2].

x. Spoofing-attacks are hacking techniques where the hacker uses attractive bait to ensnare the target, often involving the disclosure of personal information for abuse [2].

xi. The Evil Twin attack involves a hacker posing as a genuine user, creating an account mimicking their profile, and using social networking to send friend requests, gaining access to their friends [2].

xii. Cyber-bullying is the use of offensive messages or information on social media to harass or intimidate individuals, often with the intention of blackmailing or threatening them [2].

xiii. A hacker intentionally assaults a user, coercing them to disable security measures to bypass the platform's physical safeguards, posing a bodily threat [2].

2.3 Possible Risks and Privacy Issues on Social Media Platforms

Privacy analytics considers the benefits and risks of users' disclosure of personal information on social networking platforms. Privacy breaches can occur through ineffective protective measures or unauthorized access. However, if individuals have the choice to choose their data's disclosure, appropriate policies can address protection issues. The main drawback is information disclosure breaches, where users exchange their data for financial or nonfinancial benefits. The disclosure objective focuses on users' readiness to disclose information before receiving rewards and their willingness to provide information based on rewards [4]. In Table below, we have listed the various privacy mechanisms provided by the social media site for users to configure and participate in privacy-related activities. Discrimination remains prevalent in the social media landscape when it comes to providing privacy policies to users.

A survey has revealed that a significant number of social media users do not priorities their privacy settings and leave their privacy details unchanged [7].

Table 2. Privacy issues in social media platforms and comparisons

Privacy option	Facebook	X	Insta-gram	LinkedIn
Limit visibility of users who are currently active.	Yes	No	Yes	Yes
Ban users based on their photo tags.	Yes	No	Yes	No
Configure alerts for login.	Yes	Yes	No	No
Prevent the inclusion of spam users.	Yes	Yes	No	Yes
Control who can send you messages.	Yes	No	No	Yes

In order to safeguard against previously mentioned attacks, users can follow the following steps:

a. Verify that the device is equipped with the most recent version of the antivirus software [2].
b. Avoid opening emails from unfamiliar senders [2].
c. Refrain from clicking on links, files, or document media that are unidentifiable or unfamiliar [2]
d. Avoid trying to browse unexpected websites [2].
e. A Regularly updating software patch is crucial.
f. Employ browser security protocols, such as employing a pop-up blocker and enforcing connection limits [2].
g. Enforce the standards for platform privacy security, which include accessibility of personal information, the ability to write on someone's wall, and visibility of someone's status, among other aspects [2].
h. Deploy intrusion detection systems and intrusion prevention systems to provide further protection against unauthorized access, malicious activities, and spamming [2].

3 Methodology

Social media developers on the server side decide the level of security for social media accounts by using information security technologies, and users regularly use extra external tools. The selected social media platforms for the study are Facebook, YouTube, and Instagram, which are now the most commonly used. As mentioned before, there are two categories of security tools: those developed by the developer of social media and those

developed by other online services. Complete account security may be achieved by integrating these technological methods:

a. Two-factor authentication is a security measure that improves the safety of user accounts by necessitating the use of both a password and an extra method of verification. Two-factor authentication is the practice of using two separate components to confirm the identification of a person or, in certain situations, a process [2].

b. Private account maintains confidentiality by keeping all posts hidden and only allowing them to be viewed by friends and approved followers [2].

c. The security feature called "login notification" alerts users about any unusual logins to their accounts [2].

d. A security audit tool that enables the examination of approved devices. Authentication with a verification code is unnecessary when accessing a trusted device [2].

e. The ability to choose three to five trustworthy acquaintances from a list of friends in order to obtain a virtual key for a social media account through the use of dependable connections [2].

f. A security device that produces an identifying code for the purpose of two-factor authentication [2].

g. A tool that checks the strength of your passwords lets you assess how secure they are Top of Form [2].

h. Password breaches can be identified using security methods that authenticate for password breaches [2].

i. Email breaches may be identified by the utilization of a security technology referred to as the email breaches checker [2].

j. Periodic password updates: a security measure that encourages social media users to routinely change their passwords according to established security rules [2].

An External auditing of app/website access is a security feature that allows you to restrict third-party developers and websites from accessing your account [3].
Experts evaluated social media security tools in a study. Five information security experts were hired. The security tools were rated 1-10. This determined the average estimation values for each security tool, the range (1-5) security levels are as:

a. Absolute security, which uses all social media and external service security features, is the highest level [3].

b. The Optimal security—the highest level of security featuring all social media and external service security measures and features [3].

c. Fundamental security: all social media security measures are implemented [3].

d. Implementing robust security measures and techniques provided by social media platforms [3].

e. Insufficient security—a critically a low level of security using social media security
f. tools and measures [3].

Table 3 presents the results of an expert evaluation of social media security tools.

The table illustrates that two-factor authentication is the most crucial tool in social media apps, whereas identification code creation is the least significant one [3].

Security features	Experts scores					The Mean value of estimates
	1	2	3	4	5	
A two-factor authentication system.	10	10	10	10	10	10
Confidential account	9	8	10	9	10	9.2
Login Alert	9	8	7	10	9	8.8
Security assessment	8	9	8	8	9	8.4
reliable connections	6	7	8	5	8	6.8
Unique a numeric code used for identifying purposes.	5	6	6	6	4	5.48
Password strength evaluator	8	10	7	9	9	8.6
Security breach checker for passwords	7	8	8	10	9	8.4
Email breach verifier	10	9	9	8	10	9.2
The Regular password updates	9	8	7	7	8	7.8
Verification of external application/site access	9	9	8	9	9	8.8

3.1 Improving Social Media Security with Real-Time Fear Appeals

Facebook, a very popular social networking website, and identified two main types of security issues: platform-related problems and user-related concerns. An investigation was conducted to examine how a user's vulnerability affects the interconnectedness of a social media network. Typically, frequent users of social networks tend to disregard the potential security vulnerabilities that might pose a substantial risk to both their own safety and the safety of their friends on the platform. Moreover, they neglect to implement essential precautions to mitigate the hazards for users. Educate people on the possible risks to the security of their personal information on social networking platforms. After conducting a thorough analysis, they found that most of the 45 social media platforms had satisfactory security measures, privacy legislation, and use guidelines. Users may get information about the risks connected with social networking sites by consulting publicly accessible privacy policies, security procedures, and recommendations. Several studies have examined the correlation between a user's active engagement on social networking sites and their perception of security concerns. The efficiency of the recommended preventive measures that people should adhere to; an individual's self- perception of their own efficacy; The protective motivation theory suggests that individuals who engage in social media may be deterred from engaging in harmful behaviors due to four specific requirements. The RealTime Fear Stack swiftly identifies potential hazards and promptly alerts the user to exercise prudence while participating in precarious activities, such as disclosing their address on Facebook, for example. Real-time fear monitoring systems has the capacity to be advantageous to social media users by inspiring them to actively mitigate the dangers while participating in perilous activities [5].

3.2 The integration of social media and Artificial Intelligence to bolster security

Social media services such as Twitter and Facebook extensively employ machine learning algorithms to forecast user location, evaluate sentiment, and offer suggestions. They have been used to manage emergency operations, identify influential individuals, and predict disease spread. However, social media platforms are vulnerable to Cyber-attacks, as malicious software can alter content and create fake profiles. To address these threats, a machine learning technique can be used to identify malware and fake news. To address security and privacy concerns, a machine learning technique can be trained using articles about specific events or individuals, which can be used to test new articles and determine if the individual is a happy or not. However, the constant influx of news articles makes it difficult to identify fake news. To address privacy concerns, a machine learning technique can be modified to extract sensitive information. Various methods safeguarding privacy in machine learning are in development, but further exploration is needed to adapt these strategies to social media networks. Organizations like the United Nations are focusing on "AI for good," aiming to harness the potential of AI to promote positive outcomes while addressing Cyber-attacks and privacy concerns. The influence of social media on the advancement of AI for positive purposes is also being explored [7].

4 Discussion

This study investigates the influence of social media on strengthening interpersonal relationships and the precautions implemented to safeguard it. Additionally, overcoming geographical obstacles, thereby promoting mutual comprehension and facilitating progress in diverse fields positively, in terms of social, health, and economic sectors. This review

analyses different platforms as illustrative instances. Moreover, it explains the use of social media on a large geographical scale and provides statistics on the usage of popular global social media platforms like Facebook, Insta-gram, X and YouTube. The future expansion of worldwide users will be ascertained through the examination of data spanning from 2017 to 2027. This discussion will focus on the vulnerabilities of social media platforms to cybercriminals, including various types of assaults such as theft of identities, spam attacks, software assaults, impersonation, hijacking, and malicious activities. Malicious intent and cyberbullying. The risks pertaining to each of these users when utilizing social media are clarified. Each of these attacks has a unique effect on the user, which varies in intensity. In order to reduce these risks, it is advisable to implement precautionary measures. This form of attack requires the user to follow multiple protocols and employ a range of tools, such as a two-factor authentication system, a secure account, login notifications, security evaluations, trustworthy connections, a distinct numerical code for identification, a password strength analyser, email breach verifier, a password breach checker, periodic password changes, and verification of external application or website access. Each of these measures has its own effect on protecting our social media account from any type of unauthorized access, and they have been tested to prove their efficacy. A two-factor authentication system is widely recognized as an essential tool for augmenting social media security. Concurrently, the incorporation of multiple features into social media platforms can augment the security of our platforms. The features encompass restricting the visibility of presently active users, prohibiting users based on their photo tags, setting up notifications for login, thwarting the inclusion of spam users, and managing the senders of messages. The incorporation of these characteristics into specific social media platform functions to protect and secure the platform. Nevertheless, it is important to acknowledge that certain platforms lack these features. This study examines two dependable techniques for protecting social media platforms. Improving the security of social media by implementing real-time fear appeals. Lee found out on Facebook that users often ignore possible security vulnerabilities and fail to take necessary precautions. Most social media platforms have sufficient security measures, privacy regulations, and usage guidelines. Users can obtain information regarding potential risks by consulting openly available privacy policies and security protocols. The study also examined the relationship between active engagement in social media and the perception of security issues. Real-time fear stacks can be employed to identify potential dangers and promptly alert users to exercise caution when engaging in perilous activities. The researcher proposes that the integration of social media and artificial intelligence can bolster security. Social media platforms such as a twitter (X), and a Facebook utilize machine learning algorithms to predict user location, assess sentiment, and provide recommendations. However, these platforms are vulnerable to cyberattacks. To mitigate these potential hazards, a machine learning algorithm can be utilized to detect and categorize malevolent software and falsified information. Training methodologies can be utilized to assess new subjects and obtain sensitive information. The United Nations and similar organizations prioritize the utilization of artificial intelligence (AI) for advantageous objectives, with the goal of harnessing its potential for favourable results and addressing challenges associated with cyber-attacks and privacy issues. After conducting thorough research on a social-media platform, and the accompanying risks, as well as methods to improve their security, it has been identified that there are two significant vulnerabilities that continue to exist among social media users. Exercising authority over user-generated content, such as archived web pages and backup files, may lead to unauthorized entry into data. While privacy controls are necessary, they are not enough on their own. Furthermore, the user's limited understanding regarding social media precaution tools. It’s worth mentioning that, attaining flawless control of data is impossible due to the fact that users must possess substantial knowledge and experience in order to modify controlled data.

5 Conclusion

An overview of social media, its usage, and a breakdown of users by a country are presented at the outset of this review article. The list of the most widely used social media sites, ranked by user population, has also been included in the article. The second section of the essay explains security risks that come with both technological and physical attacks on social media platforms. Additionally, the tools you need to protect your social network accounts have been overhauled. Consequently, risks and losses are reduced or avoided. In addition, protection tactics such as artificial intelligence and real-time appeals are utilized to support social media platforms' security protocols and lessen obstacles and difficulties related to their use. This article explores the main factors that are influencing the younger generation's use of social media. Therefore, social networking applications must be secured in order to protect user data and offer a secure surfing experience. A well-designed social networking platform should have two strong user authentication methods: multi-factor authentication and secure session management. Protecting personal information and preventing unauthorized access and eavesdropping require encrypting data while it is in transit and at rest. To protect user privacy, employ secure transmission technologies like HTTPS. To avoid breaches of data, user data must be securely preserved with encryption and access controls. Applications need to include extensive privacy settings so that users can choose who may access and share their personal information and content. Regular vulnerability assessments, security scans, and user education are necessary to maintain security. To handle security incidents effectively, make use of fast incident response plans and safe account recovery mechanisms. By implementing these security measures, regularly analyzing and updating logs, and providing a secure environment for user interaction, social networking applications can protect critical data.

References

1. Tannous, G., & Barbar, A. M.An expert system to detect privacy's vulnerability of social networks. 2016 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET).volume 140,7 (2016)..
2. Etuh, E., Bakpo, F. S., and Agozie, H. E. 'Social Media Network Attacks and Their Preventive Mechanisms: A Review', *Science Direct*, Volume 140,14 (2022).
3. Shevchuk, R. and Pastukh, Y. 'Improving the security of social media accounts', Journal Title in Italics, Volume (Issue), 5 (2019).
4. Thuraisingham, B. 'The Role of Artificial Intelligence and Cyber Security for Social Media', *Science Direc*t,vol issues ,3 (2020).
5. herd. Digital/blog/facebook-statistics-2022
6. Zhang, Z., and Gupta, B. B. 'Social Media Security and Trustworthiness: Overview and New Direction', *Science Direct*, volume 86 ,12 (2018).
7. Kumar, S. N., Saravanakumar, K., and Deepa, K. 'On Privacy and Security in Social Media – A Comprehensive Study', *Science Direct*, volume 78 , 6 (2016).
8. Li, L. and Qian, K. 'Using Real-Time Fear Appeals to Improve Social Media Security', Science Direct, *Science Direct* ,volume 125 , 4 (2016).
9. Pattnaik, N., Li, S., and Nurse, J. R. C. 'Perspectives of Non-Expert Users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter', *Science Direct*, volume 125 , 15 (2022).
10. Yue, H., He, S., & Liu, Z. Social Media Users Send Promotional Links to Strangers: Legitimate Promotion or Security Vulnerability? IEEE Access, volume 140 , 14 (2020).

11. Senthil Kumar, N., Saravanakumar, K., & Deepa, K ,On Privacy and Security in Social Media – A Comprehensive Study, *science direct* , *Science Direct*, volume 78 , 6 (2016).
12. Gordhan Jethava a, Udai Pratap Rao b ,Exploring security and trust mechanisms in online social networks: An extensive review, volume 140 ,13 (2023).
13. David Tayouri,,The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages, Science Direct, Volume 3, 5 (2015)
14. Lionel Khalil a, Nancy Abi Karam b ,Security Management: Real versus Perceived Risk of Commercial Exploitation of Social Media Personal Data, *Science Direct* ,Volume 65,10 (2015) , .