TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

# Cybersecurity Challenges and Risks in Social Networking Platforms

Vishal Vikram Singh[1], Bineet Kumar Gupta[2], and Satya Bhushan Verma[3]

[1, 2]Shri Ramswaroop Memorial University, Barabanki, India 225003
[3] Department of Computer Science and Engineering, University of Lucknow, Lucknow
vishal29.singh@gmail.com[1], bkguptacs@gmail.com[2], satyabverma1@gmail.com[3]

**KEYWORDS**

*Cybersecurity, Social Network Security, Confidentiality, Integrity, Vulnerabilities.*

**ABSTRACT**

*Cybersecurity has become a critical challenge in the digital era, requiring focused attention from researchers, practitioners, and policymakers to protect the confidentiality, integrity, and availability of information systems. With social networks evolving into influential platforms for real-time communication, users gain unprecedented access to news, opinions, and multimedia content. Yet, this openness also creates significant vulnerabilities, making social media a prime target for threats such as identity theft, data breaches, misinformation campaigns, and behavioral profiling. This paper explores the intersection of cybersecurity and social networking, emphasizing risks arising from user-generated content, metadata exposure, and insufficient privacy safeguards. It further analyzes existing security measures, identifies gaps in user awareness, and proposes strategic frameworks to strengthen resilience against emerging threats. By cultivating a culture of cybersecurity and adopting robust protective mechanisms, stakeholders can foster safer digital interactions and maintain the credibility of social platforms.*

## 1. Introduction

Today, social networks have evolved into advanced platforms for information dissemination, providing users with unrestricted access to news, updates, and diverse viewpoints [1]. Their growing popularity is driven by changing user behavior, technological advancements, and shifting societal norms [2]. These platforms operate through a novel network architecture that connects users directly to centralized service providers, enabling seamless communication, data storage, and interaction [3].

In this interconnected digital ecosystem, social applications act as essential hubs, all linked to central service providers that form the backbone of the infrastructure. Users from around the world access these platforms to share content, collaborate, and communicate in real time, generating continuous streams of digital traffic [4]. This flow includes messages, multimedia, and other information, creating a dynamic network of online relationships. Central service providers play a crucial role in managing system performance and stability, ensuring a reliable and seamless user experience within this complex and vibrant digital environment.

### A. Impact Assessment of Cyber Threats on Social Networking Services

As the number of users and organizations engaging with social network platforms continues to rise,

**Corresponding Author: Vishal Vikram Singh,** Shri Ramswaroop Memorial University, Barabanki, India 225003.
**Email:** vishal29.singh@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

so too does the presence of malicious actors. These attackers exploit vulnerabilities in the interconnected systems of various social applications, which rely on a centralized infrastructure governed by specialized algorithms. This centralized system is responsible for overseeing and securing the services offered by multiple social platforms.

On average, social network applications face three primary types of cyberattacks:

Sybil Attacks – 70%

Botnet Attacks – 18%

Anomaly Attacks – 12%

Let's consider a model of the social network comprising external and internal architectural layers (as illustrated in Fig. 1). Internally, organizations provide services to users through social applications, all connected by switches and routers. While many users are genuine, some are adversaries seeking to compromise user data.

Within this internal network, two prominent attack vectors emerge:

Sybil attackers impersonate multiple identities to infiltrate user profiles and inject malicious traffic.

Spammers distribute harmful messages across the network to collect sensitive information.

Externally, additional threats aim to destabilize the network, including:

- Distributed Denial-of-Service (DDoS) attacks
- Malicious traffic injection
- Attempts to breach overall security mechanisms

The primary goal in defending this ecosystem is to accurately differentiate legitimate users from fraudulent entities, safeguarding trust and privacy within the social networking environment.

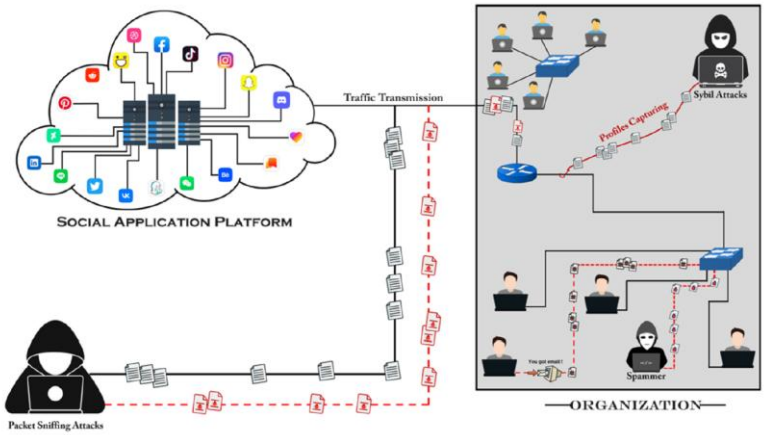


Figure 1: External and Internal attack vectors in the social networks

## 2. Literature Review

Abusive behaviors continue to plague social platforms, with Instagram frequently highlighted in recent studies. To bolster system defenses, Wu et al. [5] introduced an advanced feature extraction framework paired with Support Vector Machines (SVM), achieving a remarkable 99.8% accuracy in detecting malicious activities across network environments.

However, the use of Virtual Private Networks (VPNs) complicates attacker identification by encrypting and masking traffic patterns, rendering traditional monitoring methods less effective. To counter this,

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

researchers developed FlowPic [6], a robust anomaly detection technique capable of analyzing encrypted traffic, reaching an accuracy of 99.2%.

Building on cybersecurity advancements, Bakhshi et al. [7] proposed a hybrid deep learning model combining Convolutional Neural Networks (CNNs) and Gated Recurrent Units (GRUs). This architecture effectively distinguishes malicious traffic from legitimate social media interactions, significantly enhancing detection performance.

As obfuscation tools like VPNs and Tor become more widespread, tracing user behavior grows increasingly difficult due to altered IP addresses and port values. To address this, the AI-FlowDet framework [8] was introduced, analyzing 294 statistical and structural features to overcome issues like "one-flow" limitations and flow timeouts, achieving 98.5% classification accuracy.

In encrypted environments, identifying spoofed versus genuine web pages poses another challenge. The ENiD method [9], utilizing four distinct machine learning models, achieved 97% accuracy and a strong F1 score in encrypted web traffic classification.

Recognizing the privacy risks posed by metadata analysis in encrypted traffic, Kour et al. [10] applied the XGBoost algorithm to differentiate VPN from non-VPN traffic, attaining 92.4% accuracy across multiple open datasets.

Beyond security, Kour et al. [11] explored AI's potential in mental health diagnostics by developing a Depression Detection Framework. This system analyzes Twitter data to identify depressive symptoms, reporting an accuracy of 94.28%.

Wu et al. [12] introduced BehaveSniffer, a behavior classification system leveraging Graph Convolutional Networks (GCNs) and a Traffic Burst Graph (TBG) model, achieving 99.8% accuracy in encrypted traffic analysis.

Zhou et al. [14] developed a 1D-CNN model enhanced with normalization and attention mechanisms, extracting features from hexadecimal traffic data with 98.8% accuracy.

To overcome the limitations of single-modal classification, researchers in [18] proposed FusionTC, a multi-model integration framework using a two-layer stacking classifier, improving robustness in traffic analysis.

Addressing the rise of automated social bots, Bazm et al. [21] curated a dataset of 2,000 real and fake profiles. Their AdaBoost-based classifier, trained on behavioral features, reached 95% accuracy.

Long et al. [19] applied L1 regularization to refine feature selection for anomaly detection in encrypted networks, achieving an outstanding 99.98% accuracy.

As smart cities expand, cyberbullying across multimedia platforms has intensified. In response, researchers in [20] introduced a hybrid model combining GoogLeNet and Graph Neural Networks, effectively classifying text, image, and video content with 96% accuracy.

To move beyond basic arithmetic-based feature methods, Wang et al. [13] developed a graph-based approach using temporal attack graphs and GNNs, reaching 99% accuracy across three benchmark datasets. Despite these advances, encrypted traffic still presents major classification challenges.

Finally, [22] proposed a popularity-driven spam detection technique using Particle Swarm Optimization (PSO) for feature selection. When paired with machine learning classifiers, this method achieved 99.5% accuracy.

## 3. Challenges Of Cyber Security

In today's digital age, cybersecurity has become a pressing concern for individuals, corporations, and governments. As technology usage expands, so does the need to safeguard networks, devices, and personal data from theft, misuse, or damage. Despite advancements in security tools,

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

defending against cyber threats is increasingly complex. This article explores major challenges in the cybersecurity industry and outlines potential future solutions.

A. The Evolving Nature of Cyber Attacks

Modern cyber-attacks are growing more sophisticated and harder to detect. Hackers now employ advanced techniques such as multi-layered intrusions, fileless malware (which leaves no trace), zero-day exploits, and long-term hidden threats known as Advanced Persistent Threats (APTs).

B. Advanced Persistent Threats (APT)

APTs are not random attacks—they are strategic, often state-sponsored or backed by organized criminal groups. These threats typically target critical sectors like national security, defense, chemical industries, and IT firms. A notable example is the Aurora Operation in 2009, where attackers infiltrated major tech companies including Google, Adobe, and Juniper Networks to steal intellectual property using sophisticated methods [17].

C. -Day Exploits

Zero-day exploits take advantage of unknown software vulnerabilities—issues that developers haven't yet discovered or patched. These attacks are especially dangerous due to the absence of immediate fixes. A prominent case is Stuxnet, a worm that targeted Iran's nuclear infrastructure by exploiting multiple zero-day flaws. The lifecycle of such exploits includes five stages: discovery, weaponization, delivery, exploitation, and remediation. Detecting them requires robust monitoring systems, behavior-based analysis, and timely updates [17].

D. Security Issues in Internet of Things (IoT) Devices

The Internet of Things (IoT) connects billions of smart devices—sensors, appliances, and machines—through internet protocols, enabling seamless data exchange. However, this interconnectedness introduces significant cybersecurity risks [18]. Most IoT devices have limited memory and processing power, making it difficult to implement strong security features. Weak default configurations and outdated software further expose them to attacks [16]. IoT devices collect vast amounts of sensitive personal data. Without proper encryption and secure storage, this information is vulnerable to breaches. Wireless communication channels such as Wi-Fi and Bluetooth can be intercepted, allowing attackers to eavesdrop or manipulate data [15].

E. AI-Based Cyber Attacks

The rise of Artificial Intelligence (AI) and Machine Learning (ML) has introduced new challenges in cybersecurity. Attackers now use these technologies to launch more intelligent and adaptive attacks.

Types of AI-Based Attacks

- AI-assisted attacks – AI supports human attackers in planning and execution
- AI-driven autonomous attacks – AI systems operate independently to breach systems

## 4. Emerging Cyber Threats and Security Issues in Social Networking Platforms

### A. Identification of External Threats: Challenges and Trends in Social Network Security and User Behavior Detection

Researchers have employed a wide array of techniques and algorithms to detect cyberattacks within social networks and distinguish between authentic and deceptive user behavior. Despite these efforts, a comprehensive review of the literature reveals that identifying anomalous behavior and malicious traffic remains one of the most persistent and complex challenges in social network security.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

Numerous models and frameworks have been proposed; however, a key limitation persists: the majority of these models have been trained and validated using only two or three publicly available datasets, which restricts their scalability and generalizability. The performance of any detection algorithm is heavily influenced by the quality and diversity of the datasets used during its development. Unfortunately, most existing studies rely predominantly on the ISCX dataset, which introduces a significant constraint.

To address this limitation, the proposed Magteon Turing L3TM framework aims to enhance detection capabilities by expanding dataset diversity. Notably, over 70% of datasets used in prior research originate from the Canadian Institute of Cybersecurity and focus primarily on three categories of encrypted traffic: VPN, non-VPN, and Tor [24].

VPN traffic presents unique challenges due to its encryption and obfuscation, complicating the identification of malicious transmissions. In contrast, non-VPN traffic allows for more straightforward behavioral profiling. Between 2015 and 2024, the research community made continuous advancements in traffic analysis and attacker behavior detection, striving to differentiate harmful traffic from legitimate transmissions and uncover nuanced user activity patterns [23].

Before 2016, cybersecurity efforts were largely concentrated on web-based social platforms. However, as user expectations evolved, mobile and application-based social platforms surpassed websites in popularity. This transition led to increased user engagement and a corresponding rise in cyberattacks [25].

A compilation of techniques developed between 2016 and 2024 was analyzed to track annual trends in traffic analysis versus user behavior detection. Graphical data revealed that in 2016, traffic analysis accounted for only 40% of research focus, while user behavior detection dominated at 76%. Each subsequent year witnessed the emergence of new algorithms aimed at improving the identification of traffic patterns and anomalous behaviors [26].

### B. Internal Security Threats: Defending Social Networks Against Evolving Threats

Safeguarding social media platforms and applications from a broad spectrum of cyber threats remains a top priority. Researchers have proposed various methodologies to detect malicious activities and differentiate between genuine and fraudulent users [27]. Among the most prevalent internal threats are bots, anomalies, and Sybil attacks, which significantly undermine user authenticity and platform integrity [28].

To mitigate these threats, researchers [29–30] have developed specialized algorithms and frameworks designed to identify and categorize social network attacks. The primary goal is to reduce the frequency of cyber intrusions by accurately distinguishing real users from fake or malicious entities.

Following the deployment of these methodologies, statistical evaluations and comparative analyses were conducted against existing models. These studies confirmed the effectiveness of the proposed algorithms in detecting and classifying security threats specific to social applications.

Despite the availability of robust solutions, certain limitations persist. For an algorithm to be considered truly effective in securing social networks, it must be capable of addressing a wide range of attack scenarios and adapting to the dynamic nature of online environments. Only those models that demonstrate resilience across diverse conditions can be deemed fully reliable and scalable.

## 5. Conclusions

In today’s rapidly evolving digital landscape, social networks have become central to communication, collaboration, and information exchange. Yet, this ubiquity also makes them prime targets for an expanding array of cyber threats. From identity theft, phishing, and social engineering to

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

deepfake manipulation and large-scale data breaches, the security risks associated with social networking platforms are growing in both complexity and frequency.

This study highlights the major emerging threats in social network security and underscores the urgent need for adaptive, intelligent cybersecurity strategies. As cybercriminals increasingly leverage advanced technologies such as AI and machine learning, traditional security measures alone are no longer sufficient. There is a pressing demand for continuous research, robust authentication protocols, user awareness initiatives, and proactive policy interventions to safeguard user data and privacy.

## REFERENCES

[1]. Y. Liu, J. Huang, Y. Li, D. Wang, B. Xiao, Generative AI model privacy: a survey, Artif. Intell. Rev. 58 (1) (2024) 33, https://doi.org/10.1007/s10462-024-11024-6.

[2]. Q. Lai, H. Hua, Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes, Expert. Syst. Appl. 264 (2025) 125854,https://doi.org/10.1016/j.eswa.2024.125854.

[3]. R. Chapaneri, S. Shah, Enhanced detection of imbalanced malicious network traffic with regularized generative adversarial networks, J. Netw. Comput. Appl. 202(2022) 103368, https://doi.org/10.1016/j.jnca.2022.103368.

[4]. Najafi, O. Varol, TurkishBERTweet: fast and reliable large language model for social media analysis, Expert. Syst. Appl. 255 (2024) 124737, https://doi.org/10.1016/j.eswa.2024.124737.

[5]. H. Wu, Q. Wu, G. Cheng, S. Guo, Instagram user behavior identification based on multidimensional features, in: IEEE INFOCOM 2020 - IEEE Conference onComputer Communications Workshops (INFOCOM WKSHPS), IEEE, 2020, pp. 1111–1116, https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162688.

[6]. T. Shapira, Y. Shavitt, FlowPic: a generic representation for encrypted traffic classification and applications identification, IEEE Trans. Netw. Serv. Manag. 18(2) (2021) 1218–1232, https://doi.org/10.1109/TNSM.2021.3071441.

[7]. [T. Bakhshi, B. Ghita, Anomaly detection in encrypted internet traffic using hybrid deep learning, Secur. Commun. Netw. 2021 (2021) 1–16, https://doi.org/10.1155/2021/5363750.

[8]. H.-Y. Chen, T.-N. Lin, The challenge of only one flow problem for traffic classification in identity obfuscation environments, IEEE Access. 9 (2021)84110–84121, https://doi.org/10.1109/ACCESS.2021.3087528.

[9]. G. Mengmeng, Y. Xiangzhan, V.Mysore Sachidananda, L. Shangqing, L. Likun, ENiD: an encrypted web pages traffic identification based on web visiting behavior, in: 2022 IEEE International Conference on Data Mining Workshops (ICDMW), IEEE, 2022, pp. 593–601, https://doi.org/10.1109/ICDMW58026.2022.00082.

[10]. Z. Wang, B. Ma, Y. Zeng, X. Lin, K. Shi, Z. Wang, Differential preserving in XGBoost model for encrypted traffic classification, in: 2022 International Conference on Networking and Network Applications (NaNA), IEEE, 2022, pp. 220–225, https://doi.org/10.1109/NaNA56854.2022.00044.

[11]. H. Kour, M.K. Gupta, An hybrid deep learning approach for depression prediction from user tweets using feature-rich CNN and bi-directional LSTM, Multimed. Tools. Appl. 81 (17) (2022) 23649–23685, https://doi.org/10.1007/s11042-022-12648-y.

[12]. T. Wu, et al., BehavSniffer: sniff user behaviors from the encrypted traffic by traffic burst graphs, in: 2023 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), IEEE, 2023, pp. 456–464, https://doi.org/10.1109/SECON58729.2023.10287511.

[13]. L. Wang, Z. Cheng, Q. Lv, Y. Wang, S. Zhang, W. Huang, ACG: attack classification on encrypted network traffic using graph Convolution attention Networks, in: 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2023, pp. 47–52, https://doi.org/10.1109/CSCWD57460.2023.10152599.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
**https://www.tejasjournals.com/**
**https://doi.org/10.63920/ICFCSAI2025.007**

[14]. Y. Zhou, et al., Identification of encrypted and malicious network traffic based on one-dimensional convolutional neural network, J. Cloud Comput. 12 (1) (2023) 53, https://doi.org/10.1186/s13677-023-00430-w.

[15]. Satya B Verma, Shashi B V, Data Transmission in BPEL (Business Process Execution Language), ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue, Vol. 9 N. 3 (2020), 105-117 eISSN: 2255-2863 DOI: https://doi.org/10.14201/ADCAIJ202093105117 105

[16]. SB Verma, Brijesh P., and BK Gupta, Containerization and its Architectures: A Study, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Vol. 11 N. 4 (2022), 395-409, eISSN: 2255-2863, DOI: https://doi.org/10.14201/adcaij.28351

[17]. Anamika Agarwal, S. B. V., B. K. Gupta, A Review of Cloud Security Issues and Challenges, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Issue, Vol. 12 N. 1 (2023), pp 1-22, eISSN: 2255-2863, 2023 https://doi.org/10.14201/adcaij.31459

[18]. S. Li, et al., FusionTC: encrypted app traffic classification using decision-level multimodal fusion learning of flow sequence, Wirel. Commun. Mob. Comput. 2023 (2023) 1–15, https://doi.org/10.1155/2023/9118153.

[19]. S.R. Sahoo and B.B. Gupta, "Popularity-based detection of malicious content in Facebook using machine learning approach," 2020, pp. 163–176. doi:10.1007/978-981-15-0029-9_13.

[20]. B.A. Scott, M.N. Johnstone, P. Szewczyk, S. Richardson, BGP anomaly detection as a group dynamics problem, Comput. Netw. 257 (2025) 110926, https://doi.org/10.1016/j.comnet.2024.110926.

[21]. C. Jisi, B. Roh, J. Ali, An effective scheme for classifying imbalanced traffic in SDIoT,leveraging XGBoost and active learning, Comput. Netw. 257 (2025) 110939, https://doi.org/10.1016/j.comnet.2024.110939.

[22]. X. Chen, et al., High-performance routing for hose-based VPNs in multi-domain backbone networks, Comput. Netw. 57 (4) (2013) 944–953, https://doi.org/10.1016/j.comnet.2012.11.010.

[23]. C. Xenakis, C. Ntantogian, I. Stavrakakis, A network-assisted mobile VPN for securing users data in UMTS, Comput. Commun. 31 (14) (2008) 3315–3327,https://doi.org/10.1016/j.comcom.2008.05.018.

[24]. S. Lv, C. Wang, Z. Wang, S. Wang, B. Wang, Y. Zhang, AAE-DSVDD: a one-class classification model for VPN traffic identification, Comput. Netw. 236 (2023) 109990, https://doi.org/10.1016/j.comnet.2023.109990.

[25]. J. Li, B. Feng, H. Zheng, A survey on VPN: taxonomy, roles, trends and future directions, Comput. Netw. 257 (2025) 110964, https://doi.org/10.1016/j.comnet.2024.110964.

[26]. K. Raghavan, et al., Advancing anomaly detection in computational workflows with active learning, Fut. Gener. Comput. Syst. 166 (2025) 107608, https://doi.org/10.1016/j.future.2024.107608.

[27]. B. Bertalaniˇc, V. Hanˇzel, C. Fortuna, Explainable semantic wireless anomaly characterization for digital twins, Comput. Netw. 251 (2024) 110660, https://doi.org/10.1016/j.comnet.2024.110660.

[28]. S. Corli, L. Moro, D. Dragoni, M. Dispenza, E. Prati, Quantum machine learning algorithms for anomaly detection: a review, Fut. Gener. Comput. Syst. 166 (2025) 107632, https://doi.org/10.1016/j.future.2024.107632.

[29]. Muhammad Nadeem, Advancing social network security with magteon-turing L3TM: A multi-layered defense system against cyber threats, Computer Networks, 267 (2025), https://doi.org/10.1016/j.comnet.2025.111375

[30]. A.J. Hashim, M.A. Balafar, J. Tanha, A. Baradarani, Adaptive deep learning models for efficient multivariate anomaly detection in IoT infrastructures, Appl. Soft. Comput. 167 (2024) 112377, https://doi.org/10.1016/j.asoc.2024.112377.