Social Media Security and Attacks

Sarah Almalki[1], Reham Alghamdi[1], Gofran Sami[2] and Wajdi Alhakami[1]

[1]College of Computers and Information Technology, Taif, Saudi Arabia
[2] Joint First Year Deanship, Umm Al-Qura University, Makkah, Saudi Arabia

Abract
The advent of social media has revolutionized the speed of communication between millions of people around the world in various cultures and disciplines. Social media is the best platform for exchanging opinions and ideas, interacting with other users of similar interests and sharing different types of media and files. With the phenomenal increase in the use of social media platforms, the need to pay attention to protection and security from attacks and misuse has also increased. The present study conducts a comprehensive survey of the latest and most important research studies published from 2018-20 on security and privacy on social media and types of threats and attacks that affect the users. We have also reviewed the recent challenges that affect security features in social media. Furthermore, this research pursuit also presents effective and feasible solutions that address these threats and attacks and cites recommendations to increase security and privacy for the users of social media.

Key words: *Social media security; Social media attacks; Privacy. Social media threats*

1. Introduction

Social media is a huge part of the internet today. Social media has made a qualitative leap not only in communication between individuals and groups, but has also emerged as the vehicle for several social, political, and cultural changes across the world. Social media offers an all-inclusive forum through which individuals, groups and communities can voice their thoughts. Undoubtedly, the accessibility, outreach and the speed with which the delivery of information takes place through social media platforms, has made them inseparable from the present-day lifestyles [1][5]. Yet another fascinating aspect of using social media is the flexibility to share photos, videos, applications, and more [1] [4]. Over 3 billion users use social media and it is expected that it will continue to grow in terms of the number of users, volume of data, sharing, and downloading [6]. Multiple social media can remove geographic and economic boundaries between its users for communication and information sharing [1]. Figure 1 shows the global digital population who use social media. Social media is also use- ful for achieving many goals such as education, investment, entertainment, job searching, remote work, and more [4]. However, such ubiquitous use also calls for providing security and protection for the social media users and their data. It is only by maintaining their privacy, that the users will be able to enjoy the benefits of social media [2] [3].

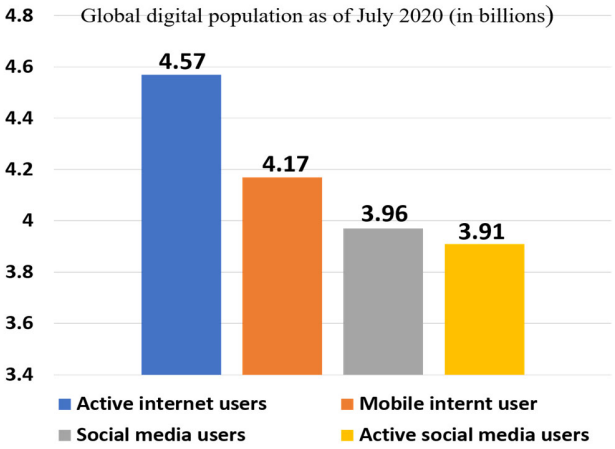

Fig. 1. Global digital population as of July 2020 (in billions)[6].

The security and privacy of social media is a subject for ex- tensive research in the present context. Security researchers are constantly providing better solutions to avoid attacks such as identity theft, social phishing, impersonation, malware attacks, and image retrieval on social media. Plug-in attacks are yet another new threat that has been detected. Such attacks affect the users' privacy such as cross-site scripting, clickjacking and malicious applications [4][5]. The widespread use of social networks (Facebook, Twitter, WhatsApp, YouTube and others), and the desire of many segments of society to connect through them, necessitates a consistent monitoring of the security risks that threaten these networks [3]. It has become imperative to mitigate cyber-crimes and other illegal activities that take advantage of users' data and violate their privacy on social media [3] [4]. According to the global platform, Statista.com, Figure 2 shows the number of users is variable and growing for each social media platform. Facebook is the first social media to exceed billion registered users and there are now over 2.6 billion monthly active users [6].

This paper has been organized into 7 sections: Section 2 discusses about the security requirements in social media and the challenges in ensuring optimum privacy for the users and the attacks that threaten security while using social media. Section 3 highlights the recent studies that are associated with privacy and security and attacks and threats on social media. Section 4 details the

Manuscript received January 5, 2021
Manuscript revised January 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.1.22

proposed solutions to improve security and protection for the users. Section 5 discusses the methodologies to achieve privacy and security requirements i n social media,

and in Section 6, we have presented many recommendations to improve privacy and security during the use of social media. Section 7 concludes this paper.

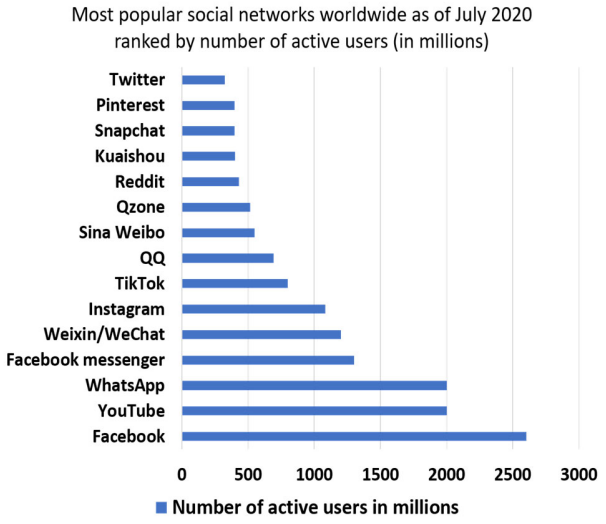

Fig. 2. Most popular social media worldwide as of July 2020, ranked by number of active users (in millions)[6].

2. Background

This section discusses the security requirements for social media: Confidentiality, Integrity, and Availability, the CIA triad. The present section also reviews the challenges that threaten the users' security when using social media.

2.1 Security Requirements in Social Media

Integrity, Confidentiality, and Availability are three elemen- tal security requisites while using social media. As shown in figure 3, the CIA Triad has been developed to ensure data secu- rity and protection. It is an approved and developed model that monitors/ regulates security policies for data and the system used in troubleshooting problems and provides solutions to security problems in information security. It consists of three basic elements that are considered to be the most important security objectives in any system: Confidentiality, Integrity, and Availability [14][15].

1) Confidentiality: is a set of rules that are concerned with preserving the privacy of sensitive and important information and prevent access to it. Encryption can preserve users' data during storage or transmission and prevent unauthorized people from accessing it [8].

2) Integrity: is ensuring that information is reliable and accurate. It includes taking all proactive measures to restrict unauthorized changes to information, and the ability to recover the lost information [14][22].

3) Availability: is ensuring that the authorised users are allowed to access the information systems, networks, and data freely to perform their daily tasks, which is the consistency of data networks and systems. Regular maintenance of programs and devices is especially important to ensure authorized access [14][22].

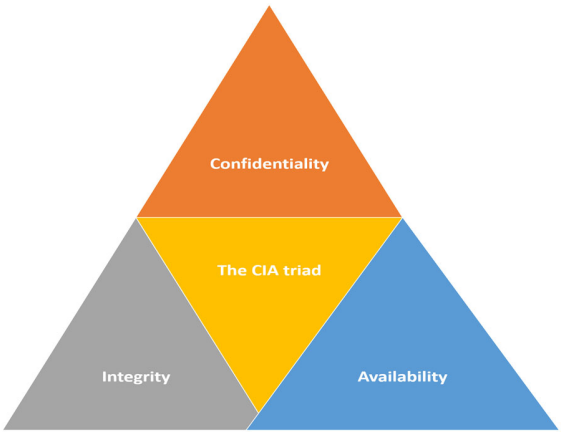

Fig. 3. Confidentiality, Integrity, and Availability (CIA triad).

Considering the burgeoning use of social media sites among different groups and ages from different fields and the huge amount of data that is shared daily, there is a need to provide protection and security for users of social media to maintain their privacy from attacks, theft, and loss [11]. Some of the basic requirements for security and privacy in Social media are:

- **Security in Communication:** During direct conversa tions and chats on social media, the sender/s and the recipient/s must be authenticated, and the connection itself must provide confidentiality and integrity [9].

- **Registration and Login:** The registration step and logging into the user's account on social media are important for granting access to the network to the user for authentication. After the registration process on social media, the user receives a personal ID file that contains login information and personal account data, which should be stored confidentially [9].

- **Access Control:** Must define access privileges in groups on social media to distinguish between one user and another. Granting control and access power is very important in groups with thousands of users to determine the ability to see shared items, various personal files, or other users 'data. Therefore, the aim of defining access control is to ensure integrity, confidentiality, and availability of common elements such as media files, links, etc. [10].

2.2 Security Challenges and Attacks in Social Media

The percentage of social media users has increased by a large margin over the past few years. The use of social media reached 49 percent in January 2020. This is a significant percentage compared to the last three years. The number of social media users is expected to reach 4.41 billion users in 2025 [12]. Table 1 shows the number of social media users worldwide from 2018 to 2025.

Table 1. Number of Social Media Users Worldwide from 2018 to 2025(IN BILLIONS)

Year	Number of Users (in billions)
2018	3.14
2019	3.4
2020	3.6
2021	3.78
2022	3.96
2023	4.12
2024	4.27
2025	4.41

With the increase in the number of users, as we mentioned previously, there has been an increase in attacks and threats to the security and protection of users' accounts and their data on social media. Moreover, security challenges have affected the key security objectives such as confidentiality, integrity, and privacy of users' accounts and their data on social media [13]. Security challenges appear on social media because of the desire to share with others a lot of personal and sensitive data that appears in the users' personal accounts. The fascination to share one's preferences/interests with the like-minded people across the world through social media unfortunately allows the attackers to access personal information of the users and exploit it in attacks [11]. The biggest challenge to security in social networking sites is how to ensure the safety and protection of users' accounts and their data.

1) Privacy Risks: Although many social media platforms have the mechanisms to modify privacy settings to protect user's accounts, these settings may not be sufficient on their own to protect the users' data [21]. The problem with pre- serving privacy is that social media networks do not warn the users of the dangers of publishing their personal and sensitive information. Thus, the users often do not realize the hazards of publishing their highly sensitive data [11].

2) Integrity and Confidentiality Risks: The attackers use social engineering and create fake accounts to communicate with the users of social media. Attackers use these accounts to send fake messages to alert the users about resetting their passwords to gain access to the users' sensitive information [22]. This affects the integrity and confidentiality of social media and makes the user vulnerable to security attacks. Some social media posts contain links and codes or malware that are intentionally uploaded by the attackers to prey upon the users' personal information and harm them.Threats on social media can be classified into four major categories: Classic threats, Modern Threats, Combination Threats and Threats Targeting Children. Figure 4 shows the most common threats in social media.

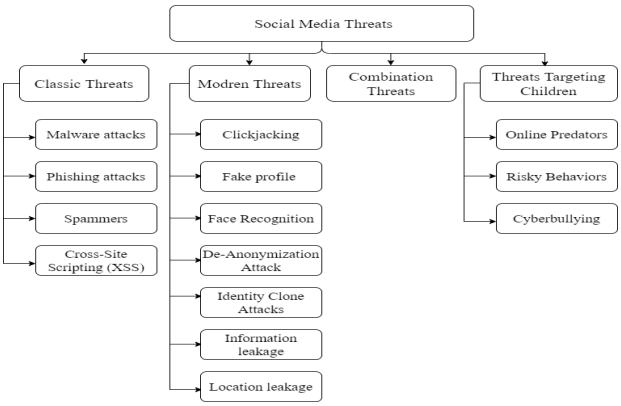

Fig. 4. Threats in social media.

- **Classic Threats:** are among the most widespread threats. They have proliferated even more with the increased use of the Internet along with social media. Classic threats threaten the security of users due to the structure and method of communication on social media [23]. Although the classic threats have been addressed in the past, they are still persistent and can be categorized as malware, cross-site scripting (XSS), spam, phishing attacks, and others. These threats affect the users' accounts and data on social media and harm the content of the users and their friends [17][24].

Table 2 shows types of classic attacks in social media.

Table 2. Summary of Classic Attacks in Social Media

Attack	Description
Malware Attacks	It is common among social networking sites where the attacker sends injected malware scripts to the user and upon clicking the malicious URL, a malicious program is installed, or it may lead to a fake website targeted to steal the user's information.
Phishing Attacks	An attack wherein the aim is to obtain sensitive information from a user through some fake website or by impersonating as a person the user knows.
Spammers	In this type, attackers send unwanted messages such as ads to different users by creating fake accounts and they can also add comments to pages that many see on social media accounts.
Cross-Site Scripting	An attack that an attacker exploits the web client's trust in web applications and causes the web client to run code that leads to the gathering of personal and sensitive information that would harm users' access. Because of the structure of social media, this loophole can be exploited to create an XSS worm that can spread among social media users and cause harm.
Internet Fraud	It is the use of the Internet to deceive people and defraud them, such as accessing another user's account and logging in from it and requiring people to transfer money to a specific bank account.

- **Modern Threats:** These are specific types of threats associated with social media platforms. The intent of these threats is to gain access to sensitive and personal information of the users and their friends who follow and communicate with them. For example, attackers target the

users with certain privacy settings to re- veal and compromise their personal information. The most modern threats are: Clickjacking, Fake profiles, DeAnonymization, Face Recognition, Identity Clone Attacks [17]. Table 3 shows different types of modern attacks in social media.

- **Combination Threats:** This type of threats combines the modern and classic threats together, as today's attackers can create a more complex attack; a mixture of attacks types [23].

- **Threats Targeting Children:** children and adolescents face classic and modern threats, but there are threats that specifically target the children and adolescents with malefic intent. [25]. Few examples of threats of this type are: Online Predators, Risky Behaviors and Cyberbullying attacks. Table 4 shows types of threats targeting children in social media.

Table 4 Summary of Threats Targeting Children in Social Media

Attack	Description
Online Predators	The purpose of the attacker in this type of attack is to harm the personal and sensitive information of children on social media. It has three sections: the content to expose the children to inappropriate content or to communicate with the children with the aim of harming them.
Risky Behaviors	It consists of the child's behaviour while using the Internet and social networking sites. When the child communicates with strangers and this may threaten the safety of the child's behaviour and affect him/her, such as sexual conversations, the exchange of pictures and other sensitive information. The transmission of such content can harm the safety of the child.
Cyberbullying	In this type, the attackers target the victims and abuse or blackmail them by posting pictures and threats, and the users most affected by it are children.

3. Related Work

Several research studies discuss the security and privacy in social media. However, we have focused on the most important and recent research studies published from 2018-2020 only for our reference and analysis. Furthermore, we have also included the research studies that specifically dwell on attacks on social media.

3.1 Security and Privacy in Social Media

The authors in [8], focused on explaining the importance of improving anonymity techniques to protect the privacy of users and their data. The authors proposed a new adversarial attack by focusing on users' privacy and preserving their data on social media. They presented a method for assessing different aspects of the effectiveness of anonymity on social media. They explained the new privacy risks of the different data that users share and protect them on social media. A new technology, Athd, was proposed and the results showed that anonymity of social media users was not sufficient to protect the users' privacy.

In [5], published in 2018, the authors conducted a comprehensive survey of the latest security and reliability features in social media, particularly regarding the increasing complexity of the attacks. The authors presented a new research direction, which was to assess and measure the reliability and security of social media platforms by determining the platform's availability and ensuring its quality as evidence-driven research. The study focused on how to assess, measure, and improve trustworthiness and security to achieve the goal of building reliable social media and maintaining security. The paper concluded by reviewing the growing challenges in social media.

The authors in [16] introduced the common security and privacy issues on social media. Their approach was based on educating social media users on how to protect their data from attacks when using social media. Hence, the proposed work gave several recommendations for social media users on how to avoid and solve these security issues.

The authors in [17] presented the history of social media, its importance and development in recent years. They explained the threats and attacks that occur while using social media and suggested the use of "Web0.2" technology, which maintains data security and overcomes threats. The mechanism was aimed at mitigating risks to protect the security and confidentiality of social media users' data at the institutional and individual levels.

In [18], the authors highlighted the issues related to cyber- attacks on social media. They reviewed cyber threats in social media and ways to thwart these threats and prevent attackers from accessing and damaging the users' data. Finally, they introduced many effective measures of cybersecurity.

In [19], the authors focused on improving the security of accounts in social media such as Facebook, YouTube, and Instagram. First, the security tools for Facebook, YouTube, and Instagram accounts were identified and compared. The study demonstrated that social media security tools were not adequate in protecting the users' account security and data. Then a mathematical model was constructed to form a social media security level indicator. In this model, the authors used direct estimation to estimate the security tools of social media accounts and determine their average value. Five levels of security were proposed for estimating the level of security on social media. The mathematical model presented in the paper developed a Chatbot. It is a developer program for chatting that estimates the level of security of a user's account in social media and provides recommendations for improvement in the level of security of the user's account in social media.

The authors in [20] proposed an alternative method for the public to assess the security and reliability of social media based on the signal theory being used in information management. First, the authors ranked critical security and trust signals for social media platforms, formal static traits, and dynamic behavior features by using OWL and temporal logic. After that, the authors proposed a mathematical model to measure the level of security and reliability inspired by crowd computing, based on Fuzzy Analytic Hierarchy Process Comprehensive Evaluation. Finally, they

conducted evaluations by using the collective assessment structure on a multimedia social platform called CyVOD MSN. The results yielded assessments of both security and trust signals for social media platforms and focused on raising development awareness for CyVOD MSN by developing insecure and untrustworthy vulnerabilities.

The authors in [21] explained privacy issues in social networks. The authors classified privacy in social networks into three categories: site privacy, user privacy, connection privacy, and threats categorized for each category. A detailed break-down of the privacy preservation solutions was also proposed under each privacy criterion. The study also presented appraisal of several data sets and data creation tools which the future researchers could use. Then they produce a detailed summary of the various solutions proposed by other researchers to resolve privacy issues**.**

3.2 Security Threats and Attacks in Social Media

This section presents a summary of the latest research on attacks and threats on social media.

3.2.1 Classic threats: In [28], the authors presented a new approach to spam detection for Twitter spammers whose approach focuses on the use of deep learning (DL) techniques. The performance of the proposed approach was compared to five ML-based approaches by using Twitter user metadata and the text of Tweets. The study demonstrated the effectiveness of the proposed approach.

In study [29], the authors reviewed and surveyed eight survey papers related to phishing attacks on social media platforms, where they analyzed mechanisms for detecting and preventing different phishing methods associated with social media.

The authors in [30] discussed spam attacks and proposed a methodology for detecting different types of spam attacks drawing on a graph and studying them on some attack scenarios and comparing them. This method was based on the values of honesty, trust and reliability, respectively. The study showed the effectiveness of the proposed method as it was able to detect and block the sender of spam. Furthermore, the authors compared the quality of the results with other methods by reviewing some case studies.

3.2.2 Modern Threats: The authors in [26] discussed about the importance of learning to protect personal information from attacks on social media. They proposed an effective method for detecting fake profiles on social media to reduce damages. The method depends on the similarity of the profile characteristics and the network characteristics. The stated method was compared with the victim's profile based on network relationships. Although the method was effective in detecting false identities, the authors highlighted the need to learn how to protect files and personal information on social media.

In [27], the authors were interested in launching hostile attacks to uncover fake Twitter accounts. Twitter is a platform that contains many fake accounts. With the aim of harming other users or creating false news or opinions to influence a topic that is circulating among users, the authors launched attacks against a detection engine that used machine learning to expose fake Twitter accounts. The results demonstrated the effectiveness of the proposed measures. The study proposed the use of k-NN as a measure to address the effects of hostile attacks carried out by the authors.

In [33], the authors suggested an automatic method for identifying the cloned profiles on social media and implemented it on the Hadoop framework by using MapReduce programming paradigm. The method consisted of three steps. In the first step, the number of followers per user was counted and stored as a profile tagging attribute. Then in the second step, the network users were classified based on the number of followers and the characteristics of the profiles. After that, all the personal files were transferred within the same group for verification and then in the third step, the highest rated profile was selected. The methodology for arranging these profiles was based on the result of the PageRank algorithm. The authors collected a bunch of data from Instagram. The results showed the effectiveness of the method and in some attacks, all the cloned profiles were identified with 100 percent accuracy.

3.2.3 Threats Targeting Children*:* In [32], the authors presented the CONcISE proposal, a method for identifying the bullying of Instagram posts.They based their proposed approach on categorizing comments in a session and raising a session level alert when the threshold exceeded. This work proved accurate when tested on a real dataset on Instagram with 4 million users and 10 million comments.

In [34], the authors present a methodology for detecting cyberbullying in addition to the element of sarcasm that was not addressed in previous studies. This methodology was based on the application of machine learning algorithms. The results showed that the performance of SVM and Ensemble was higher than others with an average accuracy of 79 percent Whereas, the SVM classifier proved to be the best. Table 5 enlists the suggested security techniques to detect attacks on social media.

4. Solution of Threats and Attacks on Social Media

Social media operators, security companies, and academic researchers have proposed a suite of solutions to address cur- rent attacks and threats. These solutions contribute to providing security and privacy for users' accounts and their data. Figure 5 shows security solution types.

4.1 Social Media Operators Solutions

It is a set of solutions, settings, and security and privacy measures that social media players provide to users of their services, such as using user authentication mechanisms and applying user privacy settings [36].

- **Authentication Mechanisms:** These mechanisms are used in social media when registering or logging in to verify the identity of the user and establish the user's authenticity. This is done by sending a verification code when logging into the user's Twitter account [35].

- **Security and Privacy Settings:** All social media networks provide many privacy settings to enable the users to protect their data [35]. For example, the privacy settings in Instagram ensure that the private file can only be viewed by one's friends, and the privacy settings in Snapchat determine who can see the pictures and videos that are posted. Even in Facebook, through the privacy settings, the users can choose which friends can view their profile details.

Table 5. Suggested Security Techniques to Detect Attacks on Social Media

Ref	Year	Category	Attack	Security Technique
[28]	2020	Classic	Spam	A new approach to spam detection for Twitter spammers. The approach focuses on the use of deep learning (DL) techniques.
[29]	2020	Classic	Phishing	Analyse mechanisms for detecting and preventing different phishing methods associated with social media.
[30]	2020	Classic	Spam	Propose a methodology for detecting different types of spam by a graph and studying them on some attack scenarios and comparing them. This method is based on the values of honesty, trust and reliability.
[26]	2019	Modern	Fake profile	An effective method for detecting fake profiles on social media. The method depends on the similarity of the profile characteristics and the network's characteristics.
[27]	2020	Modern	Fake profile	The authors launched attacks against a detection engine that uses machine learning to expose fake Twitter accounts.
[33]	2020	Modern	Identity Clone	An automatic method for identifying the cloned profiles on social media and implemented the Hadoop framework by using MapReduce programming paradigm.
[32]	2019	Threats Targeting Children	Cyberbullying	The CONcISE proposal, a method for identifying the bullying of Instagram posts. This approach was based on categorizing comments in a session and raising a session-level alert when the threshold exceeded.
[34]	2020	Threats Targeting Children	Cyberbullying	A methodology for detecting cyberbullying was proposed in addition to the element of sarcasm that was not addressed in previous studies. This methodology was based on the application of machine learning algorithms.

- **Internal Protection Mechanisms:** They are protection mechanisms provided by social media networks to their users to protect their data from attacks and threats [35].

- **Report Users:** Social media provides options for reporting abuse upon exposure to any security issue. Social media operators deal with it to protect its users [35].

4.2 Security Companies' Solutions

This type of solution is provided by a number of commercial companies to provide safety and privacy for users on the Internet, and now these companies offer a number of software solutions for users of social media to protect their personal accounts and sensitive information, such as AVG PrivacyFix and McAfee Social Protection [36].

4.3 Academic Researchers' Solutions

This type of solutions is presented by practical studies that aim to improve the safety and privacy of social media users and protect them from attacks and loopholes that are increasingly emerging due to the rapid development of the Internet and the spread of social media. The solutions include improving Privacy Setting Interfaces and Phishing Detection [36].

In [23], the authors provide a comprehensive explanation of the threats and attacks on social media that affect the protection and security of users' accounts and their data. They classified threats that affect the users' security on social media into three categories: account-based threats, URL-based threats, and content-based threats. They reviewed the most prominent methods and solutions for protecting and securing users and explaining their main advantages and disadvantages.

In paper [31], the authors proposed a new framework based on perceptual hashing and semantic privacy rules for calculating the privacy level of images. There are two methods of segmentation of perception to preserve privacy: the first method focuses on SIFT features that are concerned with describing sensitive objects in images, and the second focuses on the LBP features that are interested in describing faces in pictures. The level of privacy can be presented as a measure of the sensitivity of a user's digital photos before they share the photos on social media.

In [37], the authors proposed a new methodology called DeepScan to protect malicious computation by performing location-based content analysis by using long-term memory on the neural network platform to perform

time series analysis. The authors used a machine-learning algorithm to detect mali- cious accounts. The results indicated that DeepScan achieved a prediction performance with an F1 score of 0.964. The authors also found that time series was highly accurate in the detection system.

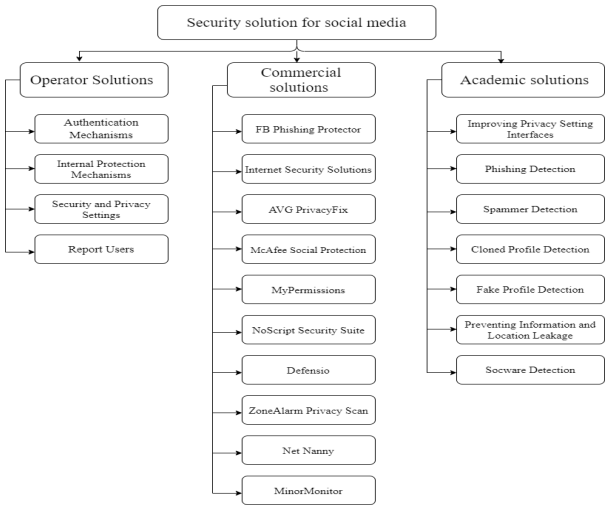

Fig. 5. Security solution for social media.

5. Discussion

The present study discusses about security and privacy in social media and the attacks and threats that affect sensitive information on social media. Our study also perused many recent studies in this field, some of which were presented in this paper. The ensuing paragraphs in this section deliberate upon the most important methodologies and results suggested by the researchers to achieve security and privacy in social media and provide many solutions to address attacks and threats.

The key concern in providing security and privacy on social media arises due to the intrinsic heterogeneity of user-generated information which requires adjustment between sharing users' information and securing users' privacy. Researchers have suggested many methods and techniques to achieve security and privacy of social media users. One of the techniques, as presented in [8], is Athd- a novel antagonistic procedure by misusing heterogeneous characteristics of social media information. Despite the results that proved the efficiency of this methodology, we still need to consider privacy to protect the user from hackers. Moreover, anonymity alone is not sufficient to protect the user's identity and privacy. The researchers in [5] worked on creating a reliable and safe environment that protects social media. They suggested a method to evaluate and measure the reliability and security of social media platforms. However, this method has many disadvantages, including the inability to solve the problem of exploiting the user's information by others and the user's inability to control it, thus increasing risks and reducing user's trust. Hence, there is still an urgent need to improve defensive and offensive solutions. There is also a need to research on prevention tools to ensure user privacy and increase trust. In [21], the researchers classified privacy on social media into three categories and also classified the threats for each category to improve privacy and safety tools for the users of social media. It is a very effective and easy classification to divide attacks and threats in a modern and elaborate way. This classification divides privacy based on the diversity of attacks and threats and their sources.

Researchers have presented several methodologies to detect attacks on social media, and studies have demonstrated the effectiveness of proposed methodologies to meet the security requirements of social media, for example in [28], a new approach to detect spam on Twitter was suggested by using Deep Learning (DL). The study demonstrated the efficiency of the results obtained through the proposed methodology on Twitter. However, in [30], a different methodology was proposed to detect different types of spam attacks. Thismethod was based on the values of honesty, trust, and reliability. The research used and studied diagrams for some attack scenarios and compared them. The study achieved high effectiveness in detecting and blocking SPAM sender. This study is considered to be the best because it focused on several types and proved its effectiveness with higher accuracy.

To achieve integrity and avoid fake profile attacks, the researchers, in [26], proposed an effective method for detecting fake profiles on social media. The method relied on the similarity of the profile characteristics and network's characteristics, comparing them with the victim's profile based on network relationships. Although the method has proven effective in detecting fake identities, there is a strong need to know how to protect files and personal information on social media and this is one of the drawbacks. On the other hand, the authors in [27] used a completely different technology from the previous one. The researchers launched attacks against a detection engine that used machine learning to detect fake Twitter accounts. The results illustrated the effectiveness of the proposed measure, and the use of k-NN was proposed to counter the hostile attacks that were carried out by the authors. This method was effective, but one of its drawbacks was that it relied on launching an attack and then using k-NN to treat its effects. The main purpose of the study was to verify the effectiveness of the attack by only revealing fake Twitter files. The proposed mechanism, however, cannot be applied on the other social media.

Recently, cyberbullying has become one of the most common attacks on social media. Hence, many researchers have suggested ways to discover it. [32] One of these is CONcISE, which is a method for identifying bullying in Instagram posts. The authors based their suggested approach on categorizing comments in the session and raising a session-level alert when the threshold was crossed. This methodology has proven its accuracy with a large number of real users on Instagram only, but the method for

detecting bullying differs between social media platforms. It depends on several other factors. Thus, the previous study is not applicable on other social media sites. The authors in [34] suggest a methodology for detecting the element of cynicism in cyberbullying that has not been addressed in previous studies. This methodology is based on application of machine learning algorithms and the results are SVM and Ensemble accuracy with an average accuracy of 79 percent. The SVM classifier proved to be the best.

To achieve security and privacy for social media users, researchers have provided many solutions to counter attacks on social media. Furthermore, in the wake of increasing number of attacks and the number of users, more solutions are being researched. In [23], the authors provide a new classification of threats that affects the users' security on social media. The three categories are: account-based threats, URL-based threats, and content-based threats. It is a very effective classification as solutions have been classified on the basis of dividing threats to meet the security and preventive requirements of social media, and there are also solutions proposed to achieve privacy for the photos that users share on social media. Since the social media is based on sensory segmentation and semantic privacy rules, the authors in [31] proposed a new framework to calculate the level of privacy of the images. The authors in [37] focused on the use of a machine learning algorithm to detect harmful accounts and introduced a new methodology called the DeepScan. The results indicated that DeepScan was effective in detecting malicious accounts.

6. Measures for Protecting User's Account and Information on Social Media

We have enumerated certain measures that would help the users to achieve greater security and privacy while interacting on social media. The specific measures that the users can adhere to are:

- Establish strong passwords to protect your login to social media [40][41]. Table 6 shows the most popular passwords from 2018 to 2020.
- Change the passwords periodically [40].
- Focus more on activating two-factor authentication to increase the security of your account on social networking sites [38]..
- Beware of using the same password for all your social media accounts, because when one of your accounts is hacked, this can cause the rest of the accounts to be hacked [41].
- Make sure to use anti-virus programs to avoid losing or stealing your important information and files due to a virus from social networking sites [41].
- Secure and protect mobile devices through which you can access your personal accounts in social media and lock them with strong passwords to ensure their protection when lost or stolen [38].
- Use computers in public places with caution and log out of your personal accounts on social media when using them on public computers [38].
- When adjusting the privacy settings in the personal account on social media, you must turn off location sharing [39].
- Do not click and enter links sent from strangers because they may contain malware [39].
- Be sure to customize the security and protection settings in social media to your liking, and not rely solely on the default settings [40][41].
- Do not publish your private information and do not make friends with strangers by sharing your private and sensitive data with them because that may lead to hacking [41].

Table 6. The Most Popular Passwords from 2018 to 2020

2018	2019	2020
123456*	123456*	123456
qwerty	password	123456789
password	111111	qwerty
iloveyou	sunshine	password
111111	qwerty	1234567
123123	iloveyou	12345678
abc123	princess	12345
qwerty123	admin	iloveyou

7. Conclusion

People all over the world use social media. Social media platforms are for sharing opinions, ideas, interests, notes, and all kinds of files. With the increasing development of social media and the increase in the number of users, it has become necessary to focus on security and privacy of the users. In this paper, we conducted a comprehensive survey of the latest and significant research studies done in this league from 2018 to 2020. This study also discussed the security requirements and how to achieve them in social media and reviewed the challenges in achieving the desired levels of security and privacy for the users' data. Furthermore, the study enlisted the types of threats and attacks on social media and proposed workable solutions to confront these threats. Thus, the present study will be helpful for the readers in gaining a deeper understanding of the key aspects that determine security and ensure privacy while using the social media. In future work, we will continue to search for more modern curriculum papers that essentially focus on raising the level of privacy and security in social media for various users, whether individuals or institutions.

References

[1] Shevchuk, R., Pastukh, Y. (2019, June). Improve the Security of Social Media Accounts. In 2019 9th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 439-442). IEEE.

[2] Such, J. M., Criado, N. (2018). Multiparty privacy in social media. Communications of the ACM, 61(8), 74-81.

[3] Du, S., Li, X., Zhong, J., Zhou, L., Xue, M., Zhu, H., Sun, L. (2018). Modeling privacy leakage risks in large-scale social networks. IEEE Access, 6, 17653-17665.

[4] Sahoo, S. R., Gupta, B. B. (2019). Classification of various attacks and their defence mechanism in online social networks: a survey. Enterprise Information Systems, 13(6), 832-864.

[5] Zhang, Z., Gupta, B. B. (2018). Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems, 86, 914-925.

[6] Clement, J. Number of social media users worldwide 2010-2021 — Statista. [online] Statista. Available at: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (accessed date 2020).

[7] Beigi, G., Liu, H. (2018). Privacy in social media: Identification, mitigation and applications. arXiv preprint arXiv:1808.02191.

[8] Beigi, G., Shu, K., Zhang, Y., Liu, H. (2018). Securing social media user data: An adversarial approach. In Proceedings of the 29th on Hypertext and Social Media (pp. 165-173).

[9] Sharma, V.D., Yadav, S. K., Yadav, S. K., Singh, K. N. (2019, December). Social Media Ecosystem: Review on Social Media Profile's Security and Introduce a New Approach. In International Conference on Advances in Computational Intelligence and Informatics (pp. 229-235). Springer, Singapore.

[10] Zuo, X., Li, L., Peng, H., Luo, S., Yang, Y. (2020). Privacy- Preserving Subgraph Matching Scheme with Authentication in So- cial Networks. IEEE Transactions on Cloud Computing, 1–1. https://doi.org/10.1109/tcc.2020.3012999

[11] Srivastava, S. R., Dube, S., Shrivastaya, G., Sharma, K. (2019). Smartphone triggered security challenges–Issues, case studies and prevention. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies, 187-206.

[12] Clement, J. Number of social mediausers world wide 2010-2021Statista. Retrieved: from-Statista websitehttps://www.statista.com/statistics/278414/nuber-of-worldwide-social/network-users/ (accessed date 2020, July 15).

[13] Sharma, S., Jain, A. (2020). Role of sentiment analysis in social media security and analytics. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, e1366.

[14] Eian, I. C., Lim, K. Y., Yeap, M. X. L., Yeo, H. Q., Fatima, Z. (2020). Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges.

[15] Chandini, M. S. (2020). An Overview about a Milestone in Informa- tion Security: STEGANOGRAPHY. International Journal of Progressive Research in Science and Engineering, 1(2), 33-35.

[16] Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., Rodrigues, J. J. (2018). Privacy and security issues in online social networks. Future Internet, 10(12), 114.

[17] Almarabeh, H., Sulieman, A. (2019). The impact of cyber threats on social networking sites. International Journal of Advanced Research in Computer Science, 10(2), 1.

[18] Thakur, K., Hayajneh, T., Tseng, J. (2019). Cyber security in social media: challenges and the way forward. IT Professional, 21(2), 41-49.

[19] Shevchuk, R., Pastukh, Y. (2019, June). Improve the Security of Social Media Accounts. In 2019 9th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 439-442). IEEE.

[20] Zhang, Z., Wen, J., Wang, X., Zhao, C. (2018). A novel crowd evaluation method for security and trustworthiness of online social networks platforms based on signaling theory. Journal of computational science, 26, 468-477.

[21] Sai, A. M. V. V., Li, Y. (2020). A Survey on Privacy Issues in Mobile Social Networks. IEEE Access, 8, 130906-130921.

[22] Edwards, N., Kiser, S. B., Haynes, J. B. (2020). Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability. Journal of Strategic Innovation Sustainability, 15(4), 10–14.

[23] Yassein, M. B., Aljawarneh, S., Wahsheh, Y. A. (2019, April). Survey of Online Social Networks Threats and Solutions. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 375-380). IEEE.

[24] P. Velayudhan, S., Somasundaram, M. S. B. (2019). Compromised account detection in online social networks: A survey. Concurrency and Computation: Practice and Experience, 31(20). https://doi.org/10.1002/cpe.5346.

[25] Alguliyev, R., Aliguliyev, R., Yusifov, F. (2018). Role of Social Networks in E-government: Risks and Security Threats. Online Journal of Communication and Media Technologies, 8(4), 363-376.

[26] P, S., Chatterjee, M. (2019). Detection of Fake and Cloned Profiles in Online Social Networks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3349673

[27] Kantartopoulos, P., Pitropakis, N., Mylonas, A., Kylilis, N. (2020). Exploring Adversarial Attacks and Defences for Fake Twitter Account Detection. Technologies, 8(4), 64.

[28]] Alom, Z., Carminati, B. and Ferrari, E. (2020). A deep learning model for Twitter spam detection. Online Social Networks and Media, 18, p.100079.

[29] Ali, M. M., Qaseem, M. S., Rahman, M. A. U. (2020). A Survey on Deceptive Phishing Attacks in Social Networking Environments. In Proceedings of the Third International Conference on Computational Intelligence and Informatics (pp. 443-452). Springer, Singapore.

[30] Bidgolya, A. J., Rahmaniana, Z. (2020). A Robust Opinion Spam Detection Method Against Malicious Attackers in Social Media. arXiv preprint arXiv:2008.08650.

[31] Hu, D., Chen, F., Wu, X., Zhao, Z. (2016, June). A framework of privacy decision recommendation for image sharing in online social networks. In 2016 IEEE First International Conference on Data Science in Cyberspace (DSC) (pp. 243-251). IEEE.

[32] Yao, M., Chelmis, C., Zois, D. S. (2019, May). Cyberbullying ends here: Towards robust detection of cyberbullying in social media. In The World Wide Web Conference (pp. 3427-3433).

[33] Zare, M., Khasteh, S. H., Ghafouri, S. (2020). Automatic ICA detection in online social networks with PageRank. Peer-to-Peer Networking and Applications, 1-15.

[34] Ali, A., Syed, A. M. (2020). Cyberbullying Detection using Machine Learning. Pakistan Journal of Engineering and Technology, 3(2), 45-50.

[35] P, S. (2018). A comparative study of threats and solutions in online so- cial networks. International Journal of Advanced Research in Computer Science, 9(1), 760–764.

[36] Sahoo, S. R., Gupta, B. B. (2018). Security Issues and Challenges in Online Social Networks (Osns) Based on User Perspective. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspec- tives, 591–606.

[37] Gong, Q., Chen, Y., He, X., Zhuang, Z., Wang, T., Huang, H., ... Fu, X. (2018). DeepScan: Exploiting deep learning for malicious account detection in location-based social networks. IEEE Communications Magazine, 56(11), 21-27.

[38] Protect Your Social Media Accounts — Investor.gov. Retrieved from Investor.gov website: https://www.investor.gov/protect-your-investments/fraud/how-avoid-fraud/protect-your-social-media-accounts (accessed date 2020).

[39] How to Protect Your Privacy on Social Media?. Retrieved from Data Privacy Manager website: https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media/(accessed date 2020, July 14).

[40] Kumar, S., Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), 125-129.

[41] Singh, A., Singh, A. (2017). Review of Cyber Threats in Social Networking Websites. International Journal of Advanced Research in Computer Science, 8(5).p2695-2699.

SARAH ALMALKI received the B.Sc. degree in Information Technology from Taif University, Saudi Arabia, in 2019. She is currently a master student in Cyber Security, Taif University, Taif, Saudi Arabia. Her research interests include the Cyber Security, Social media security, and Artificial intelligence.

REHAM ALGHAMDI received the B.Sc. degree in Computer Science from Taif University, Saudi Arabia, in 2015. the diploma degree in Education from Taif University, Saudi Arabia, in 2019. She is currently a master student in Cyber Security, Taif University, Taif, Saudi Arabia. Her research interests include the Social media security, Cyber Security, and Computer Networking.

GOFRAN SAMI received the B.Sc. degree in Information System, college of Computer Science & Engineering, Taibah University, Saudi Arabia, in 2011. the M.Sc. degree in Information Management and Security from the University of Bedfordshire, United Kingdom in 2015. She is currently a lecturer with Joint First Year Deanship, Umm Al-Qura University, Makkah, Saudi Arabia. Her research interests include human computer interaction, information systems and security, and big data analytics.

WAJDI ALHAKAMI received the B.Sc. degree in Computer Science from Jeddah University, Saudi Arabia, in 2007. the M.Sc. degree in Computer Network, and the Ph.D. degree in Network Security from the University of Bedfordshire, United Kingdom in 2011 and 2016 respectively. He is currently an Assistant Professor with department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. His research interests include the Internet of Things, Cyber Security, and Computer Networking.