ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20220124140610

Preliminary communication
Received: 2022-01-24, Accepted: 2022-01-31

Major Security Issue That Facing Social Networks with Its Main Defense Strategies

Abdullah Safhi*, Adel Al-Zahrani, Mohammed Alhibbi

Abstract: The Social Network Service "SNS" has enabled significant advancements in a wide variety of scientific fields, and as a result, it has become an extremely popular subject in both academia and business. SNSs can be extremely beneficial to users because they eliminate economic and geographical barriers and can be used for job searching, entertainment and education. Regardless of the economic and social benefits, protecting businesses and users' security and privacy remains a critical issue that must be addressed. It is critical to address and evaluate social network service challenges, as they vary according to the variety of SNS sites. Thus, by discussing SNS challenges alongside available and potential solutions, users, developers, and businesses can identify relevant and timely responses to specific threats, resulting in the best SNS-based services possible. The objective of this article is to discuss the inherent challenges of social networking sites and some critical solutions for resolving them. We extracted and analyzed seminal papers to add to the corpus of literature by focusing on several critical challenges in the social network service domain and shedding light on how these challenges affect a variety of domains, including users, sites, and business. The most frequently mentioned difficulties concerned privacy risks, anonymity risks, malware, spam, identity theft, phishing, business data, social content, technical issues, and psychological difficulties. By incorporating previously discovered solutions, this paper addressed these issues. The implications for both researchers and practitioners have been discussed.

Keywords: SNS; Social Network; Social Network Challenges; Strategies and Defense

1 INTRODUCTION AND LITERATURE REVIEW

A **S**ocial **N**etwork **S**ervice (SNS) has recently gained a lot of attention due to a variety of features. SNS enables users to make new friends and expand their social circle. Another critical feature of SNS is the ability for users to share their interests, videos, photos, and activities. In today's world, social networks are extremely popular. SNSs can be extremely beneficial to users because they reduce economic and geographical barriers and can be used to accomplish goals such as job searching, entertainment, and education [16].

By definition, social networking is about fostering and reflecting personal and social ties among people who have similar values, aspirations, or interests [1]. The massive amount of data shared and disseminated on social media platforms includes users' personal information, location, address, email, usernames, and interests. Additionally, users provide updates in the form of status information, which includes their thoughts or contributions to an online discussion [3].

In a bounded system, social network sites (SNS) enable users to build an open or semi-public profile, to identify other users with whom they share a connection and to view and navigate their own list of connections as well as those made by others [1]. However, issues regarding the privacy and security of a user's information can arise, particularly when the user's uploaded content is multimedia in nature, such as photos, videos, and audios [16].

Numerous security researchers have examined and discussed security issues in social networking sites. According to Gao et al. (2011) [7], major security issues in SNSs are classified into four categories: (a) privacy concerns, (b) viral marketing, (c) network structural-based attacks, and (d) malware attacks. Their research included a detailed examination of each issue and its associated defense mechanisms. Novak & Li (2012) [14] conducted a survey of the major security and privacy concerns associated with SNSs. They discussed current techniques for protecting SNS users from a variety of entities, including SNS providers, third-party application developers, advertisers, and other users. Additionally, they provided a concise overview of link prediction, location hubs, and user attributes in SNS inference.

Jin et al. (2013) [8] examined four aspects of user behavior in SNSs: (a) malicious behavior, (b) mobile social behavior, (c) traffic activity, and (d) connection and interaction. With the proliferation of traditional threats and challenges posed by multimedia data on social networking sites, numerous researchers and security firms have proposed a variety of solutions to mitigate these threats. Watermarking [20], steganalysis [12], and digital oblivion [19] are all examples of solutions for protecting SNS users from threats posed by multimedia data. On the other hand, various solutions have been proposed to mitigate traditional threats, such as spam detection [13] and phishing detection [11].

Despite the aforementioned efforts, the gap appears in how these threats and solutions can be handled in Arabic countries. In recent years, Facebook, Twitter, YouTube, LinkedIn, Skype, 9jabook, and Logbook, among other social networking sites, have cemented their place at the center of many users' daily internet activities, becoming a primary target for hackers and vehicles for political revolutions in some countries (examples are Tunisia, Egypt, Libya, and Saudi Arabia) [1]. As a result, social network challenges must be addressed and introduced cautiously in Arabic-speaking countries, as they require a more holistic approach in these countries. The study's objective is to identify the most serious security threats that could jeopardize social network service and then determine how to manage these threats. Thus, the research questions for the article could be phrased as follow: ***What are the most significant challenges facing social network services and how are they being addressed?*** The documentary analytical descriptive strategy

will be used in this study, which entails referring to documents and literature such as research, articles, and books and addressing them in the study through description and analysis in order to elicit results and indications. To address the study's subject, this study will evaluate and critique existing literature on security issues in an internet of things environment. It will accomplish this through the use of the following research tools: databases made available via the Saudi Digital Library and international search engines. Several seminal publications have been extracted and analyzed in their entirety.

To accomplish the study's objective, a qualitative approach is taken in order to adequately describe the phenomenon under investigation. According to Saunders et al. (2003) [17], a quantitative approach examines what occurs during a phenomenon, whereas a qualitative approach sheds light on why it occurs. The descriptive analytical method is used in this study to conduct the research. Descriptive assessments place a greater emphasis on environmental variables and are based on direct observation of an individual's behavior and events occurring in his or her natural environment [4]. Descriptive research may help us better understand how reinforcement works in nature [4]. This article begins with article body section, then the discussion section, before it ends with conclusion.

2 ARTICLE BODY

The researcher will discuss extracted papers related to social network challenges: in this section. A total of ten papers will be presented, ranging from the most recent.

Al-Obeidat et al. (2020) [3] study titled "The Socio-economic Impacts of Social Media Privacy and Security Challenges": This article examined and analysed the socioeconomic impacts of social media challenges. A framework for defining the scope of the research findings allowed for the identification of appropriate measures to address challenges and mitigate socioeconomic impacts. The findings also highlighted the importance of solutions that go beyond technology, such as social science solutions that address behavioural issues and how to address them. This study identified the following social media privacy and security issues:

- **Privacy challenges:** The threats to privacy are multi-media, traditional, and social. Content exposure and transparency are harmful aspects of multimedia content. Personal and corporate reputations can be damaged by bullying, espionage, stalking, and other privacy violations such as data leakage, and profiling.
- **Security Challenges:** There are two types of security threats: classic threats that social media inherited from the web, and modern threats that are specific to social media. Both challenges are presented in Tab. 1.

Al-Obeidat et al. (2020) [3] discussed the socioeconomic consequences of social media challenges and categorized them into the following:

- Financial Crimes: Social media crimes generate an estimated $3.25 billion annually in global cybercrime. Card fraud and data hacking/selling. Hire a botnet or booter for $10/month or $25/life.
- Cyber Threats: Social media users face virtual cyber-threats. Cyber-bullying is online intimidation. Threats to cyber security, digital autonomy, and privacy are common.
- Physical Threats: Social media threats can cause property damage or death. Violence in society is one example. Social media allows virtual information exchange.
- Other Social Vices: Privacy and security issues in social media Politicians and gangsters are two examples. Social media manipulation has shaped democracy.
- Health Issues: Concerns about social media privacy and security also affect health. There's also death and depression. Financial loss and cyber-threats are typical.

Table 1 Classic and Modern Threats

Classic Threats	**Malware** is malicious software designed to steal personal data from users. Due to the nature of social media and high user interaction, malware attacks are easier on social media than other platforms.
	Phishing is another well-known threat in which cybercriminals obtain user data by impersonating legitimate third parties and using a false identity.
	Spam is unsolicited mail. Social media spam is more dangerous than email spam because users spend more time there. Spam usually contains ads or malicious links that lead to malware or phishing sites.
	Cross-site scripting is a serious security issue affecting web applications. Cross-site scripting allows cybercriminals to run malicious code on targeted users' web browsers, compromising their data or stealing cookies or other confidential data.
Modern Threats	**Sybil attacks:** Creating multiple fake identities to send messages to legitimate users and collect private data only friends can see.
	User profiling: Social media platforms analyze routine user activity, which can be accessed by cybercriminals.
	Social engineering: Using social devices and mechanisms to deceive users into disclosing confidential data.
	Identity theft: Attempts to collect personal data to benefit or harm users. They can occur when users share account details, download malicious apps, or have low privacy settings.
	Clickjacking: Tricking users into clicking on links they didn't intend to click.
	Compromised accounts: Malicious users hijacking accounts and gaining access to users' social media data.
	Inference attacks: Using data mining to collect sensitive information by analyzing available and authorized data and drawing conclusions.
	De-anonymization attacks: It's a type of inference attack where users' identities are inferred from their mobility traces.

Kožuh & Debevc (2018) [10] study titled "Challenges in Social Media Use among Deaf and Hard of Hearing People": This study examined the deaf and hard of hearing community's use of social media, including the benefits and challenges. Existing recommendations for overcoming obstacles were reviewed, and approaches for designing and

using social media efficiently were proposed. Inclusion advisors, educators, and policymakers may find the findings useful in determining how to best use social media as an inclusive tool for social participation. Based on the selected studies, this study defined three major issues facing the deaf and hard of hearing when using social media. Among the challenges are:

- **Technical issues:** There are issues with accessibility, privacy and security as well as disorganised layouts. Users are frequently digitally illiterate. Also, the social media gaffe Captions/subtitles for deaf people are rare on social media (e.g. searching jobs).
- **Psychological issues:** When users encounter privacy issues and share their passwords with peers, they risk becoming a bully or a victim of cyber bullying.
- **Social issues:** Individuals may overlook their social networks, eroding their social capital.

The study of (Kožuh & Debevc, 2018) [10] proposed recommendations for overcoming barriers to social media use among the deaf and hard of hearing. These recommendations are explained in terms of the constituent groups they serve. The following stakeholders are targeted by the recommendations found in the selected studies:

- **Social media developers and producers:** Deaf users' needs were emphasized. Communication will improve. Extend and caption web page elements to improve privacy and security.
- **Education, health and business sectors:** However, the majority of deaf and hard-of-hearing people do not own a computer. Social media educators can teach readers and writers.
- **Policy makers and other stakeholders:** Creators and developers of online content should consult disabled users. Use social media to post official alerts and track community traffic.

Rathore et al. (2017) [16] study titled "Social network security: Issues, challenges, threats, and solutions". This article examined the various security and privacy risks that every social networking user faces. It also addressed the threats posed by sharing multimedia content on social networking sites. It also discussed current state-of-the-art defense solutions for protecting social media users. Then, a future direction was discussed, along with some simple response techniques, to create a trustworthy and secure social network ecosystem. Fig. 1 depicts the paper's social network service threats.

As Rathore et al. (2017) [16] classified social network threats as multimedia, traditional, and social, they proposed solutions for establishing a more trustworthy, secure, and privacy-conscious SNS ecosystem. These solutions are described in Tab. 2.

Shaw et al. (2016) [12] study titled "Social Network Forensics: Survey and Challenges". This article discussed the forensic issues that arise in numerous social networking sites like Facebook, MySpace, LinkedIn, and Twitter. A social network is made up of nodes, or officialdoms. These nodes are linked by acquaintances, likes, and relationships. These nodes handle a lot of data. Social network forensics is the study, protection, and extraction of data using various network forensic tools. A few threats to social networking sites are listed in Tab. 3.

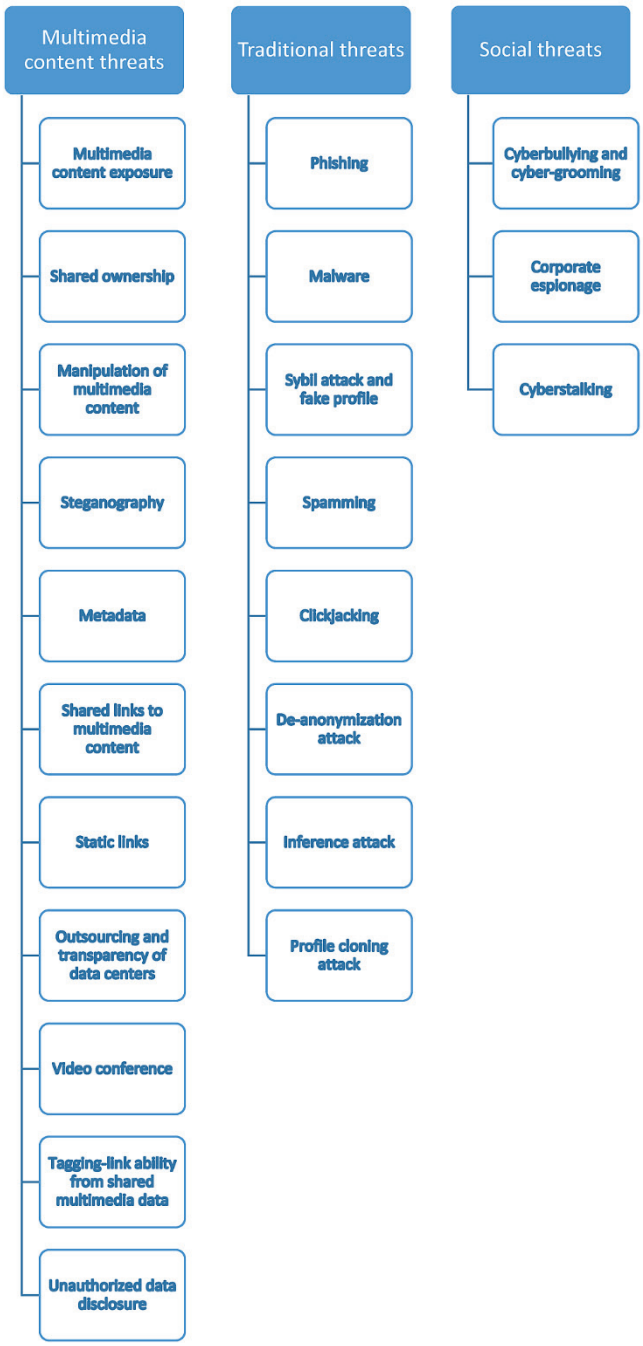

Figure 1 Classification of SNSs security threats

Chaudhary & Kumar (2015) [5] study titled "Challenges in protecting personnel information in social network space". This paper discussed a variety of cyber-related topics, including cyber-bullying, Internet banging, and cyber-attacks. The various techniques employed by the attackers have been discussed. It included a review of the privacy issues that arise as a result of the actors in the social network

graph's lack of privacy knowledge and skills or their ignorance. Finally, this paper discusses possible solutions to privacy attacks. The authors introduced privacy issue and challenges regarding social network service as follow:

- There may be little or no protection for privacy in connection with activities that involve third parties or are conducted in public. The same is true for activities that are regulated by the government.
- With the subject's permission, activity data can be used, collected, and monitored.
- When a person saves their home address as the source GPS address, one of the privacy concerns arises.
- Identity theft, personalized spam, and digital stalking are all threats on social media. Users' data can be used to train predictive models. These can be used to deduce user behavior and information.

Table 2 Solutions for social network service threats

Solution	Description
Watermarking	It embeds data into media to prove ownership. Hidden or visible watermarking An image's visible watermarking usually contains text or a logo identifying the owner. This type of watermarking is difficult to remove.
Co-ownership	Multiple users can apply their privacy settings to co-owned videos and images using the co-ownership model.
Steganalysis	Finding malicious data in multimedia files requires steganalytic software. Many traditional steganalysis methods exist. For these methods, a large dataset of images is used to train a general model that is then used to classify new images.
Digital oblivion	Digital data is given expiration date so that no one can access it after that. Thus, digital oblivion can protect large amounts of data.
Storage encryption	Encryption protects user data from malicious providers or other organizations. In SNSs, users can securely store and retrieve data without exposing it to a third-party service provider, such as a cloud-based service provider.
Metadata removal and security	Remove metadata and protect privacy in SNSs using many methods. For example, storing multimedia metadata encrypted in a file. A user may also request to edit file metadata and re-create it.
Malware detection	One proposed system detects malware. As an example, an SNS malware detection system that takes advantage of topology and malware propagation. The system adds decoy friends to a group of legitimate SNS users to monitor communication.
Sybil defense and fake profile detection	SybilDefender, for example, defends against Sybil attacks using network topology. For large SNSs, it relies on a small number of arbitrary walks within social graphs.
Phishing detection	Anti-phishing techniques are numerous. In real-time, phishAri detects phishing on Twitter That is, it can differentiate between phishing and legitimate tweets with URLs.
Spammer detection	Spam detection and SNS protection have taken time. Researchers have developed graph and content-based features, a novel social honeypot-based approach, and a data-mining technique to detect spam in SNSs.
Commercial solutions	Several security firms have developed SNS security solutions to combat evolving threats. Like FB Phishing Protector, Check Point Software developed SocialGuard Privacy Scan for Facebook.
Built-in SNS security solutions	Features like user privacy, authorization, and reporting abusive content are built into SNS. SNSs provide authentication mechanisms to ensure users are genuine (socialbot). Nowadays, CAPTCHA and MFA are used.

Table 3 Threats that social networking websites face

Facebook	**Most Hilarious Video Attack:** When the operator clicks on the video link, he or she is directed to a bogus Facebook login page. This allows the invader to steal the operator's login credentials.
	Like Jacking: Like Jacking is an attack that tricks the operator into liking a link that is potentially harmful. These worms use catchy messages to attract other users.
	Phishing Attack: Sending a unique subject email to catch the operator's eye. By clicking on this link, the user is taken to a fake Facebook page.
	Worm Based Virus: "Know who viewed your profile" entices. An extension is required to use this link. The extension installs a malware function.
MySpace	**Koobface Attack:** This attack downloads a malicious code into a user's MySpace account, turning their computers into botnets. This worm sends spam messages to operators on the acquaintance list.
	Image Attack: Fake MySpace cover pages redirect users to fake MySpace login pages. The attacker gains access to the operator's login information.
Twitter	**Denial of Service Attack:** MySpace detected a DoS attack by "Cyxymu". Tweeting the worm caused massive network traffic. Cybercriminals use SEO to lure victims to malicious websites.
	Worm Infects Twitter: The worm attacked Twitter in four stages, each increasing the worm's ability to spread and steal personal information from Twitter accounts.
	Phishing: Attackers create malicious links that redirect users to the Twitter login page and ask for login credentials.
Orkut	**XSS:** Recently, Orkut users received a message from friends containing malicious code. The attack used cross-site scripting to redirect Orkut users to a fake page. A malicious computer program is automatically installed on the victim's computer.
	Spam Phishing Attack: An operator is redirected to a fake home page in Orkut Spam Phishing. If the operator enters its login credentials, the attacker will gain access to the operator's credentials.
	Spoofed Email Attack: In a spoofed email attack, Orkut users are informed that their accounts will be terminated if the link in the message is not visited. When you click the link, a Trojan downloads other malicious files. The file monitors browser activity to steal user credentials.

Chaudhary & Kumar (2015) [5] proposed solutions for privacy breach in social network. These solutions include:

- Sanitization techniques can help protect privacy. Removing all details and friendship links from the graph reduces the classifier's accuracy.
- To maintain privacy, data mining algorithms can be developed that make use of sensitive actor information.
- Consideration can be given to policy formulation in order to protect the privacy of social networking site users.

- More privacy protection on social media. Unified access control is suggested. Control behavior is an attribute or a session. It should include: Need long-term privacy and security policies User and resource policies.
- Implement a distributed system's privacy policy. Consist of privacy metadata tables for external recipients and authorized users.
- Social media privacy is protected in two ways. Query answering can obtain insensitive information about social network actors. Attackers can re-identify actors' data. Actor identifiers are also public.

Abdulhamid et al. (2014) [1] study titled "Privacy and national security issues in social networks: the challenges". This article examined the structure and components of a member profile, as well as the privacy concerns that individuals and governments who engage in social networking face. It also examined how it can be used to distort national security, how social media platforms have evolved into new weapons of mass mobilization, and how social media platforms have evolved into rallying forces for revolutions and social justice. The following are some of the most serious threats to social networking sites.

- **Viruses:** Due to their popularity, social networking sites are frequently attacked. Infecting millions of computers by embedding a virus in a website or third-party application is simple.
- **Tools:** Hacking user accounts is very common. It can then access personal information and contacts. They can post malware as them.
- **Social Engineering Attacks:** Attackers may send phony emails or posts. Email virus or personal data request. This compromises data security and system security.
- **Identity Theft:** On-line thieves can steal your or a friend's identity. A data hacker can guess your security questions and passwords.
- **Third-party Applications:** Online games and quizzes are available. These apps may gain access to your profile data without your permission. Ads could be targeted, spam sent, or contacts accessed.
- **Business Data:** Putting company data on social media can backfire. Any information about the business could lead to liability, bad publicity, or even help competitors.
- **Professional Reputation:** Unsafe content can jeopardize a user's Colleges can be found online. Pre-interview searches are common. Respect and integrity can hurt an application.
- **Personal Relationships:** Any internet-connected computer or smartphone can post comments. Even retraction can harm. One cannot control who saves it online.
- **Personal Safety:** Not all information posted online is safe. Declaring an absence increases the risk of a break-in, especially if your address is public.

Obiniyi et al. (2014) [15] study titled "Social Network and Security Issues: Mitigating Threat through Reliable Security Model". This paper focused on educating social network users about some of the unique security issues associated with social media. It proposed an algorithm and a model for evading security threats classified as user authentication, data confidentiality, and data integrity. This paper concentrated on the following social network security issues:

- **Malware:** Tweet Worm and Koobface VIDEOMESSAGE WORMS Twitter prank attack Profile Spy is a third-party app that collects personal data and sends spam to the victims' followers.
- **Digital Dossier of Personal Information:** An attacker collects victim profiles and uses them to harm them. It's possible to harm a profile's image on most social media sites.
- **Spam:** Unsolicited email or social media messages are known as spam. Some have tried to advertise with it, but most are malicious.
- **Cross-Site Request Forgery and Cross-Site Scripting:** Unsafe websites or programs are opened on computers, and then used to attack legitimate websites (possibly submitted by the legitimate user).
- **SQL Injections:** SQL injection is a database hacking technique. Hackers can use SQL queries to target vulnerable social media apps.
- **Identity Theft:** Social media identity theft is rampant. This Facebook user attack is ongoing.
- **Phishing:** Websites pretend to be passwords to trick users. Phishing was a common problem in 2012. It's not a retreat, but a shift to social media.
- **Stalking and Cooperate Espionage:** Data leaks cost money and reputation. Employees' use of social media is unabated. Some of this data is shared blindly.
- **De-Anonymization Attack:** De-anonymization attack is another way attackers bypass user privacy settings on social networks.
- **Awareness:** What users see and share on social networking sites may be a way for attackers to gain access. Be wary of fancy stories, images, and URLs.

The approach developed by Obiniyi et al. (2014) [15] emphasizes the confidentiality, integrity, and authentication of information/data. Confidentiality is the assurance given to an entity (data or information) that it will not be read or accessed by anyone other than the recipient specified by the sender. The integrity of an entity (data or information) entails the assurance that it has not been altered, either intentionally or unintentionally. Finally, authentication provides an entity (system, data, or information) with the assurance that another entity (which could be a user or agent) is who it claims to be. Cryptography is critical for maintaining the confidentiality and integrity of data. Fig. 2 shows user-to-user encrypted post model for confidential and Integrity of user post.

Ajami et al. (2011) [2] study titled "Security Challenges and Approaches in Online Social Networks: A Survey". This article discussed various methods and approaches for ensuring social network security for both providers and users (SNs). This article discussed several examples of this type of research. While all models surveyed prioritized user privacy,

they ignored other critical issues. These areas offer numerous opportunities for new or existing mechanisms to investigate and design mechanisms that do not require (or at least minimize) trade-offs in terms of user privacy, data security and performance. Social network security poses the following technical challenges:

- **Privacy risks:** Data sharing risks must be disclosed to users. Also, the SN privacy tools are hard to use and lack customization. Personal information like photos and friends is also uncontrollable.
- **Security risks:** Passwords are reset using fake social media accounts or emails. Cybercriminals can use SN sites to steal users' data.
- **Anonymity risks:** Users' identities and privacy are stolen. A mobile device connecting to an SN site exposes users' personal information and location.
- **Other risks:** Other risks on SN may compromise the user or the SN providers. Some are physical, but most are logical. Some examples:
  - Connecting home devices to an SN site may reveal more about the users. Unprotected devices may compromise other devices on the home network.
  - The SN and its users are exposed to SN site operators and possibly their partners. Large-scale SN privacy breaches may compromise user data. Intentional or accidental data disclosure violates privacy.
  - Furthermore, many SN sites are free, and providers may disappear at any time, denying users access to their data. Using a false identity or group collusion may allow access to personal data.
  - The lack of user-provider trust jeopardizes the success of SN sites. Users must trust each other, service providers, and in many cases, partners. It's difficult to build or maintain trust.

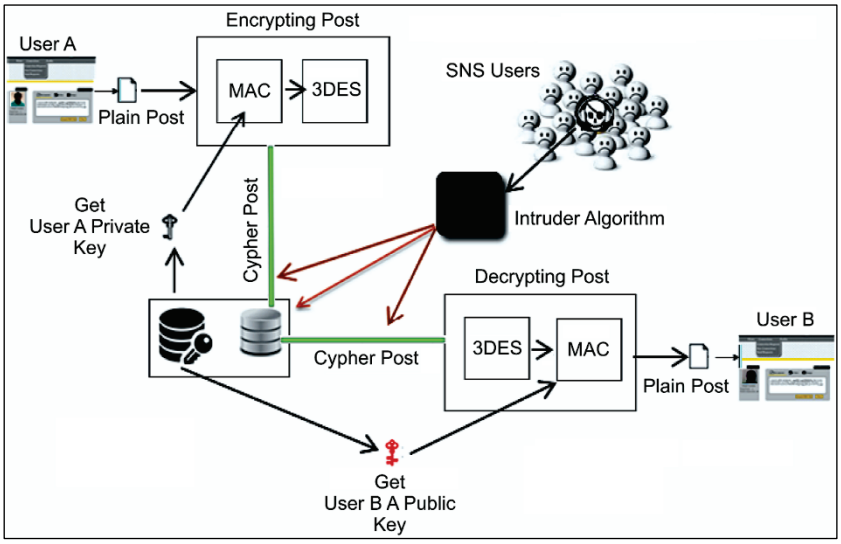

Figure 2 User-to-User Encrypted post model

Table 4 Advices for companies deciding to use Social Media

Five points about using media	Choose carefully: The best medium for any purpose depends on the target audience and the message.
	Pick the application, or make your own: In some cases, it may be better to simply join an established Social Media application and leverage its popularity and user base.
	Ensure activity alignment: It is critical to coordinate all of your Social Media activities.
	Media plan integration: The same holds true for the relationship between Social Media and traditional media: Igniting is key While you may think these two areas are distinct, your customers see them as part of the same entity: your corporate image.
	Access for all: After the company has decided to use Social Media applications, it is important to ensure that all employees can access them.
Five points about being social	Be active: Social media is all about sharing and interacting so keep your content fresh and engage with your customers.
	Be interesting: As a result, if you want your customers to engage with you, you need to give them more than just the best airline or the best kitchen blender.
	Be humble: Before entering any application, learn about its history and basic rules. Start participating only after you have gained the necessary understanding.
	Be unprofessional: People on social media, like you, recognize that life is not always easy. A nice person may even offer free advice on how to improve your performance next time.
	Be honest: Because you're dealing with some of the most technologically advanced people on the planet, don't expect other participants to remain anonymous.

Kaplan & Haenlein (2010) [9] study titled "Users of the world, unite! The challenges and opportunities of Social Media". This study began by defining Social Media and comparing it to related concepts like Web 2.0 and User Generated Content. Based on this definition, it classified Social Media into more specific categories by characteristic:

collaborative projects, blogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. Finally, it offered ten suggestions for businesses using social media.

Kaplan & Haenlein (2010) [9] proposed ten pieces of advice for companies deciding to use Social Media. Tab. 4 summarizes these advices.

3 DISCUSSION

The study emphasized in this section how each study included in the review addressed social network challenges from a unique perspective.

Concentrating on the socioeconomic consequences of social media challenges, Al-Obeidat et al. (2020) [3] discussed the socioeconomic consequences of social media challenges and categorized them into financial Crimes, cyber Threats, physical Threats, other Social Vices, health Issues, and reputational Damage. Concentrating on the people suffering from deaf and hard of hearing, Kožuh & Debevc (2018) [10] proposed recommendations for overcoming barriers to social media use among the deaf and hard of hearing focusing on stakeholders such as social media developers and producers, education, health and business sectors, and policy makers and other stakeholders. As Rathore et al. (2017) [16] classified social network threats as multimedia, traditional, and social, they proposed solutions for establishing a more trustworthy, secure, and privacy-conscious SNS ecosystem. This ecosystem include Watermarking, Co-ownership, Steganalysis, Digital oblivion, Storage encryption, Metadata removal and security, Malware detection, Sybil defense and fake profile detection, Phishing detection, Spammer detection, Commercial solutions, and Built-in SNS security solutions. To handle social network challenges, a security enforcement algorithm and model for a social networking site have been proposed by Obiniyi et al. (2014) [14]. This approach emphasizes the confidentiality, integrity, and authentication of information/data. Fig. 3 shows user-to-user encrypted post model for confidential and Integrity of user post. Similarly, Ajami et al. (2011) [2] proposed fourteen distinct security strategies for SNs.

Regarding privacy defenses and awareness, Chewae et al. (2015) [6] recommended strategies such as a privacy awareness campaign can help users understand their rights, the role of schools and institutes in educating students, and stronger authentication and access control to prevent the threats. Chaudhary & Kumar (2015) [5] proposed solutions for privacy breach in social network. These solutions include sanitization techniques, data mining algorithms, policy formulation, user-centered approach to access control, and system's privacy policy.

More generally with concentrating on companies, Kaplan & Haenlein (2010) [9] proposed ten pieces of advice which divided into company level and personal level for companies deciding to use Social Media. Company level includes choosing the medium carefully, ensuring activity alignment, integrating media plan and access for all employees. While on the other hand, personal level includes active, interesting, humble, unprofessional, and honest.

On the other hand, Shaw et al. (2016) [16] introduced a process model (Fig. 2) and tools for each stage of network forensic analysis (Table 4) in order to investigate the point of vulnerability of social networking sites in order to gain a better understanding of the challenges these sites face.

4 CONCLUSION AND FUTURE WORKS

As a result of the social network service challenges, enormous opportunities have opened up. Along with influencing everyone's social and economic behavior, the social networking service has had an impact on their way of life and thought. While social networking sites have improved economic and social outcomes, they have also introduced a slew of security risks. This article discusses a variety of security features and issues in the social network service environment, including privacy risks, anonymity risks, malware, spam, identity theft, phishing, business data, professional reputation, and personal relationships.

Additionally, it encompasses difficulties associated with multimedia content, social content, technical issues, psychological issues, and the majority of threats directed at Facebook, MySpace, Twitter, and Orkut. Additionally, it discusses preventative measures for these issues. These contributions to research can be found on both a theoretical and practical level. Theoretically, this study focuses on the most prevalent challenges in a variety of fields, which can aid scholars in developing a holistic understanding of these issues and validating the methods used to address them. To address these issues, this study incorporates previously identified solutions. In practice, these solutions would benefit organizations and individuals who interact with these social media platforms. While some progress has been made, much more work remains to be done to safeguard social network service and privacy. To address social network service security concerns effectively, technological solutions must be combined with appropriate laws and regulations.

5 REFERENCES

[1] Abdulhamid, S. M., Ahmad, S., Waziri, V. O., & Jibril, F. N. (2014). Privacy and national security issues in social networks: the challenges. ArXiv Preprint ArXiv: 1402.3301.

[2] Ajami, R., Ramadan, N., Mohamed, N., & Al-Jaroodi, J. (2011). Security challenges and approaches in online social networks: A survey. *IJCSNS, 11*(8), 1.

[3] Al-Obeidat, F., Hani, A. B., Adedugbe, O., Majdalawieh, M., & Benkhelifa, E. (2020). The Socio-economic Impacts of Social Media Privacy and Security Challenges. In G. Xu, K. Liang, & C. Su (Eds.), *International Conference on Frontiers in Cyber Security* (pp. 553-563). Springer Singapore. https://doi.org/10.1007/978-981-15-9739-8_41

[4] Anderson, C. M. & Long, E. S. (2002). Use of a structured descriptive assessment methodology to identify variables affecting problem behavior. *Journal of Applied Behavior Analysis, 35*(2), 137-154. https://doi.org/10.1901/jaba.2002.35-137

[5] Chaudhary, M. & Kumar, H. (2015). Challenges in protecting personnel information in social network space. *International*

Conference on Emerging Trends in Networks and Computer Communications (ETNCC 2015), 99-104. https://doi.org/10.1109/ETNCC.2015.7184816

[6] Chewae, M., Hayikader, S., Hasan, M. H., & Ibrahim, J. (2015). How much privacy we still have on social network? *International Journal of Scientific and Research Publications, 5*(1), 2250-2315.

[7] Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security Issues in Online Social Networks. *IEEE Internet Computing, 15*(4), 56-63. https://doi.org/10.1109/MIC.2011.50

[8] Jin, L., Chen, Y., Wang, T., Hui, P., & Vasilakos, A. V. (2013). Understanding user behavior in online social networks: a survey. *IEEE Communications Magazine, 51*(9), 144-150. https://doi.org/10.1109/MCOM.2013.6588663

[9] Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons, 53*(1), 59-68. https://doi.org/https://doi.org/10.1016/j.bushor.2009.09.003

[10] Kožuh, I. & Debevc, M. (2018). Challenges in Social Media Use among Deaf and Hard of Hearing People. In N. Dey, R. Babo, A. S. Ashour, V. Bhatnagar, & M. S. Bouhlel (Eds.), *Social Networks Science: Design, Implementation, Security, and Challenges* (pp. 151-171). Springer International Publishing. https://doi.org/10.1007/978-3-319-90059-9_8

[11] Lee, S. & Kim, J. (2013). WarningBird: A Near Real-Time Detection System for Suspicious URLs in Twitter Stream. *IEEE Transactions on Dependable and Secure Computing, 10*(3), 183-195. https://doi.org/10.1109/TDSC.2013.3

[12] Li, F., Wu, K., Lei, J., Wen, M., Bi, Z., & Gu, C. (2016). Steganalysis over Large-Scale Social Networks with High-Order Joint Features and Clustering Ensembles. *IEEE Transactions on Information Forensics and Security, 11*(2), 344-357. https://doi.org/10.1109/TIFS.2015.2496910

[13] Miller, Z., Dickinson, B., Deitrick, W., Hu, W., & Wang, A. H. (2014). Twitter spammer detection using data stream clustering. *Information Sciences*, 260, 64-73. https://doi.org/https://doi.org/10.1016/j.ins.2013.11.016

[14] Novak, E. & Li, Q. (2012). A survey of security and privacy in online social networks. *College of William and Mary Computer Science Technical Report*, 1-32.

[15] Obiniyi, A. A., Oyelade, O. N., & Obiniyi, P. (2014). Social Network and Security Issues: Mitigating Threat through Reliable Security Model. *International Journal of Computer Applications, 103*(9). https://doi.org/10.5120/18099-9163

[16] Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421, 43-69. https://doi.org/https://doi.org/10.1016/j.ins.2017.08.063

[17] Saunders, M., Lewis, P., & Thornhill, A. (2003). Research methods for business students. Essex: Prentice Hall: *Financial Times*.

[18] Shaw, U., Das, D., & Medhi, S. P. (2016). Social Network Forensics: Survey and Challenges. *International Journal of Computer Science and Information Security, 14*(11), 310.

[19] Stokes, K. & Carlsson, N. (2013). A peer-to-peer agent community for digital oblivion in online social networks. *2013 Eleventh Annual Conference on Privacy, Security and Trust*, 103-110. https://doi.org/10.1109/PST.2013.6596043

[20] Zigomitros, A., Papageorgiou, A., & Patsakis, C. (2012). Social Network Content Management through Watermarking. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 1381-1386. https://doi.org/10.1109/TrustCom.2012.264

Authors' contacts:

Abdullah Safhi
(Corresponding author)
King Abdulaziz University, Jeddah, Saudi Arabia
sardjijo12@hotmail.com
https://orcid.org/0000-0002-6385-1721

Adel Al-Zahrani
King Abdulaziz Medical City NGHA, Jeddah, Saudi Arabia

Mohammed Alhibbi
King Abdulaziz Medical City NGHA, Jeddah, Saudi Arabia