Journal of Artificial Intelligence and Computational Technology

Journal homepage: https://ojs.omgfzc.com/index.php/JECT

Combatting Cybersecurity Threats on Social Media: Network Protection and Data Integrity Strategies

Ashraf jalal yousef Zaidieh

Faculty applied college, Imam Mohammad Ibn Saud Islamic University, Saudi Arabia

*Correspondence: E-mail: *Azedia3@gmail.com*

Article Info

Article History:
Submitted/Received 06 July 2024
Revised in revised format 10 August 2024
Accepted 13 September 2024
Available 15 October 2024
Publication Date 15 October 2024

Keyword:
Social media cybersecurity, network protection, data integrity, identity theft, phishing, malware, multi-factor authentication, encryption, user education, regulatory compliance.

Cite this article: *Zaidieh, A. J. Y. (2024). Combatting cybersecurity threats on social media: Network protection and data integrity strategies. Journal of Artificial Intelligence and Computational Technology, 1(1).*

ABSTRACT

The rise of social media has transformed global communication, but it has also introduced significant cybersecurity threats, including identity theft, phishing, malware distribution, and data breaches. These challenges not only compromise individual users but also pose risks to businesses and governments. This research explores the prevalent cybersecurity threats on social media and proposes an integrated framework to enhance network protection and data integrity. The framework combines both technical solutions such as encryption, multi-factor authentication, and AI-based threat detection and non-technical strategies like user education, platform policies, and collaborative efforts among stakeholders. By synthesizing findings from a comprehensive literature review, this study identifies the most common cyber threats and assesses their impacts on users, businesses, and society at large. The research highlights the importance of proactive measures, including real-time monitoring, secure data practices, and user behavior modification, to mitigate these risks. Additionally, the study emphasizes the need for greater collaboration between platform providers, governments, and users to create a safer digital environment. The proposed framework is flexible and applicable across various social media platforms, providing a holistic approach to combatting evolving cyber threats. This study contributes to the growing body of knowledge on social media cybersecurity, offering practical recommendations for improving security and maintaining the integrity of online networks.

1. INTRODUCTION

has revolutionized the way individuals and organizations communicate, share information, and interact with each other on a global scale [1]. However, the exponential growth in the use of social media platforms has also brought about an increase in cybersecurity threats such as identity theft, misinformation, data breaches, and cyberstalking. These threats have become a significant concern for users, businesses, and governments alike, as they can lead to severe economic, social, and political repercussions is a multifaceted challenge that requires a comprehensive understanding of the underlying issues and the development of robust strategies for network protection and data integrity [2]. This article aims to explore the current state of cybersecurity threats on social media, propose a framework for network protection and data integrity strategies, and evaluate the effectiveness of these strategies through a rigorous literature review and analysis. The rapid growth and adoption of social media have transformed how individuals, businesses, and governments communicate and share information on a global scale. Platforms like Facebook, Twitter, Instagram, and LinkedIn have become integral parts of modern communication. However, the pervasive use of social media has exposed users and organizations to a wide array of cybersecurity threats, including identity theft, misinformation, data breaches, and cyberstalking. These threats are not only growing in frequency but also in sophistication, leading to significant economic, social, and political repercussions [3]. This research article seeks to investigate the landscape of cybersecurity threats on social media, with a focus on understanding the types of attacks and proposing comprehensive strategies to protect network infrastructures and ensure data integrity. Through a detailed exploration of current threats and a rigorous analysis of network protection measures, this study aims to contribute to the development of a safer digital environment on social media platforms.

While significant progress has been made in understanding and addressing cybersecurity threats on social media, there are several gaps that remain. First, [4, 5] argue that most existing studies focus on technical solutions while neglecting the social and behavioral aspects of cybersecurity. More research is needed on how social norms and psychological factors influence user behavior on social media and how these insights can be integrated into more effective cybersecurity strategies.

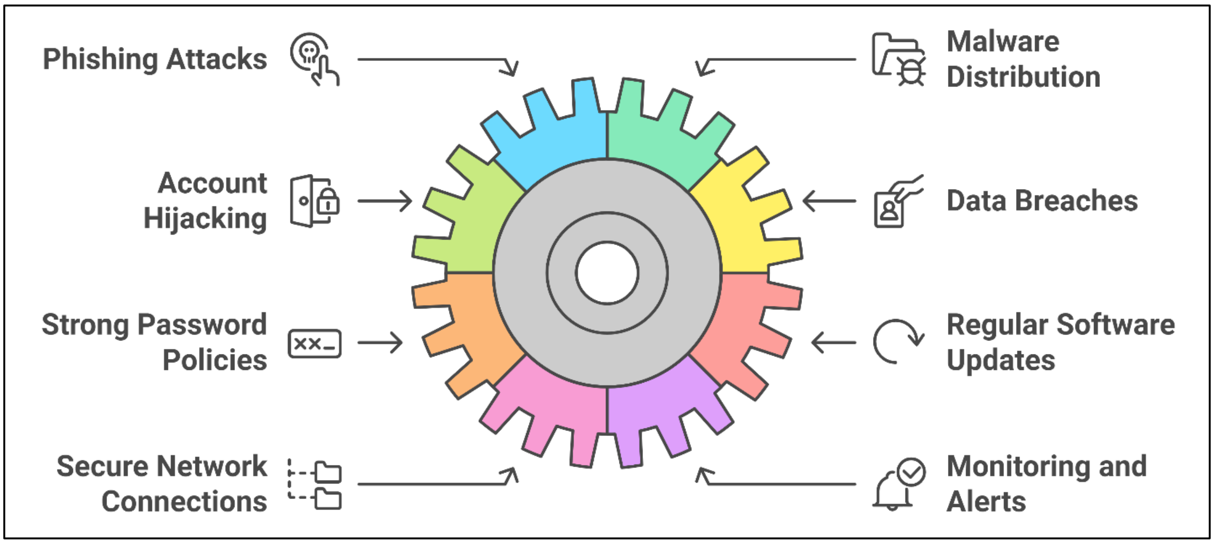

Figure 1: Safeguarding Social Media from Cyber Threats

1.2 Research Objectives

The primary objective of this research is to investigate the various cybersecurity threats prevalent on social media platforms and to develop a framework that integrates both technical and non-technical strategies for enhancing network protection and data integrity. The specific research objectives include:

1. Identifying the most common types of cybersecurity threats on social media.

2. Analyzing the impact of these threats on users, businesses, and society.
3. Examining existing network protection and data integrity strategies.
4. Proposing an integrated framework for combatting social media cybersecurity threats.

1.3 Motivations

The motivation for this research is threefold. Firstly, the increasing reliance on social media for both personal and professional purposes necessitates a thorough understanding of the risks involved. Secondly, the interconnected nature of social media platforms amplifies the potential harm of a single data breach or cyber-attack, making it crucial to implement robust protection measures. Lastly, the evolving landscape of cyber threats demands a continuous reassessment and adaptation of existing strategies to ensure that social media remains a secure and reliable communication channel.

1.4 Contributions

This study contributes to the growing body of knowledge on social media cybersecurity by:

- Proposes an integrated framework combining technical and non-technical strategies for enhancing social media cybersecurity.
- Identifies key cybersecurity threats on social media, such as identity theft, phishing, and malware.
- Offers practical recommendations for improving network protection and data integrity based on a thorough literature review.
- Highlights the importance of user education and collaborative efforts between platforms, users, and regulatory bodies.
- Provides a foundation for future research on evolving cyber threats and innovative protection strategies.

2. Literature Review

Social media platforms like Facebook, Twitter, Instagram, and LinkedIn have drastically transformed digital communication and social interaction. However, the rise of these platforms has been paralleled by increasing cybersecurity risks. These risks include identity theft, phishing, malware, cyberstalking, and misinformation campaigns, all of which have severe implications for both individuals and organizations [6]. Cybersecurity in the realm of social media is particularly challenging due to the nature of these platforms, which prioritize connectivity and data sharing over security. As a result, personal and sensitive information becomes vulnerable to cyber-attacks and exploitation [7]. Several studies have examined the types of cybersecurity threats prevalent on social media platforms. **Phishing**, where attackers masquerade as legitimate entities to trick users into revealing sensitive information, is one of the most common threats. Research by [8] indicates that phishing attacks have become more sophisticated, with attackers using personal details from social media profiles to craft highly targeted attacks. Similarly, **malware** is another frequent concern, where attackers inject malicious software into user devices via social media links or advertisements. The work of *[9]* highlight that social media platforms often become carriers for malware due to the high level of trust between users and shared content. Furthermore, **cyberstalking** and **harassment** have been identified as growing threats on social media, particularly affecting vulnerable users such as teenagers and women [10]. These forms of harassment can lead to severe psychological and emotional impacts, making cybersecurity a pressing issue for platform developers. In addition, the **social implications** of social media cyber-attacks are wide-ranging. As noted by *[11]*, identity theft and misinformation campaigns can create significant societal instability by eroding trust in digital platforms. These campaigns are often aimed at political disruption, as seen during elections in various countries, including the 2016 U.S. Presidential election, where misinformation was used to influence voter behavior [12]. The **political consequences** of such attacks are profound, as they challenge the democratic processes and undermine the credibility of political institutions.

3. Methodology

The methodology for this research focuses on a systematic review of the current literature on cybersecurity threats in social networks, particularly how these threats affect network protection and data integrity [13]. The study adopts a qualitative approach to synthesize findings from a wide array of sources, including academic journals, industry reports, and case studies [14]. This approach ensures a comprehensive understanding of the landscape of cybersecurity threats and the development of an effective framework for addressing them.

3.1 Research Design and research questions

This research follows a qualitative design, with a primary focus on conducting a systematic literature review. A qualitative approach is chosen due to the exploratory nature of the research, as it aims to provide an in-depth understanding of existing strategies and propose an integrated framework. The research does not involve primary data collection but relies on secondary data sources. As highlighted by [13], qualitative research is valuable when the goal is to gain a detailed understanding of a problem by analyzing non-numerical data such as text from literature. The systematic review method is chosen for its ability to rigorously analyze existing literature, identify gaps, and synthesize findings to create a cohesive framework [15]. The methodology integrates insights from various disciplines such as computer science, information security, behavioral psychology, and social network analysis to ensure the proposed framework addresses the technical and social aspects of network protection.

This study aims to address several critical research questions that are central to understanding and enhancing network protection on social media platforms. The formulated research questions include (Table 1):

Table 1: Research questions and its aims

Research Question	Aim
RQ1: What are the most prevalent types of cybersecurity threats faced by users on social media platforms?	This question seeks to identify and categorize the various forms of cyber threats, including identity theft, phishing, and misinformation, that pose risks to individuals and organizations using social media.
RQ2: How do these cybersecurity threats impact users, businesses, and society at large?	Understanding the broader implications of these threats will help assess their economic, social, and political consequences, highlighting the need for effective protection measures.
RQ3: What existing strategies for network protection and data integrity are currently implemented on social media platforms?	An analysis of current strategies will provide insights into the effectiveness and gaps in existing security measures, informing the development of improved frameworks.
RQ4: What integrated framework can be proposed to combat cybersecurity threats on social media?	This question aims to synthesize both technical and non-technical strategies into a cohesive framework that enhances security across various social media platforms.

3.2 Data Sources and Selection Criteria

The literature review is based on studies published within the last ten years, ensuring the inclusion of recent and relevant research. Key academic databases such as IEEE Xplore, Google Scholar, and SpringerLink are utilized to collect peer-reviewed articles, books, and conference papers. Additionally, the inclusion criteria for the literature are based on relevance to the research objectives, and the use of established research methods. The search terms used include “social media cybersecurity,” “network protection,” “data integrity,” “cyber threats in social networks,” and “user behavior and cybersecurity risks.”

Articles and reports that meet the following criteria are selected:

- Published between 2014 and 2024.
- Direct relevance to social media cybersecurity threats, network protection, or data integrity.
- Contain empirical data or systematic analyses.
- Include discussions of both technical (e.g., encryption, firewalls) and non-technical (e.g., user education, policy frameworks) strategies.

This ensures that the literature covers a wide spectrum of perspectives and approaches. Articles focusing on cybersecurity in other contexts, such as e-commerce or cloud computing, are excluded unless they offer directly transferable insights into social media security. Table 2 present inclusions and exclusions criteria

Table 1: Data Sources and Selection criteria inclusions and exclusions:

Selection Criteria	Description	Inclusions	Exclusions
Publication Date	Articles and reports must be published between 2014 and 2024 to ensure the relevance and timeliness of the information presented.	Studies published between 2014 and 2024.	Publications outside this date range.
Relevance to Cybersecurity	Selected works must have direct relevance to social media cybersecurity threats, network protection, or data integrity, focusing specifically on the unique challenges presented by social media.	Articles addressing social media cybersecurity threats specifically.	Works focused on general cybersecurity without social media context.
Discussion of Strategies	Selected articles must include discussions of both technical strategies (e.g., encryption, firewalls) and non-technical strategies (e.g., user education, policy frameworks) to provide a comprehensive understanding of the approaches to cybersecurity.	Research detailing both technical and non-technical strategies for cybersecurity.	Articles focusing on only one type of strategy.
Transferable Insights	Excluded works must primarily focus on cybersecurity in other contexts, such as e-commerce or cloud computing, unless they provide directly transferable insights into social media security.	Works offering insights that can be adapted to social media security from related fields.	Research strictly limited to e-commerce or cloud computing contexts without social media relevance.

3.3 Data Analysis

A systematic is employed to synthesize the literature. This method allows for the identification of recurring themes, patterns, and gaps in the research [16]. The analysis is conducted in several stages:

1. **Data Familiarization:** The selected articles are read multiple times to familiarize the researcher with the content and identify preliminary themes related to cybersecurity threats and network protection strategies.
2. **Coding:** Each article is systematically coded based on the research objectives. Codes are developed for key concepts such as phishing, malware, user awareness, encryption, data breaches, and platform security policies. This process ensures that all relevant information is captured in a structured manner.
3. **Theme Development:** After coding, the codes are grouped into overarching themes. These include user behavior, technical solutions, platform policies, and collaborative efforts. The goal

is to identify how these themes interact to form an integrated framework for network protection and data integrity.

4. **Synthesis:** The final step involves synthesizing the findings from the literature review to develop the proposed framework. This framework is built on the themes identified and incorporates both technical and behavioral insights to address the multifaceted nature of cybersecurity threats in social networks.

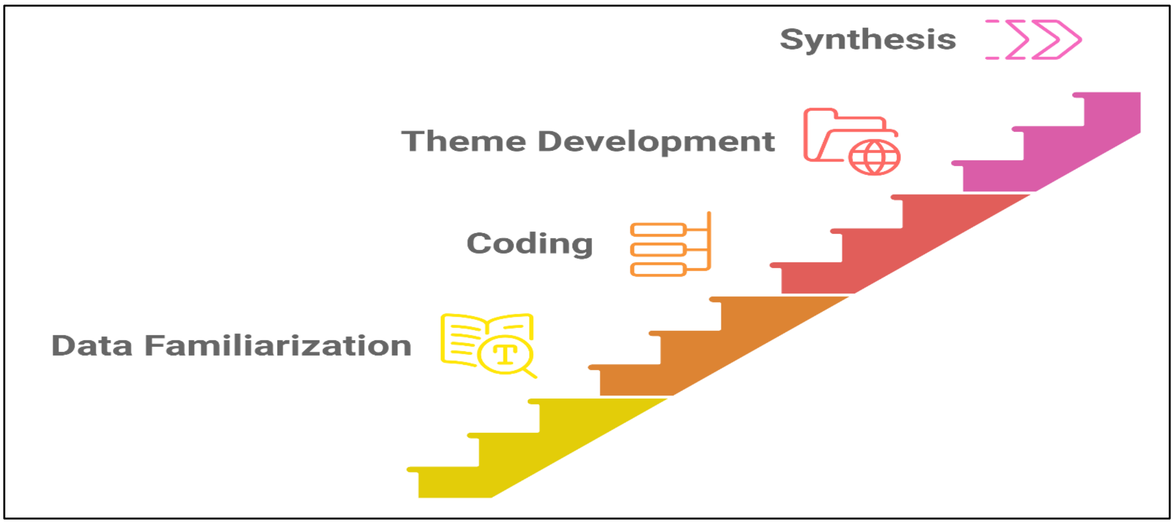

Figure 2: Research process

3.4 Framework Development

The proposed framework is based on the synthesis of technical and non-technical strategies identified in the literature. Technical solutions such as encryption, intrusion detection systems, and secure protocols are combined with user education programs and regulatory measures to create a comprehensive approach. The framework is designed to be adaptable to different social media platforms, ensuring its relevance for users, businesses, and governments. Additionally, a comparative analysis is conducted to evaluate the effectiveness of the proposed framework. This involves comparing the framework's recommendations with existing security strategies implemented by major social media platforms. Case studies of real-world cyber incidents, such as the Facebook-Cambridge Analytica scandal and Twitter's data breach, are analyzed to assess the practical applicability of the framework [17].

4. Results

RQ1: What are the most prevalent types of cybersecurity threats faced by users on social media platforms?

Social media platforms have become fertile ground for a wide array of cybersecurity threats, due to their vast user base, interconnectedness, and often relaxed security measures. As more individuals and organizations use these platforms to communicate, share data, and engage in digital interactions, they have also become increasingly vulnerable to cyber threats. This section delves into the most common types of cybersecurity threats plaguing social media platforms, focusing on identity theft, phishing, malware distribution, spam, and unauthorized access, which together represent significant concerns for users, businesses, and governments [17].

A. Identity Theft

One of the most pervasive threats on social media is identity theft, where malicious actors gain unauthorized access to personal information to impersonate individuals for fraudulent purposes [18]. Social media profiles often contain a treasure trove of personal data, including names, birthdates, addresses, and even employment details, making users prime targets for identity theft. Attackers may use this information to create fake accounts or steal financial details, which can result in significant financial loss and reputational damage for victims. According to [19], identity theft cases on social media have increased in recent years due to lax privacy settings and users' tendency to overshare personal information online.

While most platforms now provide privacy controls, many users fail to utilize them effectively, leaving their profiles and sensitive information publicly accessible [20]. Attackers may also exploit weak password practices, especially in cases where users reuse passwords across multiple platforms. Additionally, cybercriminals can hijack accounts using techniques such as password cracking or social engineering, allowing them to further perpetuate fraudulent activities.

B- Phishing

Phishing attacks are another prevalent threat on social media, wherein attackers deceive users into revealing sensitive information, such as login credentials or financial data. Social media platforms are increasingly being used as conduits for phishing schemes due to their massive user base and the ease with which malicious links can be shared. Phishing often occurs through fake messages, posts, or ads that masquerade as legitimate communications from trusted organizations or individuals [8]. A common phishing technique on social media is the use of fraudulent links embedded in direct messages or comments, leading users to malicious websites that mimic official login pages or payment gateways [2]. Once users enter their credentials, attackers capture the data for unauthorized access. This method has been particularly effective as users often trust messages that appear to come from friends or colleagues. According to research, phishing attacks accounted for a significant percentage of cyber-attacks on social platforms, as they exploit users' trust and the casual nature of social media interactions [21]. Moreover, the rise of spear-phishing targeted phishing attacks aimed at specific individuals or organizations has been amplified by the availability of personal data on social media. Attackers craft highly personalized messages that increase the likelihood of victims falling for the scam. Social platforms also enable phishing campaigns to spread rapidly as malicious content can be shared and re-shared within seconds [22].

C- Malware Distribution

Malware, or malicious software, has found its way onto social media platforms as cybercriminals exploit the openness of these platforms to distribute harmful programs. Malware can be delivered in many forms, including links in posts, ads, or messages that, when clicked, download malicious software onto users' devices. Common types of malware spread via social media include viruses, ransomware, and spyware, which are designed to steal information, encrypt data for ransom, or monitor users' activities [23]. A study by [2] revealed that social media is increasingly being used as a delivery mechanism for malware due to its ability to propagate rapidly across networks [20]. Once a user's account is compromised, attackers can use that account to share malicious links with the victim's entire friend list, spreading the malware even further [24]. Some sophisticated malware types are even able to hide within social media ads, taking advantage of third-party advertising networks to infiltrate users' devices. A particularly worrying trend is the use of social engineering to enhance malware distribution. Attackers manipulate users into clicking on seemingly harmless links or downloads, often using emotional appeals or curiosity. For example, posts promising sensational content, fake giveaways, or urgent security alerts can trick users into unknowingly downloading malware [21].

D- Spam and Scams

Spam on social media refers to the flood of unsolicited messages, comments, or posts that aim to lure users into clicking on malicious links or engaging in fraudulent schemes. While not all spam is harmful, a significant portion is linked to scams, such as fake lotteries, counterfeit goods, or investment frauds. According to a study by [25], the increase in social media spam poses a serious security threat, as it often disguises malicious content behind seemingly innocent promotions [26]. Social media scams often involve exploiting trending topics or popular events, making the scams appear timely and relevant to users. For instance, attackers may create fake accounts or posts related to disasters, elections, or pandemics to solicit donations or personal information from well-meaning individuals. As these scams often spread rapidly due to the viral nature of social media, they can reach a large audience before being detected and removed by platform administrators [27].

E- Unauthorized Access and Account Hijacking

Unauthorized access to social media accounts is another major threat, often resulting from weak passwords, phishing, or data breaches [20]. Once attackers gain control of an account, they can misuse it for various malicious activities, such as spreading malware, engaging in scams, or further compromising the victim's contacts. Account hijacking also enables attackers to impersonate the victim, which can lead to reputational damage, financial fraud, and even emotional harm [28]. Social media platforms are attractive targets for attackers due to the vast amount of personal and professional information available on user profiles. Once compromised, these accounts can be exploited for financial gain or even used as a stepping stone to infiltrate larger organizations [29]. Additionally, some hijacked accounts are sold on the dark web, where buyers can misuse them for illegal activities, such as money laundering or identity fraud. Table 3 below summarize the threats and its descriptions along with its impacts.

Table 3: Threats impacts and its descriptions

Threat	Description	Impacts	Citations
Identity Theft	Malicious actors gain unauthorized access to personal information on social media, allowing them to impersonate users for fraudulent activities. Many users neglect privacy settings, increasing vulnerability.	Victims face financial loss and reputational harm due to fake accounts and stolen information.	[30, 31]
Phishing	Attackers deceive users into revealing sensitive information through fake messages or links that appear legitimate. This exploitation of trust makes users susceptible.	Compromised accounts lead to unauthorized access, particularly through tailored spear-phishing attacks.	[8, 32]
Malware Distribution	Cybercriminals exploit social media to spread malware via malicious links in posts or messages. Types include viruses and ransomware, often disguised as legitimate content.	Infected accounts can further distribute malware among users, often through emotional manipulation.	[2, 32]
Spam and Scams	Unsolicited messages aim to lure users into clicking harmful links or engaging in fraudulent schemes, often leveraging trending topics to appear legitimate.	Scams can spread quickly, resulting in financial loss and data compromise for users.	[33, 34]
Unauthorized Access and Account Hijacking	Weak passwords and phishing lead to unauthorized access, enabling attackers to misuse accounts for various malicious activities.	Compromised accounts may be sold on the dark web for illegal activities like identity fraud.	[22, 35]

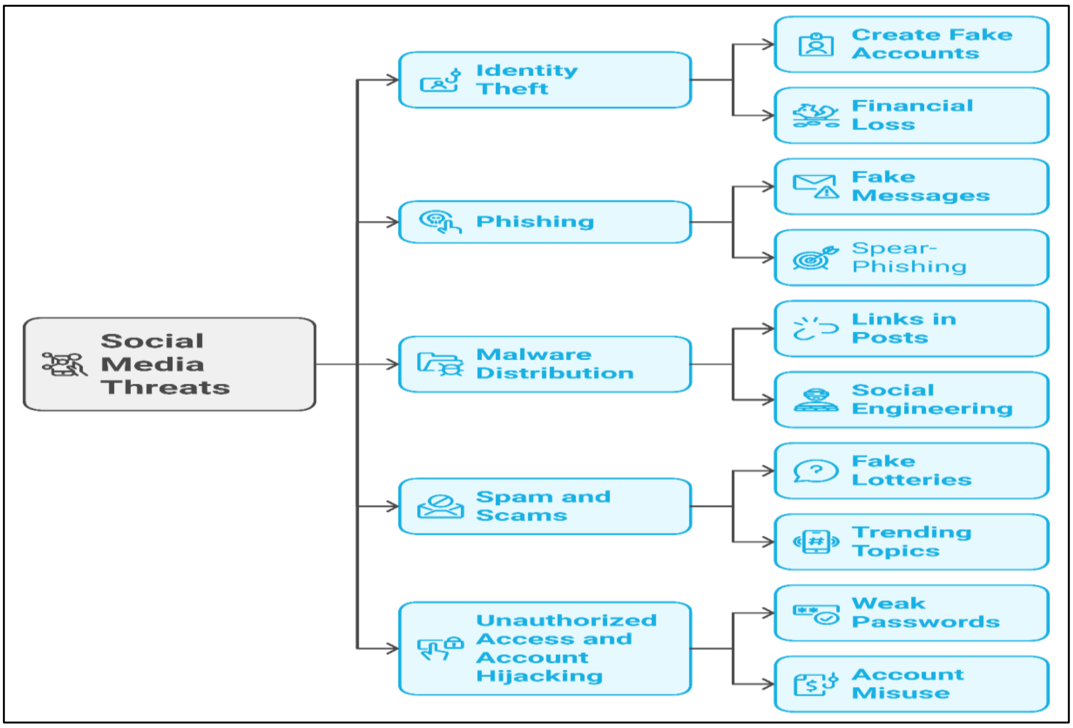

Figure 3: Social Media Threats

RQ2: How do these cybersecurity threats impact users, businesses, and society at large?.

The growing prevalence of cybersecurity threats on social media platforms has far-reaching implications for individuals, businesses, and society at large. These platforms, while revolutionizing communication, have also introduced vulnerabilities that cybercriminals exploit, resulting in personal, economic, and societal consequences. The most common cyber threats identity theft, phishing, malware distribution, spam, and unauthorized access not only compromise user privacy but also have significant effects on business operations and the social fabric of our communities. This section analyzes these impacts, highlighting the intertwined risks and challenges posed by cybersecurity threats in the digital age [36].

Impact on Users

1. **Privacy Invasion and Identity Theft** For individual users, privacy breaches and identity theft are among the most devastating consequences of cyber threats on social media. The personal data that users share on platforms like Facebook, Instagram, and Twitter including photographs, personal details, and contact information can easily be harvested by cybercriminals. This stolen information is often used for identity theft, leading to financial fraud, reputational damage, and emotional distress [37]. Identity theft through social media can result in unauthorized use of credit cards, fraudulent loans, or even impersonation in criminal activities, all of which create significant financial and psychological burdens on the victim. Furthermore, once a user's identity is stolen, it can take months, if not years, to fully recover their online presence and secure their accounts. As [38] notes, individuals may suffer long-term consequences from identity theft, including difficulty in securing future employment or loans, due to tarnished reputations or damaged credit [39].
2. **Emotional and Psychological Impact** Beyond the financial losses, cybersecurity threats also take an emotional and psychological toll on users. When a user's account is hacked or their personal data is leaked, they can experience feelings of violation, helplessness, and anxiety. Research indicates that victims of online fraud or identity theft often report feelings of mistrust and paranoia regarding the use of digital technologies thereafter [40]. The emotional trauma of being a cyber victim can lead to a reluctance to use social media or engage with online services, isolating individuals in a world that is increasingly dependent on digital interaction.

Additionally, the loss of control over one's personal data can erode confidence in the safety of digital communication, resulting in lower trust in social media platforms and technology providers. This emotional backlash against perceived security failures can reduce overall social media engagement, which is a primary source of social connection for many individuals [41].

Impact on Businesses

1. **Financial Losses** For businesses, cybersecurity threats on social media have the potential to cause significant financial damage. Companies that use social media for marketing, customer engagement, and brand development can find themselves vulnerable to phishing attacks, account hijacking, and data breaches [42]. Cybercriminals often target corporate social media accounts to spread malicious content, which can damage the brand’s reputation and lead to a loss of consumer trust [43]. Moreover, the financial costs of responding to a cyber-attack, including legal fees, compensation to affected customers, and investments in enhanced security measures, can be substantial. According to [41], businesses lose billions of dollars annually due to data breaches and cyber-attacks on social media platforms [44]. These costs are not limited to direct financial losses; they also encompass long-term expenses related to recovering a company's reputation, implementing better cybersecurity protocols, and compensating customers for any damages caused by the breach [3].
2. **Reputational Damage** Reputation is one of the most valuable assets for businesses, and cyber-attacks on social media can severely damage this. When customers lose confidence in a company’s ability to protect their personal data, they may switch to competitors, leading to decreased market share and revenue loss. A 2019 study found that 64% of consumers are less likely to purchase from a brand that has experienced a data breach [45]. For companies that rely heavily on social media for customer interaction, such as e-commerce or tech firms, the reputational damage from a cybersecurity incident can be particularly severe. The loss of trust can also extend to other stakeholders, including investors, partners, and employees, further compounding the negative effects of the breach[46].
3. **Legal and Regulatory Consequences** In addition to financial and reputational damages, businesses may face legal repercussions for failing to adequately protect customer data on social media. Regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the U.S. impose stringent requirements on companies to safeguard user information. Non-compliance with these laws can result in hefty fines and legal sanctions [47]. A study by [48] showed that organizations that fail to protect data on social media are increasingly being held accountable, not only through government fines but also through civil lawsuits filed by affected consumers [49]. These legal consequences further underscore the importance of implementing robust cybersecurity measures to avoid breaches that could expose a company to regulatory penalties and long-term legal challenges [50].

Impact on Society

1. **Erosion of Trust in Digital Platforms** At a societal level, the widespread occurrence of cybersecurity threats on social media contributes to a growing distrust of digital platforms. As more individuals and businesses fall victim to data breaches, phishing attacks, and identity theft, public confidence in the safety of online spaces declines [51]. This erosion of trust has significant implications for social cohesion and the future of digital innovation[52]. When users lose trust in social media platforms, they may be less willing to share information, engage with content, or use digital services that are critical to economic and social interaction. This hesitation can slow down the pace of digital transformation and limit the potential benefits of social media as a tool for education, commerce, and communication. Moreover, the erosion of trust in digital platforms can lead to increased polarization and the spread of misinformation, as individuals turn to less secure or reliable sources for information [53].

2. **Economic Impact** The economic consequences of cyber threats on social media are not limited to individual users and businesses; they also extend to society at large. Cybercrime on social platforms imposes substantial costs on the global economy, including the costs of cybersecurity measures, loss of productivity, and the impact on consumer confidence [54]. According to a report by the World Economic Forum, cybercrime could cost the global economy $10.5 trillion annually by 2025, a significant portion of which is attributed to social media attacks [55]. In addition, the economic impact of cyber threats on social media includes the costs of managing and preventing these threats. Governments and businesses are investing heavily in cybersecurity infrastructure, education, and regulation to mitigate the damage caused by cyber-attacks. These investments, while necessary, divert resources from other critical areas, such as innovation and public services [55].
3. **Social and Political Consequences** Cybersecurity threats on social media also have social and political implications. As platforms become conduits for misinformation, disinformation, and political manipulation, they pose threats to democratic processes and societal stability [54]. The use of social media for cyber-attacks, particularly during elections or political campaigns, can undermine public confidence in electoral systems and democratic governance [56]. For example, the spread of misinformation through social media has been linked to political polarization, social unrest, and even violence. Cybercriminals and state-sponsored actors often exploit social media vulnerabilities to disseminate false information, exacerbate existing divisions within society, and disrupt the functioning of democratic institutions [57]. Figure 4 below shows the impact in a detailed manner.

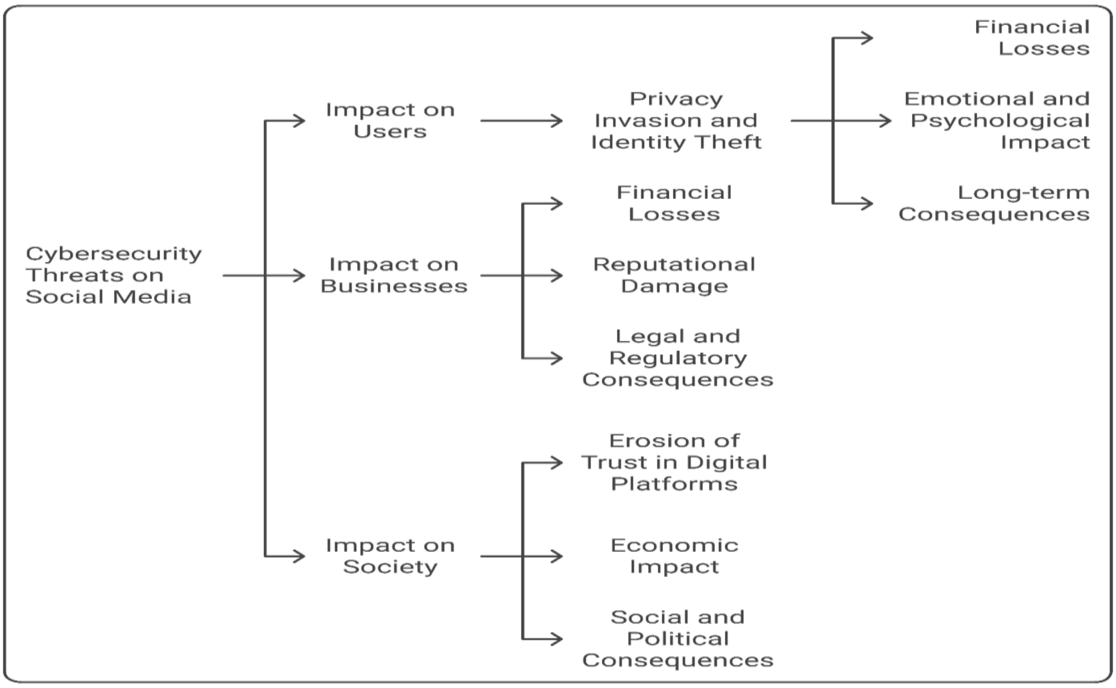
Cybersecurity Threats on Social Media
Impact on Users
Privacy Invasion and Identity Theft
Financial Losses
Emotional and Psychological Impact
Long-term Consequences
Impact on Businesses
Financial Losses
Reputational Damage
Legal and Regulatory Consequences
Impact on Society
Erosion of Trust in Digital Platforms
Economic Impact
Social and Political Consequences

Figure 4: cybersecurity threats impact users, businesses, and society

RQ3: What existing strategies for network protection and data integrity are currently implemented on social media platforms?

As social media platforms become critical communication and data-sharing tools for individuals and organizations, the need for robust network protection and data integrity strategies has grown exponentially. The increasing sophistication of cyber-attacks, coupled with the massive amounts of personal and corporate data shared on social platforms, has made cybersecurity a top priority for platform developers, businesses, and governments. To mitigate these threats, social media platforms and security experts have developed a variety of protection strategies. This section examines the existing network protection and data integrity measures employed by social media platforms, focusing

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

on encryption technologies, multi-factor authentication (MFA), anomaly detection, data anonymization, platform regulations, and user education [58].

1. Encryption Technologies

Encryption is one of the most widely adopted strategies for protecting network security and ensuring data integrity across social media platforms. Encryption transforms data into unreadable formats, making it difficult for unauthorized users to access or interpret sensitive information. End-to-end encryption (E2EE), for example, ensures that only the communicating users can decrypt and read the messages, effectively shielding data from third-party interception, including platform administrators. Platforms like WhatsApp and Facebook Messenger have integrated E2EE to protect users' conversations from being accessed by hackers or state actors [21]. While encryption offers a strong defense against data breaches, its use has sparked debates regarding privacy and law enforcement. Some governments argue that E2EE can also be exploited by criminals to carry out illegal activities under the cover of anonymity, thus posing a challenge to security agencies trying to prevent cybercrimes. Despite these concerns, encryption remains a cornerstone of data integrity strategies on social media, given its ability to safeguard both personal and corporate data from unauthorized access [21].

2. Multi-Factor Authentication (MFA)

Another crucial measure for securing network integrity on social media is the implementation of multi-factor authentication (MFA). MFA requires users to provide two or more verification factors to access their accounts, typically combining something the user knows (e.g., a password) with something they have (e.g., a smartphone) or something they are (e.g., fingerprint or facial recognition). By adding an extra layer of security, MFA significantly reduces the risk of unauthorized access to user accounts, even if passwords are compromised [59]. MFA is particularly effective in preventing account hijacking, a common cyber threat on social platforms. For instance, platforms like Instagram, Twitter, and LinkedIn now offer MFA options, allowing users to verify their identity using mobile authentication apps or text message codes. Research has shown that accounts protected by MFA are less likely to be breached compared to those relying solely on passwords [60]. However, the effectiveness of MFA is contingent upon user adoption, as many individuals fail to enable it despite the added security it provides.

3. Anomaly Detection and Behavioral Analytics

Social media platforms have increasingly incorporated anomaly detection and behavioral analytics to identify and respond to potential security breaches in real time. Anomaly detection systems monitor user behavior patterns and network traffic to identify deviations that may indicate a cyber threat, such as account compromise or data exfiltration. For example, Facebook uses machine learning algorithms to detect suspicious logins, such as those from unfamiliar locations or devices, and triggers security checks to confirm the user's identity before allowing access [61]. Behavioral analytics further enhance security by analyzing how users interact with the platform. Sudden changes in posting frequency, message content, or login times can be flagged as indicators of a compromised account. These systems allow platforms to detect threats like account hijacking, phishing, and malware distribution early and mitigate the risks before they cause significant damage. Additionally, some platforms offer users the ability to review and confirm unusual account activity, empowering them to take control of their security [62]. Despite the effectiveness of anomaly detection, there are challenges related to balancing user privacy and data monitoring. Overly intrusive monitoring can raise concerns about privacy violations, especially if users feel they are being constantly watched by the platform. As a result, platforms must strike a balance between protecting users and respecting their privacy by being transparent about how their data is monitored and used.

4. Data Anonymization and Tokenization

Data anonymization and tokenization are vital strategies employed to protect sensitive information on social media platforms. These techniques ensure that even if data is compromised, it cannot be traced back to its original owner. Anonymization removes personally identifiable information (PII) from datasets, allowing platforms to share or analyze data without exposing users' identities. Tokenization replaces sensitive data with non-sensitive equivalents, which can be used without exposing real data, thus protecting users’ personal information from unauthorized access [63]. Platforms like Google and Facebook implement these techniques to safeguard user data when conducting analytics or sharing information with third-party advertisers. Anonymized data allows platforms to provide targeted services without compromising users’ privacy, making it a critical component of data protection strategies. However, anonymization and tokenization are not foolproof; sophisticated attackers may still be able to re-identify users by correlating anonymized data with external datasets [64].

5. Platform Policies and Regulations

Social media platforms have increasingly introduced security policies and regulations designed to protect users from cyber threats and ensure data integrity. These policies often include guidelines for data collection, storage, and sharing, as well as protocols for responding to data breaches. Regulations such as the General Data Protection Regulation (GDPR) in the European Union have prompted social media platforms to enhance their data protection measures, requiring stricter consent protocols and giving users more control over their data [65].

Platform-specific policies have also been developed to address the unique security challenges posed by social media. For instance, Twitter has implemented strict measures to detect and remove malicious bots, which are often used to distribute spam or phishing links. Facebook has introduced transparency measures to combat misinformation and protect user data, including restricting third-party access to personal information without explicit user consent [66]. Compliance with global regulations like GDPR and the California Consumer Privacy Act (CCPA) has also forced social media companies to reevaluate how they handle user data. While these regulations have strengthened data protection, platforms continue to face challenges in enforcing their policies effectively across regions with varying legal frameworks [67].

6. User Education and Awareness

One of the most critical, yet often overlooked, components of network protection and data integrity is user education. Even the most advanced security measures can be rendered ineffective if users are unaware of the risks or do not take appropriate actions to protect their accounts. Social media platforms have responded to this challenge by launching security awareness campaigns that educate users on best practices, such as creating strong passwords, recognizing phishing attempts, and enabling MFA [67]. For example, Facebook’s security center provides users with tips on safeguarding their accounts, while Twitter regularly prompts users to review their privacy settings and security preferences. Educational efforts are particularly important in combating phishing, as users often fall victim to scams due to a lack of awareness about the risks involved. Research suggests that when users are informed about the dangers of phishing and other cyber threats, they are more likely to adopt secure practices, such as using MFA and avoiding suspicious links [68]. However, user education remains an ongoing challenge. Despite platforms’ efforts, many users still exhibit risky behaviors, such as reusing passwords or sharing personal information publicly. As a result, continued efforts are necessary to improve user engagement with security best practices and to foster a culture of cybersecurity on social media [69].

7. AI-based security systems

have emerged as a promising solution for real-time threat detection and mitigation. Studies by *[70]* show that AI-powered algorithms can identify suspicious activities and potential cyber-attacks with high accuracy, allowing for faster response times. However, the same study highlights challenges in implementing AI at scale, particularly in terms of computational costs and data privacy concerns.

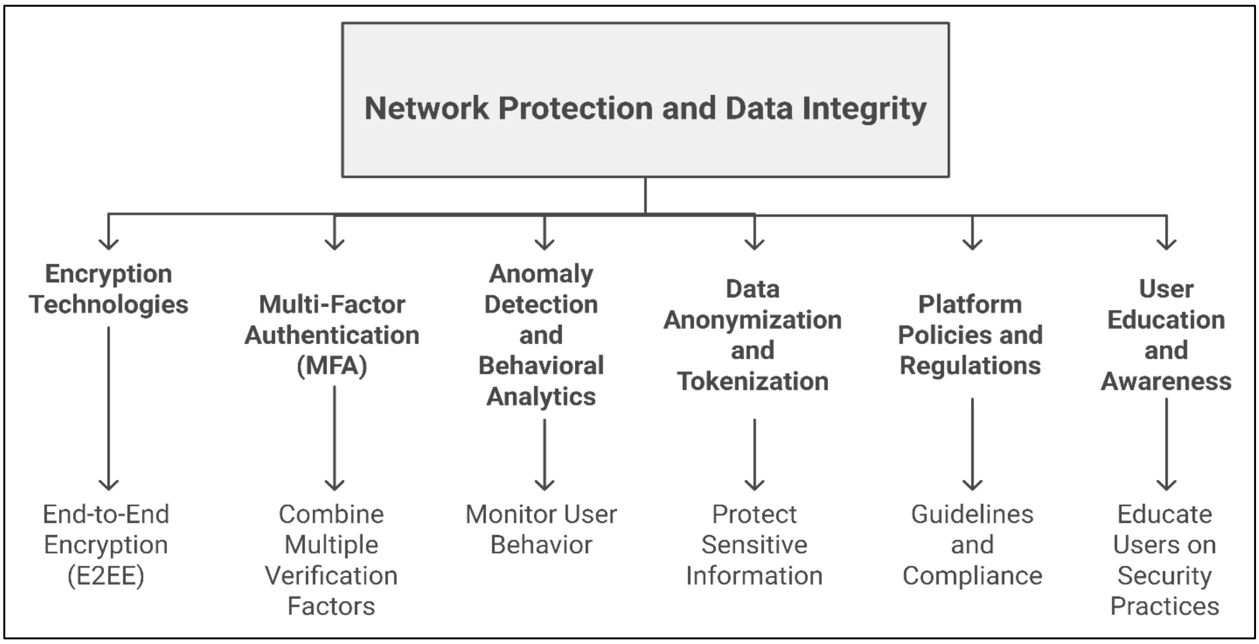
Network Protection and Data Integrity
Encryption Technologies
Multi-Factor Authentication (MFA)
Anomaly Detection and Behavioral Analytics
Data Anonymization and Tokenization
Platform Policies and Regulations
User Education and Awareness
End-to-End Encryption (E2EE)
Combine Multiple Verification Factors
Monitor User Behavior
Protect Sensitive Information
Guidelines and Compliance
Educate Users on Security Practices

Figure 5: Strategies for network protection and data integrity

RQ4: What integrated framework can be proposed to combat cybersecurity threats on social media?

As social media platforms evolve into critical tools for personal, professional, and business communications, the cybersecurity challenges associated with them continue to grow. While individual solutions such as encryption, firewalls, and multi-factor authentication (MFA) have made significant strides in protecting users, an integrated approach is essential to fully combat the multifaceted threats that plague social media ecosystems. This section outlines a comprehensive framework aimed at mitigating cybersecurity risks on social media by blending technical measures with behavioral, regulatory, and collaborative strategies [71].

1. User Education and Awareness

User behavior is often the weakest link in cybersecurity on social media platforms. Many users are unaware of the threats they face, such as phishing, identity theft, and malware. According to research by [72], over 40% of social media users fail to implement basic security measures, such as strong passwords or enabling MFA [73]. Therefore, a core component of the proposed framework involves improving user education and awareness about these risks.

Awareness Campaigns: Social media platforms can implement continuous security awareness campaigns aimed at educating users about the importance of privacy settings, recognizing phishing attempts, and avoiding suspicious links. These campaigns should be interactive, incorporating videos, quizzes, and scenario-based training to engage users effectively [74]. For example, platforms like Facebook and Twitter could provide real-time alerts to users when they engage in risky behaviors, such as clicking on unverified links.

Security Prompts and Nudges: To further promote safe behavior, platforms could employ “nudges” subtle prompts that encourage users to take actions like updating passwords regularly or enabling MFA. Research by [75] found that timely security prompts can reduce account hijacking incidents by up to 25%. By integrating these nudges into the user experience, platforms can make security practices habitual for users.

2. Technical Solutions: Strengthening Security Architecture

The technical backbone of social media platforms plays a crucial role in protecting users from cyber threats. The proposed framework includes several advanced security measures that address both current and emerging threats.

A. Encryption: Encryption remains a foundational technology for securing communications and data on social media platforms. End-to-end encryption (E2EE) ensures that messages are encrypted from the sender to the receiver, preventing unauthorized parties, including the platform itself, from accessing the content. This technique is already used by platforms like WhatsApp but should be extended to other social media platforms, including Facebook Messenger and Instagram, where private communications are frequent **[76]**.

B. AI-Based Threat Detection: Artificial intelligence (AI) has shown promise in detecting cybersecurity threats before they escalate. AI systems can monitor user behavior, network traffic, and interaction patterns to identify anomalies indicative of phishing, malware distribution, or account hijacking [77]. Machine learning algorithms, for instance, can be trained to detect unusual login locations or rapid, automated activity consistent with botnets. Social media platforms like Twitter have started deploying AI to combat spam and malicious activity, but this needs to be integrated across all major platforms in a unified manner.

C. Multi-Factor Authentication (MFA): MFA adds a critical layer of security by requiring users to verify their identity through more than one authentication method, such as a password and a one-time code sent to their mobile phone. Studies show that MFA can reduce the likelihood of account compromise by over 99% [78]. However, widespread adoption remains an issue, with many users either unaware of its benefits or finding it too inconvenient. The proposed framework emphasizes the need for platforms to encourage and, in some cases, mandate MFA for sensitive activities like accessing financial data or changing account settings.

3. Platform Policies and Regulations: Governance and Compliance

Social media platforms are not just passive tools; they are responsible for the security of their users. Thus, robust platform policies and regulatory compliance are essential components of the integrated framework.

A. Data Protection Policies: Social media platforms need to adhere strictly to global data protection regulations such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States [79]. These regulations mandate that platforms protect users' personal data, provide transparency in data usage, and give users control over their information. However, adherence to these regulations is inconsistent across platforms. The framework proposes more rigorous enforcement of data protection policies across all platforms, with heavy penalties for non-compliance.

Automated Privacy Audits: Platforms should conduct periodic privacy audits, both internally and through third-party organizations, to ensure that user data is adequately protected. Such audits would assess the platform's data storage practices, encryption standards, and compliance with privacy regulations [80]. Audits should also examine the effectiveness of platform responses to data breaches, ensuring that users are notified promptly and given tools to mitigate damage.

Content Moderation Policies: A growing concern is the role of social media platforms in moderating harmful content, which is often linked to cyber-attacks. For example, fake news or misinformation can be used to manipulate users into clicking malicious links or engaging in unsafe behaviors [81]. The framework recommends the use of AI-based content moderation systems to quickly identify and remove malicious content, while ensuring transparency in how content moderation decisions are made.

4. Collaborative Efforts: Fostering Partnerships in Cybersecurity

No single entity can tackle social media cybersecurity alone. The proposed framework advocates for greater collaboration between social media platforms, government agencies, and users.

Information Sharing Between Platforms: One of the most effective ways to prevent the spread of cyber threats is through information sharing. For example, when one platform detects a phishing campaign, it should alert other platforms to prevent the same attack from occurring elsewhere [82]. A central clearinghouse could be established where platforms, cybersecurity firms, and government agencies share data on emerging threats in real time. This would enable quicker identification and containment of cyber-attacks across multiple platforms.

Public-Private Partnerships: Governments and private organizations must collaborate to develop industry standards and best practices for social media cybersecurity. Government agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States can provide resources and guidance to platforms on best practices for cybersecurity. Moreover, the government can support platforms by imposing regulations that compel them to invest in advanced security technologies and user safety features [82].

User Accountability and Cooperation: Users themselves must take responsibility for their online safety by adhering to best practices such as using MFA, creating strong passwords, and being vigilant about suspicious content. Platforms can facilitate this by offering incentives for users who demonstrate proactive cybersecurity practices. For instance, Instagram or Facebook could introduce a "Verified Secure" badge for users who adopt enhanced security measures, encouraging others to follow suit [83].

5. **Incident Response and Recovery: Minimizing Damage Post-Attack**

Even the best cybersecurity strategies cannot prevent every attack. Therefore, the integrated framework places significant emphasis on effective incident response and recovery mechanisms.

Crisis Communication: In the event of a data breach or cyber-attack, it is crucial for platforms to communicate clearly and promptly with affected users. Platforms should have pre-established crisis communication protocols, ensuring that users are notified within hours of a breach, as mandated by GDPR [84]. These notifications should provide users with detailed steps on how to secure their accounts, such as changing passwords, enabling MFA, or freezing financial accounts linked to their social media profile.

Automated Response Systems: Platforms should invest in automated incident response systems that can immediately detect and contain cyber-attacks. For example, if an account is compromised and starts sending out phishing messages, an automated system could temporarily lock the account, preventing the attack from spreading further [85].

Recovery and Compensation: Finally, social media platforms must provide users with tools to recover from an attack, such as easy access to account recovery options and financial compensation in cases where platform negligence contributed to the breach. Platforms should also collaborate with financial institutions to offer identity theft protection services to users affected by major data breaches [86]. Table summarizes the integrated framework for combating social media cybersecurity threats, detailing each component, its strategies, and expected outcomes.

Table 6: Summary of the integrated framework for combating social media cybersecurity threats

Framework Component	Description	Key Strategies	Expected Outcomes
User Education and Awareness	Focuses on improving user knowledge about cybersecurity threats on social media.	- Continuous security awareness campaigns - Interactive training materials - Timely security prompts and nudges to encourage safe behavior.	- Increased user awareness and understanding of security risks - Reduction in risky behaviors such as sharing passwords.
Technical Solutions	Involves enhancing the security architecture of social media platforms through advanced technologies.	- Implementation of end-to-end encryption - AI-based threat detection systems - Mandatory multi-factor authentication (MFA).	- Improved protection against unauthorized access and data breaches - Quick identification and response to potential threats.
Platform Policies and Regulations	Encompasses the need for social media platforms to adopt strict policies and comply with	- Adherence to global data protection laws (GDPR, CCPA) - Conducting automated privacy audits	- Enhanced user trust and data security - Proactive management of user data and swift

	data protection regulations.	- Strengthening content moderation policies.	action against harmful content.
Collaborative Efforts	Emphasizes the importance of partnerships between social media platforms, governments, and users for comprehensive cybersecurity.	- Information sharing between platforms - Public-private partnerships to develop best practices - User accountability initiatives.	- Faster identification and containment of cyber threats - Greater collective cybersecurity resilience.
Incident Response and Recovery	Focuses on establishing effective protocols for responding to and recovering from cyber-attacks.	- Clear crisis communication strategies - Implementation of automated incident response systems - Recovery tools and compensation for affected users.	- Minimization of damage from cyber incidents - Swift recovery processes to restore user trust and platform integrity.

5.Discussion

The findings of this research underscore the critical need for robust network protection strategies tailored to the unique challenges posed by social media platforms. The analysis reveals that cybersecurity threats on social media, including identity theft and misinformation, have far-reaching consequences for users, businesses, and society [87]. This study's identification of prevalent threats aligns with previous literature that emphasizes the vulnerabilities associated with digital communication channels [88].

Furthermore, the proposed integrated framework, which encompasses user education, technical solutions, platform policies, and collaborative efforts, reflects the multifaceted nature of the challenges at hand. As indicated in the literature, user awareness and education are pivotal in mitigating risks, as many users remain uninformed about potential threats and best practices for online safety [89]. This aligns with research highlighting the psychological aspects of cybersecurity, where user behavior significantly influences vulnerability levels [90].

The discussion also points to the importance of platform policies and regulations in enforcing security measures. As social media companies play a crucial role in safeguarding user data, their commitment to implementing comprehensive security policies and adhering to data protection regulations is paramount [91]. The collaborative approach outlined in the framework suggests that a partnership between users, platform providers, and law enforcement could enhance the effectiveness of cybersecurity initiatives.

Finally, the author suggest that the future research direction can be done by employing an empirical evaluation of the proposed framework against existing strategies indicates a promising direction for future research. As cyber threats continue to evolve, ongoing monitoring and adaptation of security measures will be essential for maintaining the integrity of social media platforms. This study contributes significantly to the growing body of knowledge on social media cybersecurity, offering practical recommendations for users and organizations aiming to enhance their security posture.

6.Limitations

The main limitation of this research is its reliance on secondary data. Although the systematic review provides comprehensive insights, primary data collection through surveys or interviews with social media security experts could offer additional perspectives. Future research could incorporate mixed methods, combining qualitative and quantitative approaches to enhance the framework’s empirical validation.

7.Conclusion

This research aims to contribute to the ongoing effort to ensure that social media remains a secure and beneficial tool for communication and information sharing. In conclusion, this research adopts a systematic literature review and thematic analysis to develop an integrated framework for protecting social media networks from cybersecurity threats. By combining technical innovations and non-technical strategies, this framework offers a holistic approach to safeguarding network integrity and user data on social media platforms.

REFERENCES:

[1] D. Weissenbacher et al., "Overview of the seventh social media mining for health applications (# SMM4H) shared tasks at COLING 2022," in Proceedings of the seventh workshop on social media mining for health applications, workshop & shared task, 2022, pp. 221-241.

[2] T. R. Soomro and M. Hussain, "Social media-related cybercrimes and techniques for their prevention," Applied Computer Systems, vol. 24, no. 1, pp. 9-17, 2019.

[3] W. He, "A review of social media security risks and mitigation techniques," Journal of Systems and Information Technology, vol. 14, no. 2, pp. 171-180, 2012.

[4] A. Aktayeva et al., "Cybersecurity Risk Assessments within Critical Infrastructure Social Networks," Data, vol. 8, no. 10, p. 156, 2023.

[5] M. Mijwil and M. Aljanabi, "Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 65-70, 2023.

[6] S. Konyeha, "Exploring cybersecurity threats in digital marketing," NIPES-Journal of Science and Technology Research, vol. 2, no. 3, 2020.

[7] A. Damaraju, "Social Media as a Cyber Threat Vector: Trends and Preventive Measures," Revista Espanola de Documentacion Cientifica, vol. 14, no. 1, pp. 95-112, 2020.

[8] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," Frontiers in Computer Science, vol. 3, p. 563060, 2021.

[9] B. B. Gupta, N. A. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," Telecommunication Systems, vol. 67, pp. 247-267, 2018.

[10] M. N. Banu and S. M. Banu, "A comprehensive study of phishing attacks," International Journal of Computer Science and Information Technologies, vol. 4, no. 6, pp. 783-786, 2013.

[11] M. Nadeem, S. W. Zahra, M. N. Abbasi, A. Arshad, S. Riaz, and W. Ahmed, "Phishing attack, its detections and prevention techniques," International Journal of Wireless Security and Networks, vol. 1, no. 2, pp. 13-25p, 2023.

[12] A. Bovet and H. A. Makse, "Influence of fake news in Twitter during the 2016 US presidential election," Nature communications, vol. 10, no. 1, p. 7, 2019.

[13] A. Booth, M.-S. James, M. Clowes, and A. Sutton, "Systematic approaches to a successful literature review," 2021.

[14] A. Pollock and E. Berge, "How to do a systematic review," International Journal of Stroke, vol. 13, no. 2, pp. 138-156, 2018.

[15] R. Ormston, L. Spencer, M. Barnard, and D. Snape, "The foundations of qualitative research," Qualitative research practice: A guide for social science students and researchers, vol. 2, no. 7, pp. 52-55, 2014.

[16] V. Braun and V. Clarke, Thematic analysis. American Psychological Association, 2012.

[17] E. E. Henriksen, "Big data, microtargeting, and governmentality in cyber-times. The case of the Facebook-Cambridge Analytica data scandal," 2019.

[18] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: threats and solutions," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019-2036, 2014.

[19] A. Al-Charchafchi, S. Manickam, and Z. N. Alqattan, "Threats against information privacy and security in social networks: A review," in Advances in Cyber Security: First International

Conference, ACeS 2019, Penang, Malaysia, July 30–August 1, 2019, Revised Selected Papers 1, 2020: Springer, pp. 358-372.

[20] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," Information sciences, vol. 421, pp. 43-69, 2017.

[21] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex & Intelligent Systems, vol. 7, no. 5, pp. 2157-2177, 2021.

[22] A. Hamid, M. Alam, H. Sheherin, and A.-S. K. Pathan, "Cyber security concerns in social networking service," International Journal of Communication Networks and Information Security, vol. 12, no. 2, pp. 198-212, 2020.

[23] L. Caviglione et al., "Tight arms race: Overview of current malware threats and trends in their detection," IEEE Access, vol. 9, pp. 5371-5396, 2020.

[24] M. F. Ab Razak, N. B. Anuar, R. Salleh, and A. Firdaus, "The rise of "malware": Bibliometric analysis of malware study," Journal of Network and Computer Applications, vol. 75, pp. 58-76, 2016.

[25] R. Kaur, S. Singh, and H. Kumar, "Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches," Journal of Network and Computer Applications, vol. 112, pp. 53-88, 2018.

[26] S. Alam and K. El-Khatib, "Phishing susceptibility detection through social media analytics," in Proceedings of the 9th International Conference on Security of Information and Networks, 2016, pp. 61-64.

[27] M. Singh, C. Verma, and P. Juneja, "Social media security threats investigation and mitigation methods: A preliminary review," in Journal of Physics: Conference Series, 2020, vol. 1706, no. 1: IOP Publishing, p. 012142.

[28] R. Chen, D. J. Kim, and H. R. Rao, "A study of social networking site use from a three-pronged security and privacy threat assessment perspective," Information & Management, vol. 58, no. 5, p. 103486, 2021.

[29] R. Alguliyev, R. Aliguliyev, and F. Yusifov, "Role of social networks in E-government: Risks and security threats," Online Journal of Communication and Media Technologies, vol. 8, no. 4, pp. 363-376, 2018.

[30] S. Irshad and T. R. Soomro, "Identity theft and social media," International Journal of Computer Science and Network Security, vol. 18, no. 1, pp. 43-55, 2018.

[31] A. R. Ilzan, R. F. B. Oktaviani, F. M. Yusuf, D. J. Wegman, and N. Y. Imtiyaz, "Understanding the phenomenon and risks of identity theft and fraud on social media," Asia Pacific Journal of Information System and Digital Transformation, vol. 1, no. 1, pp. 23-32, 2023.

[32] M. Silic and A. Back, "The dark side of social networking sites: Understanding phishing risks," Computers in Human Behavior, vol. 60, pp. 35-43, 2016.

[33] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A theoretical review of social media usage by cyber-criminals," in 2017 International Conference on Computer Communication and Informatics (ICCCI), 2017: IEEE, pp. 1-6.

[34] M. Apte, G. K. Palshikar, and S. Baskaran, "Frauds in online social networks: A review," Social networks and surveillance for society, pp. 1-18, 2019.

[35] I. N. Sunarta, "Juridical Review of the Crime of Using Photos and Images Legal Hijacking of Other People's Social Media Accounts Number 19 of 2016 concerning Information and Electronic Transactions," in Proceeding International Conference Faculty of Law, 2021, vol. 1, no. 1, pp. 203-216.

[36] H. Almarabeh and A. Sulieman, "The impact of cyber threats on social networking sites," International Journal of Advanced Research in Computer Science, vol. 10, no. 2, 2019.

[37] N. Z. Khidzir, A. R. Ismail, K. A. M. Daud, M. S. Afendi, A. Ghani, and M. A. H. Ibrahim, "Critical cybersecurity risk factors in digital social media: Analysis of information security requirements," Lecture Notes on Information Theory Vol, vol. 4, no. 1, pp. 18-24, 2016.

[38] N. F. Khan, N. Ikram, H. Murtaza, and M. A. Asadi, "Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach," Kybernetes, vol. 52, no. 1, pp. 401-421, 2023.

[39] M. Schiappa, G. Chantry, and I. Garibay, "Cyber security in a complex community: A social media analysis on common vulnerabilities and exposures," in 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), 2019: IEEE, pp. 13-20.

[40] T. B. Herath, P. Khanna, and M. Ahmed, "Cybersecurity practices for social media users: a systematic literature review," Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 1-18, 2022.

[41] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," Computer Systems Science & Engineering, vol. 40, no. 3, 2022.

[42] M. Mathur, "Where is the security blanket? Developing social media marketing capability as a shield from perceived cybersecurity risk," Journal of Promotion Management, vol. 25, no. 2, pp. 200-224, 2019.

[43] R. Atri, S. Prabhu, and J. Cherady, "Study of cyber security threats to online social networks," in AIP Conference Proceedings, 2023, vol. 2736, no. 1: AIP Publishing.

[44] K. Rajasekharaiah, C. S. Dule, and E. Sudarshan, "Cyber security challenges and its emerging trends on latest technologies," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 981, no. 2: IOP Publishing, p. 022062.

[45] F. A. Maskuria, M. Z. Othmanb, I. Osmana, S. Kassima, and N. Abd Razakc, "The Impact of Social Media Usage on the Organisation's Reputation Risk through its Cybersecurity," International Journal of Academic Research in Business and Social Sciences, vol. 13, no. 2, 2023.

[46] S. Perera, X. Jin, A. Maurushat, and D.-G. J. Opoku, "Factors affecting reputational damage to organisations due to cyberattacks," in Informatics, 2022, vol. 9, no. 1: MDPI, p. 28.

[47] M. T. Nguyen and M. Q. Tran, "Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices," International Journal of Intelligent Automation and Computing, vol. 6, no. 5, pp. 1-12, 2023.

[48] D. S. Wall, "Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing," Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017), 2017.

[49] A. K. Tyagi, K. Naithani, and S. Tiwari, "Security and Possible Threats in Today's Online Social Networking Platforms," Online Social Networks in Business Frameworks, pp. 159-199, 2024.

[50] M. Yar, "A failure to regulate? The demands and dilemmas of tackling illegal content and behaviour on social media," International Journal of Cybersecurity Intelligence & Cybercrime, vol. 1, no. 1, pp. 5-20, 2018.

[51] M. Thakur, "Cyber security threats and countermeasures in digital age," Journal of Applied Science and Education (JASE), vol. 4, no. 1, pp. 1-20, 2024.

[52] M. L. Miller and C. Vaccari, "Digital threats to democracy: Comparative lessons and possible remedies," The International Journal of Press/Politics, vol. 25, no. 3, pp. 333-356, 2020.

[53] D. V. Gioe, M. S. Goodman, and A. Wanless, "Rebalancing cybersecurity imperatives: patching the social layer," Journal of Cyber Policy, vol. 4, no. 1, pp. 117-137, 2019.

[54] E. Zhuravskaya, M. Petrova, and R. Enikolopov, "Political effects of the internet and social media," Annual review of economics, vol. 12, no. 1, pp. 415-438, 2020.

[55] C. M. Pulido, G. Redondo-Sama, T. Sordé-Martí, and R. Flecha, "Social impact in social media: A new method to evaluate the social impact of research," PloS one, vol. 13, no. 8, p. e0203117, 2018.

[56] L. Bode, "Gateway political behaviors: The frequency and consequences of low-cost political engagement on social media," Social Media+ Society, vol. 3, no. 4, p. 2056305117743349, 2017.

[57] R. Effing, J. Van Hillegersberg, and T. Huibers, "Social media and political participation: are Facebook, Twitter and YouTube democratizing our political systems?," in Electronic

Participation: Third IFIP WG 8.5 International Conference, ePart 2011, Delft, The Netherlands, August 29–September 1, 2011. Proceedings 3, 2011: Springer, pp. 25-35.

[58] M. S. Mushtaq, M. Y. Mushtaq, M. W. Iqbal, and S. A. Hussain, "Security, integrity, and privacy of cloud computing and big data," in Security and privacy trends in cloud computing and big data: CRC Press, 2022, pp. 19-51.

[59] H. Mehraj et al., "Protection motivation theory using multi-factor authentication for providing security over social networking sites," Pattern Recognition Letters, vol. 152, pp. 218-224, 2021.

[60] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi, and M. D. Alshehri, "A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles," Sensors, vol. 21, no. 18, p. 6018, 2021.

[61] M. S. Rahman, S. Halder, M. A. Uddin, and U. K. Acharjee, "An efficient hybrid system for anomaly detection in social networks," Cybersecurity, vol. 4, no. 1, p. 10, 2021.

[62] N. E. H. Ben Chaabene, A. Bouzeghoub, R. Guetari, and H. H. B. Ghezala, "Deep learning methods for anomalies detection in social networks using multidimensional networks and multimodal data: A survey," Multimedia systems, vol. 28, no. 6, pp. 2133-2143, 2022.

[63] S. Patil, S. Joshi, and D. Patil, "Enhanced privacy preservation using anonymization in IoT-enabled smart homes," in Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 1, 2020: Springer, pp. 439-454.

[64] Y. Şahin and İ. Dogru, "An enterprise data privacy governance model: security-centric multi-model data anonymization," International Journal of Engineering Research and Development, vol. 15, no. 2, pp. 574-583, 2023.

[65] T. Flew, F. Martin, and N. Suzor, "Internet regulation as media policy: Rethinking the question of digital communication platform governance," Journal of Digital Media & Policy, vol. 10, no. 1, pp. 33-50, 2019.

[66] S. Ashwini, "Social Media Platform Regulation in India–A Special Reference to The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," Perspectives on Platform Regulation, pp. 215-232, 2021.

[67] J. A. Pater, M. K. Kim, E. D. Mynatt, and C. Fiesler, "Characterizations of online harassment: Comparing policies across social media platforms," in Proceedings of the 2016 ACM International Conference on Supporting Group Work, 2016, pp. 369-374.

[68] R. J. Kadhim, "THE ROLE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN INCREASING AWARENESS AND EDUCATING USERS THROUGH ELECTRONIC SOCIAL NETWORKS (SURVEY STUDY ON A SAMPLE OF THI QAR UNIVERSITY STUDENTS)," Conhecimento & Diversidade, vol. 16, no. 41, pp. 507-525, 2024.

[69] Z. Xie, D. K. Chiu, and K. K. Ho, "The role of social media as aids for accounting education and knowledge sharing: learning effectiveness and knowledge management perspectives in mainland China," Journal of the Knowledge Economy, vol. 15, no. 1, pp. 2628-2655, 2024.

[70] I. H. Sarker, "Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," Security and Privacy, vol. 6, no. 5, p. e295, 2023.

[71] E. A. Sari, R. A. D. Setiawan, and U. Jandevi, "Social Media in Electoral Communication: A Case Study of Strategic Initiatives by Bantul Election Commission for the 2024 Elections," CHANNEL: Jurnal Komunikasi, vol. 11, no. 2, pp. 137-143, 2023.

[72] K. M. Abuali, L. Nissirat, and A. Al-Samawi, "Intrusion Detection Techniques in Social Media Cloud: Review and Future Directions," Wireless Communications and Mobile Computing, vol. 2023, no. 1, p. 6687023, 2023.

[73] F. Al-Turjman and R. Salama, "Cyber security in mobile social networks," in Security in IoT Social Networks: Elsevier, 2021, pp. 55-81.

[74] P. Essama-Mekongo, "Countering Hate Speech on Social Media in Cameroon: Legal and Technical Measures," Beijing Law Review, vol. 15, no. 03, pp. 1104-1126, 2024.

[75] M. Shahbazi and D. Bunker, "Social media trust: Fighting misinformation in the time of crisis," International Journal of Information Management, vol. 77, p. 102780, 2024.

[76] S. Yadav and N. Tiwari, "Privacy preserving data sharing method for social media platforms," PloS one, vol. 18, no. 1, p. e0280182, 2023.

[77] N. Khurana, S. Mittal, A. Piplai, and A. Joshi, "Preventing poisoning attacks on AI based threat intelligence systems," in 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP), 2019: IEEE, pp. 1-6.

[78] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptography, vol. 2, no. 1, p. 1, 2018.

[79] B. Custers, F. Dechesne, A. M. Sears, T. Tani, and S. Van der Hof, "A comparison of data protection legislation and policies across the EU," Computer Law & Security Review, vol. 34, no. 2, pp. 234-243, 2018.

[80] T. Libert, "An automated approach to auditing disclosure of third-party data collection in website privacy policies," in Proceedings of the 2018 World Wide Web Conference, 2018, pp. 207-216.

[81] S. Myers West, "Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms," New Media & Society, vol. 20, no. 11, pp. 4366-4383, 2018.

[82] L. Yan, X. Yan, Y. Tan, and S. X. Sun, "Shared minds: How patients use collaborative information sharing via social media platforms," Production and Operations Management, vol. 28, no. 1, pp. 9-26, 2019.

[83] F. Saurwein and C. Spencer-Smith, "Combating disinformation on social media: Multilevel governance and distributed accountability in Europe," Digital journalism, vol. 8, no. 6, pp. 820-841, 2020.

[84] Y. Cheng, "How social media is changing crisis communication strategies: Evidence from the updated literature," Journal of contingencies and crisis management, vol. 26, no. 1, pp. 58-68, 2018.

[85] L. Dwarakanath, A. Kamsin, R. A. Rasheed, A. Anandhan, and L. Shuib, "Automated machine learning approaches for emergency response and coordination via social media in the aftermath of a disaster: A review," Ieee Access, vol. 9, pp. 68917-68931, 2021.

[86] J. Hogreve, N. Bilstein, and K. Hoerner, "Service recovery on stage: Effects of social media recovery on virtually present others," Journal of Service Research, vol. 22, no. 4, pp. 421-439, 2019.

[87] "Speak - The language learning app that gets you speaking," ed.

[88] R. Das and M. Patel, "Cyber security for social networking sites: Issues, challenges and solutions," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 5, no. 4,833-838, 2017.

[89] S. K. Kapoor, K. Sankhla, P. Agarwal, and S. K. Rathi, "Security and Threat in Online Social Networking," Online Social Networks in Business Frameworks, pp. 449-477, 2024.

[90] E. Van der Walt, J. H. Eloff, and J. Grobler, "Cyber-security: Identity deception detection on social media platforms," Computers & Security, vol. 78, pp. 76-89, 2018.

[91] A. B. Shaheen, "Fake Profiles in Online Social Networks: Implications for Privacy and Cybersecurity in a Globalized World," 2020.