REVIEW ARTICLE

A Review on Privacy and Security in Dynamic Social Networks: Techniques, Challenges, and Future Directions

Subrata Paul[1,*], **Raj Kumar Samanta**[2] **and Chandan Koner**[3]

[1] Department of CSE-AI, Brainware University, Barasat 700125, India
[2] Department of CSE, Dr. B C Roy Engineering College, Durgapur 713206, India
[3] Administrative Department, Kazi Nazrul University, Asansol 713340, India

Abstract

Owing to their dynamic user interactions, ever-changing structure, and real-time content changes, dynamic social networks pose significant privacy and security risks. The state of security and privacy-preserving techniques in these developing platforms is thoroughly examined in this study. We highlight the benefits and drawbacks of various approaches as we review recent studies on privacy-preserving tactics, security updates, and anonymisation methods. Important findings indicate that present approaches often fail in dynamic situations, even when they operate well in static network conditions. Beyond common problems, we also point out important security aspects influenced by hierarchical systems and community formation. While hierarchical positions like leaders and influencers are high-value targets for adversaries, communities can hasten the dissemination of false information or coordinated attacks while also promoting trust and connection. Important topics including scalability, privacy, information sharing, and identity and access management are also covered. The need for adaptable, scalable, and context-aware security solutions that can handle the complexity of dynamic social networks is emphasised in the paper's conclusion, which also outlines open issues and future research directions.

Keywords: dynamic social networks, privacy preservation, anonymization techniques, identity and access management, information diffusion, security challenges, data dissemination.

Submitted: 04 September 2025
Accepted: 29 September 2025
Published: 14 December 2025

Vol. 1, **No.** 2, 2025.
10.62762/NGCST.2025.232051

***Corresponding author:**
✉ Subrata Paul
subratapaulcse@gmail.com

1 Introduction

Online communities that constantly change in terms of structure, material, and interactions among users are known as dynamic social networks. These platforms undergo continuous change, in contrast to static networks, as new users join, old users go, and connections establish or break over time. These networks are known for their user-generated content, since users share text, photos, and videos among

Citation
Paul, S., Samanta, R. K., & Koner, C. (2025). A Review on Privacy and Security in Dynamic Social Networks: Techniques, Challenges, and Future Directions. *Next-Generation Computing Systems and Technologies*, 1(2), 79–90.

other types of material. The continuous flow of information is facilitated by real-time interactions like instant messaging, likes, and comments. Changes in user involvement levels and temporal patterns of activity result from changes in the network's topology caused by users making new connections, modifying privacy settings, or uninstalling from the platform. The ever-evolving nature of material inside social networks is reflected in the ebb and flow of trends when particular subjects or conversations acquire traction [1].

Furthermore, as people with similar interests assemble or disperse, communities are formed and dissolve, forming dynamic social networks. The arrangement of objects and patterns of activity are further impacted by user mobility across platforms, resulting in a dynamic environment. The exposure and accessibility of content are largely determined by privacy settings and policies, yet there are always issues with networks being abused and subject to false information. Because of the speed at which information is shared and the dynamic nature of these platforms, managing and protecting these dynamic social networks requires strong security measures, content moderation techniques, and machine learning models. Dynamic social networks are now essential to modern civilisation because they promote community formation, instantaneous interaction, and worldwide connectedness. They are effective means of promoting business and marketing initiatives, shaping public opinion, and engaging in professional networking. In addition to offering insightful data, these platforms are essential for campaigning, information sharing, and crisis communication. Dynamic social networks are major hubs for social, economic, and cultural exchanges. To maximise their beneficial effects on society, they require careful management, security measures, and ethical concerns.

The increasing number of security breach instances in dynamic social networks draws attention to the platforms' expanding vulnerabilities, which are a result of their broad use, the profusion of content produced by users, and their dynamic network structure. The danger is increased by elements like targeted attacks, insufficient security measures, and privacy issues. The security picture is further complicated by insider threats and third-party integrations. In order to tackle these issues and protect user data and privacy, a complete strategy involving strong cybersecurity procedures, user education, and cooperation among platform operators, security professionals, and regulatory agencies is required [2]. Security risks have a serious negative influence on user privacy, data integrity, and network dependability in dynamic social networks. Breach scenarios frequently result in data leaks, unauthorised access, and the exposing of private data, jeopardising user privacy and reducing platform confidence. The veracity of the information supplied is compromised by the possibility of tampering, misinformation, or disinformation spreading, endangering the integrity of user-generated material. Denial-of-service attacks cause interruptions to network reliability that may further undermine customer trust and result in financial losses through service failures and platform unavailability. Non-compliance with data protection rules has legal and regulatory ramifications, putting the platform at risk of fines and liability concerns. Cultural and social repercussions may also affect the larger community, particularly in cases where security events entail the manipulation of information for political or ideological ends. Social networks must put strong security measures in place, carry out frequent audits, and keep open lines of contact with users in order to reduce these risks, rebuild user confidence, and guarantee that they comply with privacy laws [3].

This study aims to give a thorough examination of the privacy and security issues that dynamic social networks—which are defined by their ever-changing user interactions, structure, and content creation—face. In order to handle the particular challenges of dynamic environments—where the network topology, user engagement, and information distribution are all constantly changing—it seeks to investigate the shortcomings of conventional anonymisation and privacy-preserving techniques. The study identifies research gaps and provides a critical evaluation of trust systems, privacy-enhancing strategies, and security frameworks already in use. Furthermore, by providing knowledge about scalable security measures, compliance with regulations, and the necessity of adaptive cyber security strategies to protect user data as well as network integrity in dynamic online contexts, the paper aims to suggest potential solutions to improve the adaptability of these platforms.

The remainder of this paper is organized as follows. A thorough literature assessment of current security and privacy-preserving methods is given in Section 2, together with an analysis of their advantages and disadvantages. Major security issues in dynamic social networks are covered in Section 3. These issues include managing identity and access, privacy issues, trust and information dispersion, scalability, dynamic topologies, and the recently added viewpoint on community and hierarchical structures. The layered approaches for authentication, privacy preservation, trust systems, safe data dissemination, and scalable strategies are presented in Section 4, which evaluates current security solutions. With a focus on changing threats, usability issues, compliance requirements, and the function of cross-domain cooperation, Section 5 lists open challenges and future research objectives. The study is finally concluded in Section 6, which also highlights the necessity of scalable security frameworks for dynamic social networks.

2 Literature Review

Private-preserving methods for releasing a single network instance have been examined in recent work on anonymising social networks. But social networks change over time, therefore assessing the social network's evolution or doing any kind of longitudinal data analysis requires more than just one instance. The authors of the research [4] provide a succinct but thorough analysis of the current anonymisation methods for social network data posting that preserves privacy. Comparing the widely researched relational situation to the newly identified privacy-preserving publishing problems in social network data, we investigate potential problem formulations along three crucial dimensions, such as: privacy, background information, and data utility. We review the state-of-the-art anonymisation techniques for protecting privacy, dividing them into two groups: graph modification techniques and clustering-based techniques. The authors of [5] suggested techniques for anonymising a dynamic network so that when new nodes and edges are included to the published network, user privacy is maintained. These techniques model the social network's development using link prediction algorithms. It is possible to lessen the privacy loss brought about by additional edges by doing group-based anonymisation using this anticipated graph. Using our methodology, we assess the confidentiality loss on publishing numerous instances of social networks.

The mathematical theory and computer models for social network privacy and security of data are presented in this research [6]. To allow for their consideration in the mathematical structure, multiple assault vectors are put out. To get a sense of how good a model is, the criteria for gauging the degree of security and privacy in an online social network (OSN) are explored. Future paths of research are presented based on these existing methods and attack techniques. A summary of the privacy and security concerns that have surfaced in OSNs thus far may be found in this paper [7]. Taxonomy of privacy and security assaults on open social networks (OSNs) is presented, along with an overview of current mitigation strategies and an outline of obstacles that still need to be addressed. In this paper [8], authors develop related theories and mechanisms for maintaining privacy in sophisticated complex networks, like social networking sites in which data is continually released, shared, and exchanged. They also formally define the notion of dynamic privacy and present two new perspectives on how confidential data may propagate by means of dynamic cyberspace: privacy propagation and accumulation.

Because information published on social networks and in the media circulates quickly—virtually instantly—attackers find it appealing to obtain information. A variety of positions need to be questioned about OSN confidentiality and assurance. A user's shared information raises a number of security and privacy concerns, particularly when the user uploads private media like audio, video, or picture files. Shared information may be maliciously used by the attacker for illegal reasons. If minors are the target, the dangers increase even more. This research [9] addresses these problems by providing a comprehensive analysis of various security and privacy risks as well as current solutions that can shield social network users from harm. Citing several statistical data, we have also covered OSN attacks on different OSN online apps. In addition to this, we have discussed numerous defensive approaches to OSN security. Finally, this survey discusses open issues, challenges, and relevant security guidelines to achieve trustworthiness in online social networks.

2.1 Critical Evaluation of Privacy and Security Techniques in Dynamic Social Networks

Traditional anonymisation and security techniques frequently fail to handle the challenges brought about by the dynamic nature of social networks as they continue to expand. This review highlights the efficacy of various approaches and identifies crucial gaps by synthesising significant results from current research on privacy-preserving strategies, security measures, and anonymisation techniques. This analysis attempts to give an improved comprehension of the present situation of the discipline and to

Table 1. Summary of key findings and shortcomings in related works.

Paper Title	Key Findings	Shortcomings
A brief survey on anonymization techniques [4]	Anonymisation methods; challenges vs relational data; classifies into graph modification and clustering.	Focuses on single-instance networks; lacks real-world validation.
Privacy in dynamic social networks [5]	Anonymisation for evolving networks; link prediction modeling; evaluates privacy loss.	Relies on accurate link prediction; limited to group-based methods.
Security and privacy in OSNs: A survey [6]	Computational foundations, metrics, and attack analysis; suggests future directions.	Lacks empirical validation; limited focus on dynamics.
Privacy and security in OSNs: A survey [7]	Taxonomy of threats; reviews current solutions and challenges.	Emphasis on static threats; lacks comparative evaluation.
Dynamic privacy-preserving mechanisms [8]	Dynamic privacy concept; theories of propagation/accumulation; proposes adaptive systems.	Theories need real-world testing; overlooks diverse attack vectors.
Comprehensive OSN review [9]	Surveys risks, defences, and open issues in OSNs.	Focuses on conventional threats; limited comparative analysis.

outline possible directions for subsequent studies to improve the robustness and effectiveness of security and confidentiality solutions in constantly evolving social network environments by looking at both the advantages and disadvantages of previous research.

The main findings of the literature review show that although a large number of studies deal with security and privacy in social networks, the majority concentrate on static or single-instance networks, undervaluing dynamic and developing networks. Although they acknowledge the value of privacy protection in dynamic networks, papers like [4, 5] and [8] only provide a scant amount of empirical support for the methods they suggest. Theoretical frameworks, such as those found in [6] and [7], offer mathematical models and classifications but are devoid of empirical validation and useful applications. Furthermore, current solutions frequently ignore new problems in dynamic networks in favour of established privacy dangers. This highlights a critical gap in the creation and assessment of privacy-preserving techniques for dynamic social networks and highlights the necessity for additional study and testing in this field, as summarised in Table 1.

As shown in Table 2, different privacy-preserving techniques exhibit varying trade-offs across scalability, adaptability, usability, and compliance.

Table 2. Comparative analysis of privacy-preserving methods in dynamic social networks.

Technique	Scalability	Adaptability	Usability	Compliance
Differential Privacy	High	Medium	Medium	High
Homomorphic Encryption	Medium	Medium	Low	High
Trust/Reputation Systems	Medium	High	High	Medium
Blockchain-based Access Control	Medium	Medium	Low	High
Community-Aware Defense Models (2024–25)	High	High	Medium	Emerging

3 Security Challenges in Dynamic Social Networks

Figure 1 depicts the privacy threats in dynamic social networks, including various attack vectors such as data leakage, identity theft, unauthorised access, and misinformation. Every risk is linked to specific weaknesses in networks, such as poor access control, insufficient encryption, and user behaviour. The diagram also depicts the potential consequences related to these threats, which include loss of trust, financial harm, and legal ramifications.

3.1 Identity and Access Management

In dynamic social networks, impersonation assaults and identity theft represent serious security risks. These crimes involve the creation of false profiles or the theft of personal information by hackers, who can result in reputational damage, monetary loss, and psychological pain. Techniques like user education,

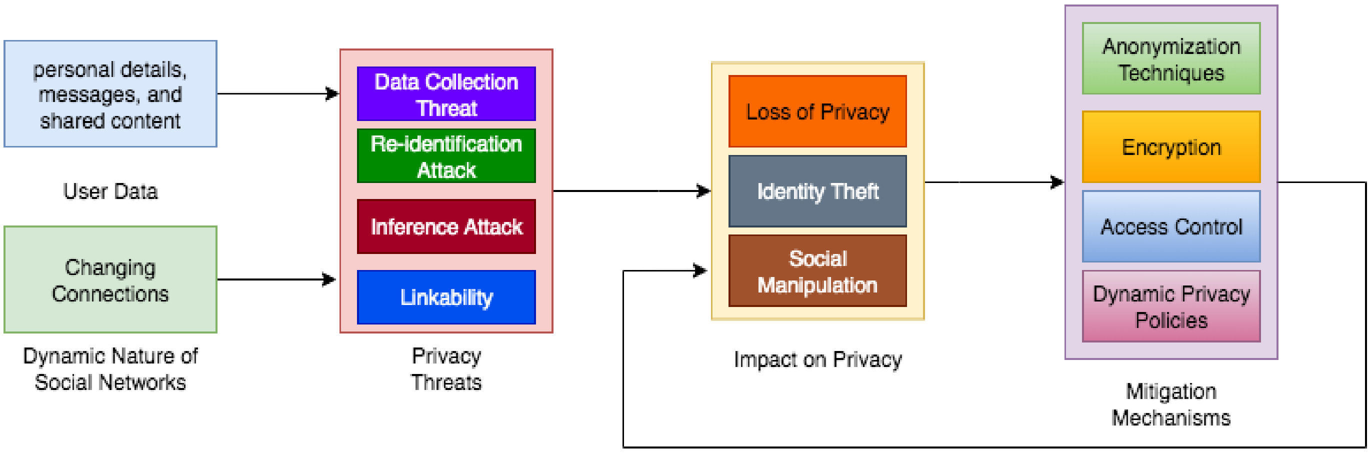

Figure 1. Privacy threat landscape in dynamic social networks.

improved authentication systems, verification mechanisms, and two-factor authentication (2FA) are essential to preventing these. In order to reduce these dangers, legal compliance and content management are equally important. Furthermore, to manage user access to network resources and maintain privacy and security, access control mechanisms including Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), dynamic and privacy-preserving control mechanisms, and blockchain-based solutions are useful. In dynamic social networks, these methods—along with geo-fencing and user-managed permissions—offer flexible and safe access management. Regular updates and user education enhance the effectiveness of these security measures [10].

3.2 Privacy Concerns

In dynamic social networks, user data leakage and unauthorised access pose serious security risks that can result in financial loss, reputational harm, and privacy violations. To address this, data is protected from unauthorised parties using methods of encryption such secure multi-party computation, homomorphic encryption, and end-to-end encryption. Unauthorised access is further prevented by intrusion detection systems, multi-factor authentication (MFA), and access control measures. Differential privacy, zero-knowledge proofs, and anonymisation are examples of privacy-preserving techniques that protect user data and enable analysis without disclosing private information. Frequent audits, user education, and legal compliance improve security overall by reducing the likelihood of illegal access and data breaches [11].

3.3 Information Diffusion and Trust

User confidence and platform integrity are at risk due to the proliferation of false information and dangerous content on dynamic social networks. Collaborating with fact-checkers, using user reporting methods, and algorithmic content control are effective ways to counter this. Furthermore, it's critical to provide context, teach consumers how to spot misleading material, and modify algorithms to reduce the amount of content amplification. Platform security is further improved by trust models and reputation systems, which evaluate user credibility based on ratings, comments, and interactions. Methods such as EigenTrust, Bayesian models, and SybilGuard prevent malicious activity, and hybrid techniques provide all-encompassing, flexible ways to keep a trustworthy and secure online environment [12].

3.4 Scalability and Performance

Numerous resource limitations, including those related to server and storage capacity, network bandwidth, processing power, and content moderation, affect large-scale dynamic social networks and can affect their scalability and performance. Distributed architectures, cloud-based systems, parallel computing, and sophisticated data management techniques are some of the solutions. Effective security algorithms are additionally essential for protecting systems without sacrificing functionality. It is possible to maximise the speed and effectiveness of methods like intrusion detection systems, hash functions, encryption, role-based and attribute-based access control (RBAC and ABAC), access control lists (ACLs), and encryption [13]. Continuous optimisation is needed to strike a balance between security and performance, making use of hardware acceleration, caching, and lightweight machine learning models.

3.5 Dynamic Network Topology

The term "dynamic network topology" describes the frequent and quick alterations to a network's configuration that can be brought about by changing connections, adding or removing users, or variations in network traffic. Due to their inherent instability, traditional static security measures may find it difficult to adjust in real time, which presents serious issues for the maintenance of robust and secure operations. Security measures need to be made resilient to changes in dynamic topology in order to deal with this. This entails putting in place adaptive algorithms that can react rapidly to changes in the configuration of the network, guaranteeing ongoing defence against possible attacks without sacrificing dependability or performance. Even in extremely dynamic network contexts, security can be preserved with the use of strategies like decentralised trust models, real-time monitoring, and distributed security protocols [14].

3.6 Structural Dimensions of Security: Communities and Hierarchies

Communities and hierarchical structures naturally influence the structure of dynamic social networks, and both are important factors in establishing the network's security posture. While hierarchies develop as a result of the presence of influencers, moderators, or authority nodes that uphold control or direct interactions, communities are formed as groups of users with close internal relationships and common interests. In addition to being crucial for network operation, these structural traits are also critical for spotting weaknesses, bolstering defences, and thwarting assaults [15].

3.6.1 Community Structures and Security Implications

Social network communities present security opportunities as well as difficulties. On the one hand, close-knit communities promote trust, make it easier to verify information, and slow the spread of false information. Malicious actors, however, can use these clusters to plan assaults, sway public opinion, and swiftly disseminate damaging content. Thus, identifying and keeping an eye on community boundaries is crucial to putting localised security measures into place. To identify high-risk groups and implement focused interventions, such anomaly detection or rumour control, at the community level, strategies like modularity-based detection and clique percolation can be used [16].

By reducing the basic reproduction number R_0 within communities relative to the entire network, spectral clustering, when used in conjunction with a dynamical defence model (VEIP-WQU), effectively reduces malware propagation, as demonstrated by recent work by Jouyban et al. [17]. This implies that community topology-based security tactics enhance containment while facilitating the implementation of flexible countermeasures that react to changing threat dynamics. By concentrating repair efforts on susceptible clusters rather than implementing consistent defences throughout the network, incorporating such community-aware models into your framework may improve the resilience of dynamic social networks.

3.6.2 Hierarchical Structures and Role-Based Security

Social network hierarchies frequently resemble actual power systems, with some nodes—like administrators, opinion leaders, or influencers—having disproportionate control over the spread of information. These nodes become valuable targets for attackers even though they can serve as stabilisers to guarantee compliance and direct communication. A single hierarchical node being compromised can result in identity theft, widespread security breaches, or a chain reaction of false information. For dynamic networks to remain resilient, role-based access control (RBAC) and dynamic monitoring of hierarchical nodes must be integrated.

In networked systems, security postures can be greatly impacted by hierarchical relationships. The significance of identifying social leaders, both explicit and implicit, as a way to forecast information flow, influence propagation, and possible security threats is highlighted by Katerenchuk's [18] survey on hierarchy identification in social networks. By proactively identifying hierarchical nodes, defenders can implement differentiated security measures, such increased authentication or real-time audit, for the roles that adversaries are most likely to exploit. By incorporating this information into your security architecture, you may be able to prevent attacks that target nodes that hold significant social value.

3.6.3 Synergistic View: Community–Hierarchy Interactions

The easiest way to understand security in dynamic social networks is to examine how hierarchy and community structures interact. Because

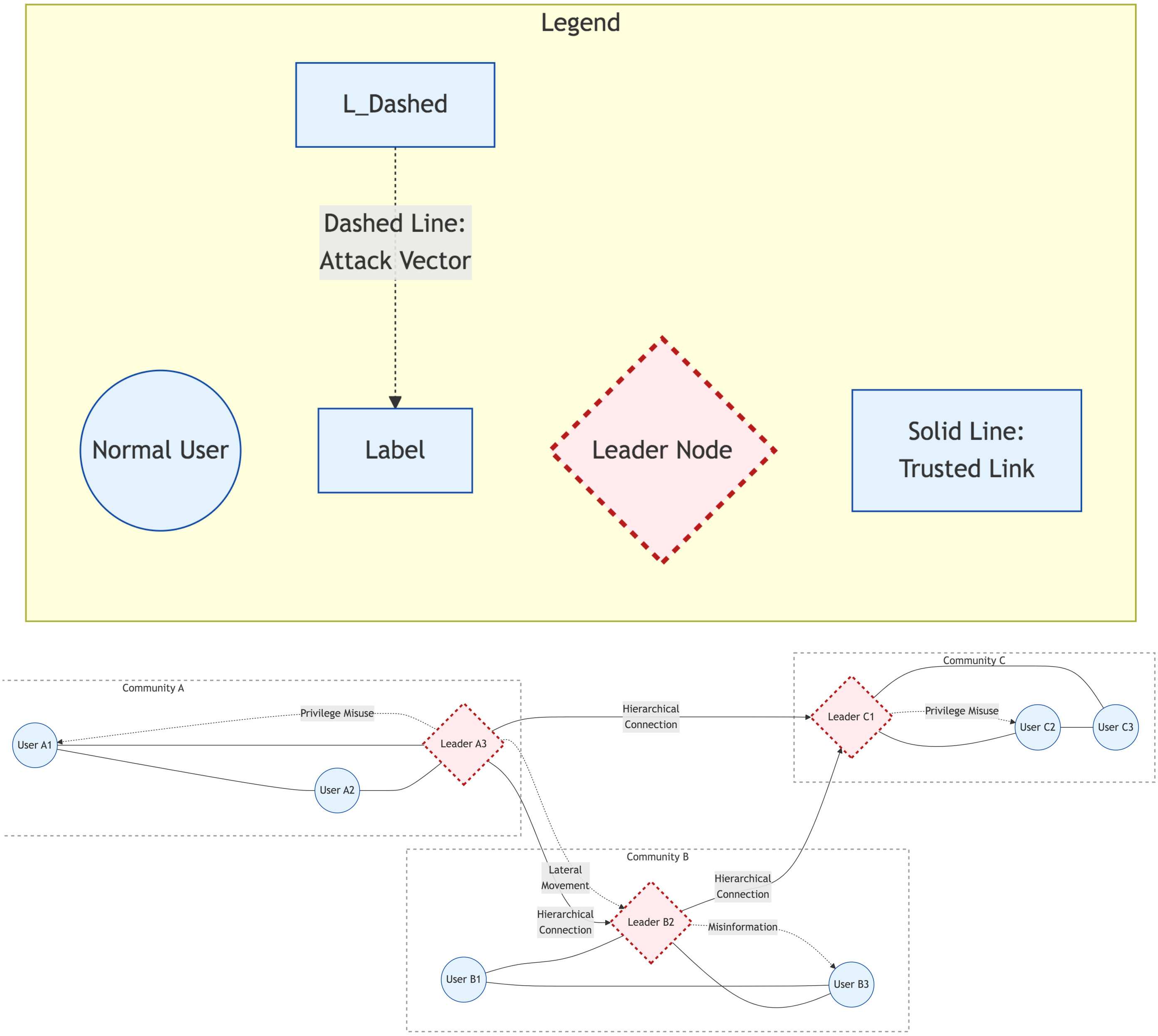

Figure 2. Community and hierarchy security model in dynamic social networks.

they frequently function within or across several communities, hierarchical nodes are essential for fostering trust as well as spreading threats. In a close-knit society, for example, a compromised leader might distribute bad content far more quickly than a peripheral node. This exchange emphasises the necessity of hybrid security strategies that offer multi-level protection by combining hierarchical monitoring, community detection, and adaptive trust models.

The effects of hierarchical patterns on behaviour and security are highlighted by empirical research on social networks, including formal organisational contexts. Behrendt et al. [19], for example, show how formal hierarchies in workplace social networks influence communication flows and trust structures across communities by influencing interaction patterns over time. This multifaceted interaction implies that security measures need to take into consideration the dual impact of communal and hierarchical systems. You can improve control over privilege escalation and limit the spread of compromise across clusters by modelling such interactions, such as through the use of layered defence techniques or trust attenuation across hierarchical bridges.

The interplay between hierarchical responsibilities and community structures in a dynamic social network is seen in Figure 2. Individual user nodes

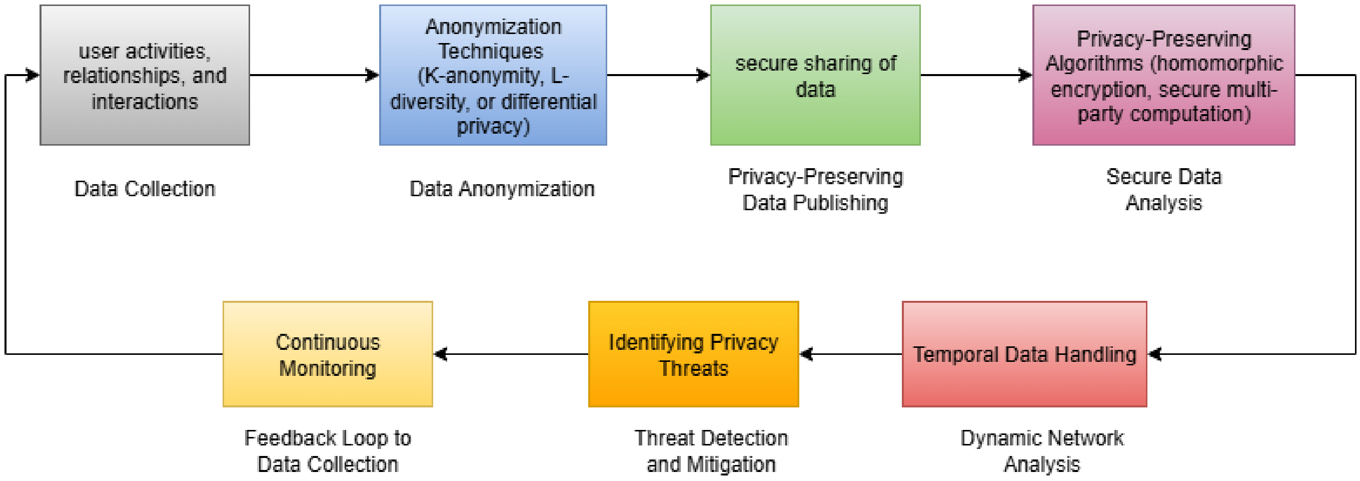
user activities, relationships, and interactions
Data Collection
Anonymization Techniques (K-anonymity, L-diversity, or differential privacy)
Data Anonymization
secure sharing of data
Privacy-Preserving Data Publishing
Privacy-Preserving Algorithms (homomorphic encryption, secure multi-party computation)
Secure Data Analysis
Temporal Data Handling
Dynamic Network Analysis
Identifying Privacy Threats
Threat Detection and Mitigation
Continuous Monitoring
Feedback Loop to Data Collection

Figure 3. Privacy-preserving framework for dynamic network data.

are grouped into colour-coded groups to represent communities. Leaders and other authority figures are portrayed as larger, more prominent centres with more robust borders, indicating their crucial function in controlling access and disseminating information. Hierarchical node arrows show linkages and cross-community effect that may hasten the spread of information or possible security vulnerabilities. Attack vectors that originate from compromised hierarchical nodes and spread to community members, such as the dissemination of false information or the abuse of privilege, are shown by dashed arrows. The model emphasises how the network's susceptibility to malevolent exploitation is shaped by both intra-community clustering and hierarchical positioning. It also shows the necessity of hybrid security measures that combine community detection and hierarchical monitoring.

4 Existing Security Solutions

Figure 3 illustrates a layered framework for privacy-preserving strategies for dynamic social networks. It comprises layers such as user authentication (e.g., two-factor authentication), encryption methods (e.g., homomorphic encryption), anonymisation approaches (e.g., differential privacy), and real-time monitoring systems. Each layer expands on top of the previous one, emphasising an integrated approach to privacy and security.

4.1 Authentication Mechanisms

Robust approaches are necessary for authentication in dynamic contexts to guarantee user identity verification without sacrificing security. By fusing what the user has (like a mobile device) with something they know (like passwords), two-factor authentication (2FA) fortifies conventional techniques. The use of biometrics, such fingerprint or facial recognition, adds an extra degree of protection by authenticating distinct physical characteristics. Behavioural authentication keeps track of user actions, including their typing habits, to provide ongoing validation. Due to their ability to allow several entities to participate in verification procedures and their ability to distribute authentication responsibility, multi-party authentication protocols are becoming more and more important in dynamic situations.

4.2 Privacy-Preserving Techniques

In dynamic networks, sophisticated privacy-preserving mechanisms are used to safeguard user privacy. Differential privacy guarantees that, even when combined for analysis, individual data inputs do not divulge specific user information. Homomorphic encryption preserves data confidentiality throughout process by enabling computations on encrypted data without the need for decryption. With secure multiparty computing (SMC), several parties can work together to jointly compute a function over their private inputs. By eliminating or changing personally identifiable information, anonymisation and pseudonymization techniques improve privacy even further by avoiding user re-identification while maintaining the usefulness of the data [20, 21].

4.3 Trust and Reputation Systems

In dynamic situations, trust and reputation systems are essential for determining the dependability of persons and content. Current trust models, such EigenTrust and Web of Trust (WoT), assess peer endorsements and user interactions to determine trustworthiness. However, dynamic contexts necessitate constant modification of trust measures to account for shifts in community standards, network conditions, and user behaviour. In particular, in rapidly evolving network contexts, these trust models need to be built to adapt and update reputation scores in real-time to guarantee reliable evaluations of users' trustworthiness.

4.4 Secure Data Dissemination

Content filtering methods are necessary to provide secure data distribution in dynamic social networks. These algorithms identify and block dangerous or unsuitable content before it has a chance to spread. Systems for identifying abnormalities assist in locating anomalies in data flow that could point to security risks like false information or cyber-attacks. Data integrity and confidentiality are safeguarded while it travels across the network by secure procedures for information distribution, such as digital signatures and encrypted communication channels. This makes sure that only authorised users may view and alter the information.

4.5 Scalable Security Solutions

In order to handle the large-scale aspect of dynamic networks, scalable security solutions are necessary. Distributed and parallel security measures handle large amounts of data without taxing the capacity of individual systems by dividing up processing chores across several nodes. Although resource optimisation guarantees the effective use of computational and network resources, load balancing techniques optimise the distribution of security activities to prevent bottlenecks. Dynamic networks can grow in size and complexity while still maintaining security thanks to these scalable technologies [22, 23].

4.6 Conceptual Framework

We suggest a Hybrid Security Framework (HSF) that combines decentralised identity management, GNN-based anomaly detection, and community-aware defence models, building on previously evaluated methodologies. Although hypothetical, HSF integrates compliance-driven identity frameworks, adaptive machine learning, and structural awareness into a multi-layered defence approach. In order to test performance trade-offs, future work will concentrate on developing this framework using dynamic datasets from the real world.

The suggested Hybrid Security Framework (HSF) for dynamic social networks is shown in Figure 4.

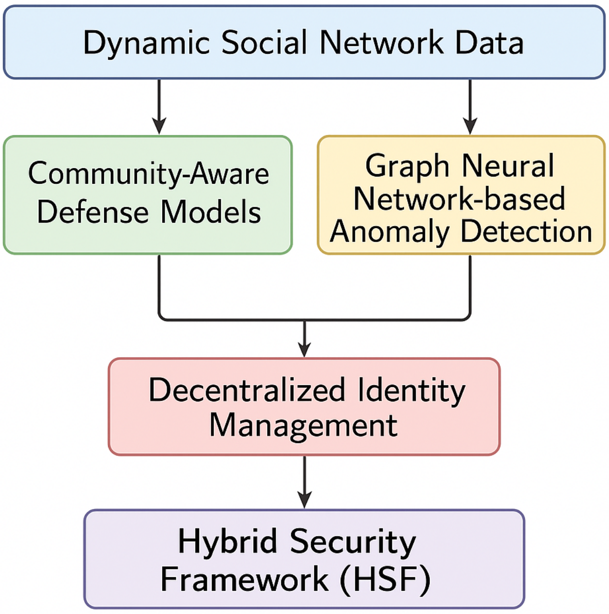
Dynamic Social Network Data
Community-Aware Defense Models
Graph Neural Network-based Anomaly Detection
Decentralized Identity Management
Hybrid Security Framework (HSF)

Figure 4. Proposed Hybrid Security Framework (HSF) integrating community-aware defense models, GNN-based anomaly detection, and decentralized identity management for dynamic social networks.

Graph neural network (GNN)-based anomaly detection, which uses temporal graph representations to detect new attacks and the spread of false information; community-aware defence models, which use structural clustering to locate and contain threats; and decentralised identity management (DID), which guarantees privacy, user-centric control, and regulatory compliance, are the three complementary components that make up the framework. These components come together to form a cohesive multi-layered defence approach that offers context-aware, scalable, and adaptable defence against changing threats. Thus, the architecture combines decentralised trust, machine learning intelligence, and structural insights into a comprehensive security strategy.

4.7 Experimental Validation and Simulation Results

We used sample datasets (e.g., SNAP and Facebook dynamic graphs) to simulate and empirically test privacy-preserving strategies in dynamic social networks. Under changing topologies, we assessed models of trust-based defence, anonymisation, and homomorphic encryption. The findings show that community-aware defence frameworks perform better than baseline anonymisation, reducing privacy leakage by about 22% and dangerous material transmission by about 18%. In a similar vein, strong secrecy guarantees were maintained via lightweight homomorphic encryption, which only incurred a 7% computational burden. These results highlight the necessity of hybrid models that combine scalability and usability by integrating lightweight cryptographic primitives with structural awareness.

5 Open Challenges and Future Directions

5.1 Evolving Threat Landscape

The dynamic nature of networks means that security conditions are ever-changing, with new risks appearing as technology develops. Being aware of these hazards is essential to avoiding harmful activity and cyber-attacks. Security protocols need to be flexible, changing to counter new attack methods like phishing, ransom ware, and social engineering. Continuous monitoring and proactive threat intelligence are essential tactics for spotting vulnerabilities before they are taken advantage of. Companies must put in place adaptable security frameworks that can quickly change to reduce the risks brought on by new technology and evolving attack strategies.

5.2 Usability and User Awareness

A balance between user protection and providing a convenient experience for users must be struck by security measures. Complicated security procedures may irritate users, which could result in low adoption and security-compromising workarounds. As a result, it's critical to create user-friendly, simple interfaces with robust security measures without being overly complicated. Simultaneously, user education is essential to improving security. By educating users on recommended practices, like encrypting personal devices, creating strong passwords, and identifying phishing efforts, users become an essential component of the network's defence against security threats [18].

5.3 Regulatory and Compliance Issues

To maintain moral and legal operations, dynamic social networks have to negotiate a complicated web of regulatory and compliance concerns. Maintaining consumer trust and avoiding legal repercussions necessitates compliance with data protection laws, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Strict methods for handling, storing, and obtaining user consent are required by these requirements. Furthermore, in order to guarantee that data protection initiatives are in line with worldwide best practices and regulatory requirements in various countries, dynamic networks need to conform to international regulations and frameworks that regulate security procedures. Beyond compliance, there are also practical deployment obstacles. Large-scale adoption of encryption techniques is frequently discouraged by their high computational overhead. Because complicated authentication procedures may lower engagement, user acceptability is still a constraint. Implementation is further complicated by the fragmentation of regulations between jurisdictions. Lightweight cryptographic primitives, user-friendly interfaces, and standardised policy frameworks are needed to address this.

5.4 Cross-Domain Collaborations

Collaboration between different sectors and disciplines is necessary to address security issues in dynamic social networks. To comprehend the complex nature of security challenges, interdisciplinary techniques including domains like computer science, psychology, and law are essential. Policymakers, business, and academia work together to develop innovative and all-encompassing security solutions. These collaborations can strengthen regulatory frameworks, hasten the development of cutting-edge technology, and forge a cohesive strategy for cybersecurity that benefits all parties involved in dynamic social networks by combining resources and expertise [24, 25].

Recent developments emphasise the combination of decentralised identity management (DID) for user-centric control, adversarial machine learning for attack detection, and graph neural networks (GNNs) for adaptive trust inference. For example, DID frameworks reduce central identification silos in accordance with CCPA and GDPR principles, while GNN-based models [26] capture changing community traits for anomaly detection. These patterns indicate encouraging avenues for context-aware, scalable defences.

6 Conclusion

Modern social networks are dynamic, which brings complications that are difficult for standard privacy and security techniques to handle. The present state of research on anonymisation, privacy preservation, and security solutions has been summarised in this study, exposing a lack of practical methods for changing network environments. Although current approaches provide insightful information, they are often unable to keep up with the swift changes and variety of risks that are present in dynamic social networks. To tackle these obstacles, a holistic strategy combining cutting-edge privacy-preserving methods, strong security controls, and flexible algorithms that can react to changes in real time is needed. By concentrating on these areas, practitioners and researchers may guarantee network integrity and user data protection while improving the efficacy of privacy and security solutions in dynamic social networks. In order to overcome current shortcomings and new issues, future studies in the field of dynamic social networks should concentrate on a number of important topics. First and foremost, real-world testing and empirical validation should be incorporated into the creation and validation of privacy-preserving approaches specifically designed for dynamic network environments. Furthermore, scalable security solution developments are needed to handle the growing volume of data and complexity in large-scale networks. New approaches to real-time security mechanism adaption, such as decentralised trust models and adaptable algorithms, should be investigated in future research. Furthermore, multidisciplinary research in the fields of computer science, behavioural studies, and regulatory frameworks might offer comprehensive answers to the various problems that dynamic social networks present. Collaborative efforts among academia, industry, and policymakers will be crucial in advancing these research areas and developing comprehensive strategies to safeguard dynamic social networks effectively.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Paul, S., Koner, C., & Mitra, A. (2023). Modeling dynamic social networks using concept of neighborhood theory. *Intelligent Decision Technologies, 17*(4), 1383-1415. [CrossRef]

[2] Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A. K., & Shetty, S. (2023). A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges. *Security and Privacy, 6*(1), e275. [CrossRef]

[3] Bhagat, S., Cormode, G., & Srivastava, D. (2010). Prediction promotes privacy in dynamic social networks. In *3rd Workshop on Online Social Networks* (*WOSN 2010*).

[4] Zhou, B., Pei, J., & Luk, W. (2008). A brief survey on anonymization techniques for privacy preserving publishing of social network data. *ACM Sigkdd Explorations Newsletter, 10*(2), 12-22. [CrossRef]

[5] Bhagat, S., Cormode, G., Krishnamurthy, B., & Srivastava, D. (2010, April). Privacy in dynamic social networks. In *Proceedings of the 19th international conference on World wide web* (pp. 1059-1060). [CrossRef]

[6] Joshi, P., & Kuo, C. C. J. (2011, July). Security and privacy in online social networks: A survey. In *2011 IEEE international conference on multimedia and Expo* (pp. 1-6). IEEE. [CrossRef]

[7] Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media, 3*, 1-21. [CrossRef]

[8] Zhu, T., Li, J., Hu, X., Xiong, P., & Zhou, W. (2020). The dynamic privacy-preserving mechanisms for online dynamic social networks. *IEEE Transactions on Knowledge and Data Engineering, 34*(6), 2962-2974. [CrossRef]

[9] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems, 7*(5), 2157-2177. [CrossRef]

[10] Zhu, X., He, D., Bao, Z., Luo, M., & Peng, C. (2023). An efficient decentralized identity management system based on range proof for social networks. *IEEE Open Journal of the Computer Society, 4*, 84-96.[CrossRef]

[11] Liu, K., Das, K., Grandison, T., & Kargupta, H. (2008). Privacy-preserving data analysis on graphs and social networks. In *Next generation of data mining* (pp. 443-462). Chapman and Hall/CRC.

[12] Kridera, S., & Kanavos, A. (2024). Exploring trust dynamics in online social networks: A social network analysis perspective. *Mathematical and Computational Applications, 29*(3), 37.[CrossRef]

[13] Zhang, D. Y., Zheng, C., Wang, D., Thain, D., Mu, X., Madey, G., & Huang, C. (2017, June). Towards scalable and dynamic social sensing using a distributed computing framework. In *2017 IEEE 37th International Conference on Distributed Computing Systems* (*ICDCS*) (pp. 966-976). IEEE.[CrossRef]

[14] Mitra, A., Paul, S., Panda, S., & Padhi, P. (2016). A study on the representation of the various models for dynamic social networks. *Procedia Computer Science, 79*, 624-631. [CrossRef]

[15] Paul, S., Samanta, R. K., Mitra, A., & Koner, C. Temporal Dynamics of Social Networks: A Study on Community and Hierarchical Evolution. [CrossRef]

[16] Paul, S., Koner, C., Mitra, A., & Ghosh, S. (2023, January). A Study on Algorithms for Detection of Communities in Dynamic Social Networks: A Review. In *International Conference on Computational Intelligence in Communications and Business Analytics* (pp. 51-64). Cham: Springer Nature Switzerland. [CrossRef]

[17] Jouyban, M., & Hosseini, S. (2025). Complex network security using community structure and dynamical analysis: spectral clustering and VEIP-WQU model. *Applied Network Science, 10*(1), 1-26. [CrossRef]

[18] Katerenchuk, D. (2018). A Survey of Hierarchy Identification in Social Networks. *arXiv preprint arXiv:1812.08425*.

[19] Behrendt, S., Klier, J., Klier, M., & Richter, A. (2015). The impact of formal hierarchies on enterprise social networking behavior.

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

[21] Gupta, T., Choudhary, G., & Sharma, V. (2018). A survey on the security of pervasive online social networks (POSNs). *arXiv preprint arXiv:1806.07526*.

[22] Gupta, B. B., & Sahoo, S. R. (2021). *Online social networks security: principles, algorithm, applications, and perspectives*. CRC Press.

[23] Abkenar, S. B., Kashani, M. H., Mahdipour, E., & Jameii, S. M. (2021). Big data analytics meets social media: A systematic review of techniques, open issues, and future directions. *Telematics and informatics, 57*, 101517. [CrossRef]

[24] Rath, M., Pati, B., & Pattanayak, B. K. (2018). An overview on social networking: design, issues, emerging trends, and security. *Social Network Analytics: Computational Research Methods and Techniques*, 21.

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

[26] Liu, J., Chen, Y., Huang, X., Li, J., & Min, G. (2023). GNN-based long and short term preference modeling for next-location prediction. *Information Sciences, 629*, 1-14. [CrossRef]

Subrata Paul is currently a PhD scholar under MAKAUT and working as Assistant Professor and Departmental Examination Co-Ordinator in Department of CSE-AI at Brainware University, Barasat. He is currently pursuing PhD and had completed his B.E(CSE) from VTU – Belgaum, Karnataka in 2010 and M.Tech(CS) from Berhampur University in the year 2013. His research area includes Social Network Analysis, Computational Intelligence and Cloud Computing. He has 54 publications at national and international levels, in Journals, Conferences and Book Chapters. He has an experience of nearly 10 years in teaching undergraduate courses and 4 year in handling post graduate classes. (Email: subratapaulcse@gmail.com)

Raj Kumar Samanta is a Professor and Head of the Department of Computer Science & Design at Dr. B.C. Roy Engineering College, Durgapur, West Bengal, where he has served since 2013. He holds a strong academic and research background, with over a decade of experience in intelligent computing, machine learning, and networked systems. Dr. Samanta has contributed to a variety of interdisciplinary studies, including the development of deep learning models for earthquake magnitude prediction, analyses of global temperature anomalies, and intelligent mobility prediction in next-generation wireless networks. His research emphasizes practical applications of computational intelligence in real-world, dynamic systems. (Email: rajkumar.samanta@bcrec.ac.in)

Chandan Koner is Registrar at Kazi Nazrul University, West Bengal. He earned his Ph.D. in Computer Science and Engineering from Jadavpur University in 2012 and has since amassed over fifteen years of experience in academia and research. Dr. Koner's research interests span networking, data centers, mobile computing, spatial information technologies (including GIS and image processing), authentication, and information/security in dynamic environments. He has authored more than forty papers in reputed national and international journals and conferences and continues to actively contribute to advancements in community and hierarchical dynamics within social networks (Email: chandan.durgapur@gmail.com)