Babylonian Journal of Machine Learning
Vol.2025, **pp**. 76–85
DOI: https://doi.org/10.58496/BJML/2025/006; ISSN: 3006–5429
https://mesopotamian.press/journals/index.php/BJML

Research Article

Privacy-Preserving Transfer Learning for Community Detection in Multiple Networks: A Review.

Marshima Mohd Rosli [1],*

[1] *College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam, Malaysia.*

ARTICLEINFO

Article History
Received 04 Feb 2025
Revised: 03 Mar 2025
Accepted 05 Apr 2025
Published 30 Apr 2025

Keywords

Privacy-Preserving Transfer Learning

Community Detection

Federated Learning

Graph-Based Machine Learning

Decentralized Networks

ABSTRACT

In order to identify communities in various networks, this study gives a thorough analysis of privacy-preserving transfer learning methods. In order to better understand the specific difficulties of implementing transfer learning in decentralized and diverse settings, it classifies current solutions according to their learning paradigms, privacy measures, and network topologies. The scalability, privacy, and utility trade-offs are used to assess anonymization, deep learning, and federated learning methods. There is a critical discussion of the gaps in the present research, including the absence of defined assessment standards and the inadequate incorporation of privacy into transfer systems. Also, this research points the way toward potential future possibilities for developing privacy-first models that can generalize across different types of networks. Researchers and practitioners in the field of graph-based machine learning may use the results as a guide to create safe and efficient solutions.

1. INTRODUCTION

The intricate interplay between privacy and community detection is critically examined and discussed in depth [1]. The growing significance of privacy is emphasized in light of the ever-increasing volumes of sensitive data that are now being acquired or derived from a plethora of varied sources. This sensitive data landscape includes information that pertains to multiple, interconnected networks, whose relations can be regarded as latent degrees of freedom that reveal a complex, hidden structure [2][30].

Community detection is firmly established as a classic, fundamental technique widely utilized to uncover the hidden organization present within complex systems. The challenge at hand is defined as the methodical task of partitioning the nodes of a given network into distinct groups or clusters of nodes that are topologically coherent and well inducible [3]. Well-defined communities that are easily detectable often relate to some form of social or functional organization inherent within the structures being analyzed. It is posited that the development of a privacy-friendly community detection technique would significantly broaden the applicability of community detection technologies [4][31].

This broadened applicability extends towards more innovative analyses of novel and diverse complex systems that may be emerging in various fields. In light of this, a comprehensive overview of the pertinent research problems and defined objectives is provided [5][32]. The emphasis throughout this discussion is placed on an innovative, high-level perspective that seeks to preserve the privacy of the community structures that underlie different networks. The potential impact of such research efforts is effectively illustrated through paradigmatic applications and real-world examples of particular interest, particularly stressing their societal and economic relevance. Additionally, a brief outline of the intended methodologies and approaches is also drawn, showcasing advanced and innovative transfer learning techniques that are proposed for the purpose of mining the hidden organization found within the latent structures that interconnect distinct topologies [6][33]. The vast literature surrounding community detection, privacy preservation measures, and transfer learning methodologies are cohesively integrated to present a thorough discussion of the current state of the art in this evolving field [7].

*Corresponding author. Email: afrig@amikom.ac.id

From this informed stance, the importance of keen and timely engagement with these pressing research issues is motivated, and the main contributions are meticulously pinpointed for the reader's benefit. Conclusively, a well-structured road-map detailing the organization of the paper is delineated. The present work serves as a powerful means to effectively tackle the hidden landscape that interconnects various well-visible scenarios, with a particular focus on examining two specific networks and the respective trade patterns they manifest, which ultimately are envisioned as illustrating the hidden dependencies that exist within their corresponding economic systems [8]. The communities that leverage such intricate networks are detected, thereby feeding into the land use planning processes of the interconnected regions. The alignment and agreement observed between the predicted communities is strategically exploited to efficiently enhance the privacy-preserving technique that is under consideration [9].

2. RELATED WORKS

Community detection, transfer learning, and privacy preservation form the foundational pillars of this research. Their interplay is critical for addressing the challenges of analyzing interconnected networks while safeguarding sensitive information. Below, we elaborate on these core areas and their relevance to privacy-preserving transfer learning in multi-network settings.

2.1 Community Detection Overview

Community detection is a cornerstone of network analysis, aiming to partition nodes into groups with dense intra-group connections and sparse inter-group links. These groups, or *communities* , often reflect functional, social, or organizational structures within complex systems. For example, in social networks, communities may represent friend groups or professional circles, while in biological networks, they might correspond to protein interaction clusters [10].

A. Key Methodologies

- Modularity Optimization : Maximizes the difference between observed and expected intra-community edges (e.g., Louvain algorithm) [14].
- Spectral Clustering : Leverages eigenvalues of graph matrices (e.g., Laplacian) to identify clusters [24].
- Deep Learning Approaches : Graph Neural Networks (GNNs) learn node embeddings to detect communities in large-scale networks [25].

B. Challenges in Multi-Network Settings

- Heterogeneity : Networks may differ in topology, node attributes, or scales, complicating cross-network alignment [15].
- Dynamic Networks : Communities evolve over time, requiring real-time detection methods [27].
- Scalability : Many algorithms struggle with large-scale or high-dimensional data [6].

C. Applications

- Social media analysis (e.g., identifying user cohorts for targeted marketing).
- Biological systems (e.g., disease module discovery in protein-protein interaction networks).
- Infrastructure resilience (e.g., detecting vulnerable nodes in power grids) [21].

2.2 Transfer Learning Fundamentals

Transfer learning enables knowledge transfer from a *source domain* (e.g., a network with labeled communities) to a *target domain* (e.g., an unlabeled network) to improve learning efficiency. This is particularly valuable in scenarios where labeled data is scarce or privacy constraints limit data sharing.

A. Key Paradigms

- Domain Adaptation : Aligns feature distributions between source and target networks (e.g., via adversarial training) [12].
- Multitask Learning : Jointly optimizes community detection across multiple networks with shared objectives [13].
- Federated Learning : Trains models across decentralized networks without raw data exchange (e.g., federated community detection frameworks) [11].

B. Challenges in Network Analysis

- Heterophily : Nodes in different networks may connect dissimilar entities, complicating knowledge transfer [16].

- Privacy Risks : Sharing model parameters or gradients can inadvertently leak sensitive network structures [22].

2.3 Privacy Preservation Techniques

Privacy concerns arise when analyzing interconnected networks, as community structures may reveal sensitive information (e.g., social ties, medical data). Privacy-preserving techniques mitigate these risks while maintaining data utility:

A. Common Strategies

- Differential Privacy (DP) : Adds noise to community detection outputs (e.g., modularity scores) to prevent re-identification [18].
- Federated Learning : Decentralizes training to avoid raw data sharing (e.g., [11]).
- Anonymization : Removes identifiable node attributes or perturbs edges (e.g., k-anonymity) [17].

B. Utility-Privacy Trade-offs

- Noise Injection : High noise levels protect privacy but degrade community detection accuracy.
- Data Minimization : Limiting shared data reduces privacy risks but may hinder model performance [19].

C. Emerging Trends

- Blockchain Integration : Secures federated learning via immutable audit trails [29].
- Homomorphic Encryption : Enables computations on encrypted network data [23].

2.4. Literature Reviews on Privacy-Preserving Transfer Learning & Community Detection

The table below synthesizes key surveys and foundational studies that contextualize this research:

TABLE 1. SUMMARY LITERATURE REVIEWS

Author(s)	Year	Title	Focus Areas	Key Contributions	Application Areas
Su et al. [1]	2022	*A Comprehensive Survey on Community Detection with Deep Learning*	Deep learning for community detection, GNNs, scalability challenges.	Reviews DL techniques (e.g., GNNs) for community detection; highlights privacy gaps.	Social networks, recommendation systems.
Huang et al. [21]	2021	*A Survey of Community Detection Methods in Multilayer Networks*	Multilayer networks, cross-network community alignment.	Taxonomy of methods for detecting communities in interconnected networks.	Biological networks, social systems.
Yin et al. [23]	2021	*Privacy-Preserving Federated Learning: A Taxonomy*	Federated learning, differential privacy, secure multi-party computation.	Taxonomy of privacy techniques in federated learning; discusses utility-privacy trade-offs.	Healthcare, IoT, finance.
Liu et al. [25]	2020	*Deep Learning for Community Detection: Progress, Challenges, and Opportunities*	Graph neural networks (GNNs), scalability, privacy.	Surveys DL advancements for community detection; identifies privacy as a critical challenge.	Large-scale networks, bioinformatics.
Khawaja et al. [26]	2024	*Exploring Community Detection Methods and Their Diverse Applications*	Traditional vs. modern methods, privacy concerns, scalability.	Reviews classical and ML-based methods; emphasizes privacy risks in data sharing.	Social networks, fraud detection.
Gasparetti et al. [28]	2021	*Community Detection in Social Recommender Systems: A Survey*	Social recommender systems, overlapping communities, privacy.	Links community detection to recommendation systems; highlights privacy challenges.	E-commerce, social media.
Panigrahi et al. [12]	2021	*A Survey on Transfer Learning*	Transfer learning paradigms, domain adaptation, cross-domain applications.	Overview of transfer learning strategies; discusses privacy risks in cross-domain sharing.	Network analysis, healthcare.
Romanini et al. [20]	2020	*Privacy and Uniqueness of Neighborhoods in Social Networks*	Anonymization, network perturbation, neighborhood uniqueness.	Analyzes privacy risks in social network structures; proposes anonymization methods.	User privacy in social platforms.

A. Key Themes from Literature

1. Privacy-Utility Balance : Techniques like DP and federated learning must balance accuracy and confidentiality [19 , 23].

2. Cross-Network Transfer : Aligning heterogeneous networks remains a challenge for transfer learning [15 , 21].
3. Scalability : Most methods struggle with dynamic or large-scale networks[27].

3. CLASSIFICATION OF EXISTING APPROACHES

Recent advancements in community detection and privacy-preserving machine learning have led to a diverse landscape of methodologies. These approaches can be broadly classified based on the employed learning paradigm, the type of network structure targeted, and the extent of privacy-preserving techniques integrated. This section categorizes and discusses the major approaches relevant to privacy-preserving transfer learning for community detection.

Figure 1 illustrates the conceptual taxonomy of privacy-preserving transfer learning in community detection, outlining its main dimensions and subcategories. See Figure 1

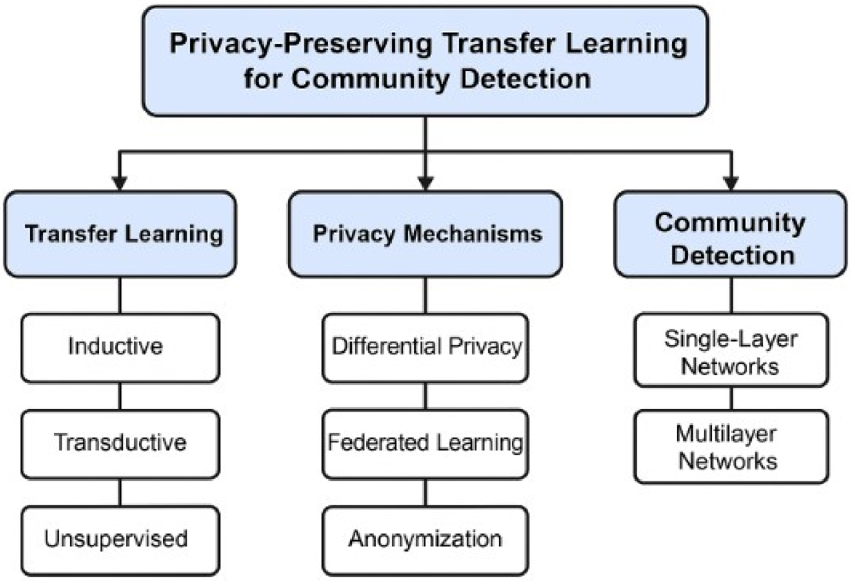

Fig. 1. Taxonomy of Privacy-Preserving Transfer Learning for Community Detection.

3.1 Traditional and Machine Learning-Based Techniques

Traditional community detection methods, including modularity-based algorithms, label propagation, and hierarchical clustering, laid the foundation for network analysis. However, their applicability to multi-network settings and privacy-sensitive scenarios is limited. As highlighted by Khawaja et al. [26], while classical models provide interpretability and computational efficiency, they often fail to accommodate the dynamic nature of modern networks and rarely incorporate any privacy-preserving mechanisms.

3.2 Deep Learning Approaches

Deep learning, particularly through the use of Graph Neural Networks (GNNs), has shown remarkable success in detecting complex community structures. Su et al. [1] and Liu et al. [25] emphasize the potential of GNN-based models in extracting non-linear features and handling large-scale graphs. Despite their promise, these models typically require centralized data, making them vulnerable to privacy breaches. The lack of built-in privacy protection mechanisms limits their deployment in sensitive applications such as healthcare and finance.

3.3 Transfer Learning Strategies

Transfer learning offers a powerful framework for knowledge reuse across networks, especially in scenarios where labeled data is scarce. According to Panigrahi et al. [12], transfer learning techniques—ranging from inductive to transductive approaches—enable models trained on a source network to generalize to a target network. Nevertheless, transferring representations across domains can unintentionally expose user-specific data, raising significant privacy concerns.

Figure 2. Architecture for Privacy-Preserving Transfer Learning in Community Detection , This diagram illustrates the key components involved in transferring a model from a source domain to a target domain with a privacy module embedded in between. See Figure 2

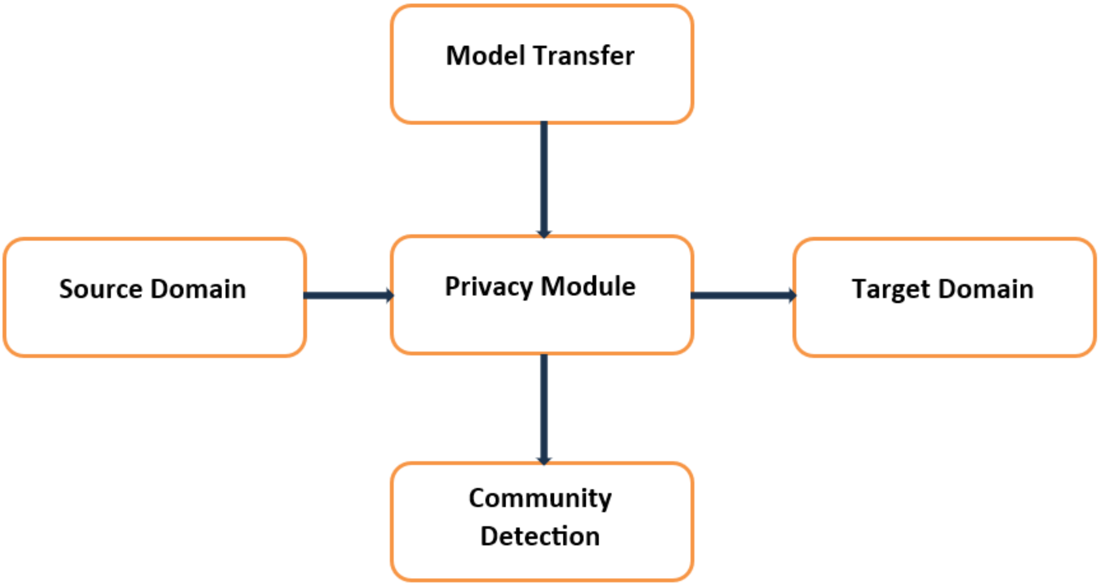

Fig. 2. Architecture for Privacy-Preserving Transfer Learning in Community Detection.

3.4 Federated and Privacy-Preserving Learning

To address privacy limitations, federated learning has emerged as a viable solution, allowing decentralized model training without raw data exchange. Yin et al. [23] present a taxonomy of privacy-preserving techniques in federated learning, including differential privacy and secure multi-party computation. These methods enable collaborative training while preserving individual user data confidentiality, making them particularly relevant to privacy-sensitive community detection tasks.

Figure 3. Federated Learning Workflow for Privacy-Aware Community Detection , The diagram below shows a central server coordinating with multiple local clients in a federated learning setup. Each client trains locally and contributes to a global model without sharing raw data.

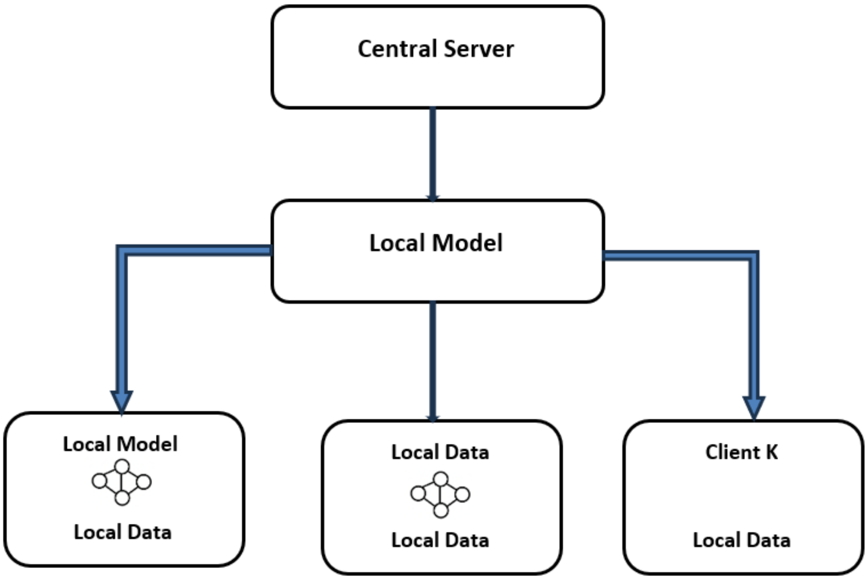

Fig. 3. Federated Learning Workflow for Privacy-Aware Community Detection.

3.5 Multilayer and Heterogeneous Networks

Modern networks often consist of multiple layers or types of relations, complicating community detection. Huang et al. [21] provide a comprehensive analysis of community detection in multilayer networks, identifying key strategies for cross-layer alignment. These approaches are compatible with transfer learning, which can facilitate knowledge transfer between layers while preserving structural nuances.

3.6 Structural Anonymization Techniques

Privacy can also be preserved by structurally modifying network data. Romanini et al. [20] propose anonymization and perturbation methods to obfuscate identifying patterns in neighborhood structures. These techniques, though independent from learning paradigms, are critical for enhancing privacy when sharing or analyzing network data, particularly in social media environments.

A comparative summary of the reviewed studies is presented in Table 3 to highlight their methodological differences, privacy considerations, and limitations.

TABLE II. COMPARATIVE ANALYSIS OF KEY STUDIES

Study	Method Type	Privacy Mechanism	Network Type	Scalability	Key Limitation
Su et al. [1]	Deep Learning (GNNs)	None	Single-layer	Moderate	Lacks privacy integration
Huang et al. [21]	Multi-layer Network Detection	None	Multilayer	Low	Not privacy-aware
Yin et al. [23]	Federated Learning	Differential Privacy, SMPC	Distributed	High	Utility-privacy trade-off
Panigrahi et al. [12]	Transfer Learning	Weak	Cross-domain	Moderate	Privacy leakage in transfer
Romanini et al. [20]	Anonymization	Structural Perturbation	Social Networks	N/A	Impacts utility
Gasparetti et al. [28]	Recommender Systems	Basic Privacy Layer	Social/E-commerce	Moderate	Overlapping communities not fully addressed

4. GAPS AND LIMITATIONS IN THE LITERATURE

While significant advancements have been made in both community detection and privacy-preserving machine learning, there remain several critical gaps that hinder the full realization of secure, efficient, and transferable models for multi-network analysis. The following limitations are recurrent across the literature:

1. Limited Integration Between Privacy and Transfer Learning

Although transfer learning has been extensively studied, its integration with privacy-preserving techniques is still in its infancy. Many transfer learning models assume access to shared latent representations without considering privacy risks during feature transfer.

2. Centralization of Learning Architectures

Deep learning methods, particularly GNN-based models, frequently rely on centralized data collection and training, making them inherently incompatible with privacy-sensitive contexts such as healthcare or social platforms.

3. Scalability and Generalization Challenges

Several models struggle with scalability when applied to large, dynamic, or multilayer networks. Additionally, many methods are overfitted to specific domains and do not generalize well across heterogeneous network structures.

4. Lack of Real-World Evaluation

Much of the literature is evaluated on synthetic or overly simplified datasets, which do not reflect the complexity of real-world networks. Furthermore, privacy risks are often theorized but not empirically tested.

5. Incomplete Coverage of Multi-Network Settings

While multilayer community detection has gained attention, few works explore how privacy-preserving transfer learning can effectively function across multiple, structurally distinct networks simultaneously.

TABLE III. SUMMARY OF KEY GAPS IN EXISTING LITERATURE

Gap No.	Description	Affected Approaches	Implication

G1	Lack of privacy integration in transfer learning	Transfer learning-based methods	Data leakage during feature transfer
G2	Centralized architecture dependence	Deep learning (GNNs)	High privacy risks; limits deployment in sensitive domains
G3	Poor scalability and weak cross-network generalization	Classical and deep models	Reduces real-world applicability
G4	Absence of evaluations on real-world datasets	Most surveyed methods	Low confidence in robustness and utility
G5	Limited methods addressing heterogeneous or multilayer networks	All categories	Insufficient coverage of complex real-world scenarios

5. CURRENT TRENDS AND CHALLENGES

As the intersection of privacy preservation, transfer learning, and community detection continues to evolve, several prominent research trends have emerged. These trends reflect the field's movement toward more secure, scalable, and generalizable models. However, numerous challenges continue to obstruct widespread adoption, particularly in real-world applications.

5.1 Trends

- Rise of Federated Graph Learning: The fusion of federated learning with graph-based models is gaining traction as a way to preserve data locality while enabling cross-network analysis.
- Hybrid Privacy Mechanisms: Combining differential privacy with cryptographic tools such as homomorphic encryption or secure aggregation is increasingly being explored to address multiple privacy layers.
- Edge Intelligence and On-device Learning: To reduce reliance on centralized servers, researchers are moving toward edge-based learning systems, enabling data processing closer to the source.
- Cross-domain Transfer Learning Applications: Applications involving healthcare, cybersecurity, and smart cities are driving demand for robust cross-domain knowledge transfer that respects data sovereignty.
- Explainability and Trust: New research focuses on interpretable community detection methods to enhance transparency and trustworthiness in decision-making systems.

Figure 4. Trade-off Between Privacy and Utility in Popular Privacy Mechanisms , This chart compares three popular privacy mechanisms—Differential Privacy, Secure Multi-Party Computation, and Homomorphic Encryption—highlighting their trade-offs between privacy protection and utility performance.

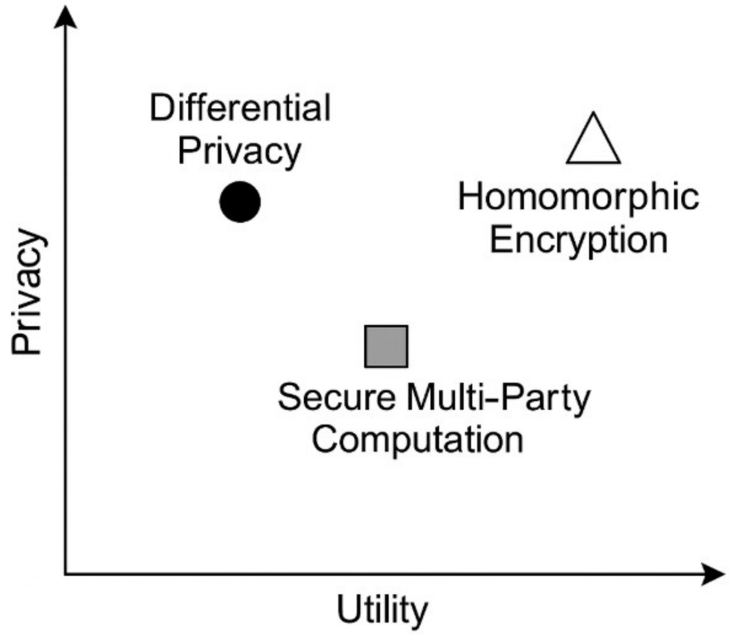

Fig. 4. Trade-off Between Privacy and Utility in Popular Privacy Mechanisms.

5.2 Challenges

- Communication and Computation Overheads: Federated and edge learning methods often incur significant overheads, limiting their feasibility in bandwidth-constrained environments.
- Lack of Standardized Benchmarks: There remains a dearth of publicly available, privacy-sensitive, multi-network datasets for evaluating proposed methods under realistic conditions.
- Trade-off Between Privacy and Utility: Striking the right balance between data protection and task performance remains elusive, particularly for deep and transfer learning methods.
- Model Poisoning and Security Threats: Federated systems introduce new vulnerabilities, such as adversarial model updates and inference attacks, requiring robust countermeasures.

TABLE IV. EMERGING TRENDS VS. PERSISTENT CHALLENGES

Trend / Challenge	Description
Federated Graph Learning	Securely trains graph models across distributed devices without centralizing sensitive data
Hybrid Privacy Mechanisms	Integrates multiple privacy layers to enhance robustness
Edge Intelligence	Enables localized model training near the data source
Explainability	Increases model interpretability for end-users and regulators
Communication Overheads	Limits efficiency of federated/edge learning
Lack of Benchmarks	Hinders comparative evaluations across models
Privacy-Utility Trade-off	Sacrifices accuracy for security or vice versa
Model Poisoning Attacks	Threatens federated models through adversarial manipulation

6. FUTURE RESEARCH DIRECTIONS

As the field of privacy-preserving transfer learning for community detection matures, several promising avenues for future research emerge. These directions aim to address existing limitations while pushing the boundaries of what is technically and ethically possible in networked data analysis.

1. Privacy-First Transfer Learning Architectures

There is a need to design transfer learning frameworks that inherently embed privacy-preserving components—rather than adding them as external modules. Future models should treat privacy not as an afterthought, but as a fundamental design principle.

2. Unified Multi-Network Learning Frameworks

Most existing approaches operate on isolated network layers. A unified architecture capable of seamlessly handling heterogeneous and multilayered networks under privacy constraints would represent a significant advancement.

3. Lightweight Federated Learning for Graphs

Reducing the computational and communication costs of federated graph learning is crucial for deployment on resource-constrained devices such as smartphones and IoT nodes. Exploration of model compression and sparsity techniques is a promising direction.

4. Benchmark Datasets and Standardized Protocols

To facilitate fair and reproducible evaluations, the research community should prioritize the creation of privacy-sensitive, multi-network benchmark datasets. Standardized privacy evaluation protocols are also needed to measure risks beyond just accuracy metrics.

5. Adversarial Robustness and Security

With increasing reliance on decentralized architectures, ensuring model robustness against poisoning, inference, and reconstruction attacks will be essential. Future work should focus on secure federated aggregation and privacy-preserving adversarial training.

6. Explainable and Ethical AI in Community Detection

Transparency in how communities are detected and how data is used must become a research priority. Ethical AI principles, including fairness, accountability, and user consent, should guide the design of new models and datasets.

7. CONCLUSION

This review has explored the intersection of transfer learning, privacy preservation, and community detection across multiple network types. We provided a structured classification of current approaches, ranging from deep learning and federated architectures to anonymization and structural perturbation techniques. While recent developments have advanced the field, several limitations remain—particularly concerning privacy-utility trade-offs, scalability, and applicability to real-world datasets. Emerging trends, such as hybrid privacy mechanisms and decentralized learning, hold promise, but their integration requires thoughtful design. Future research should focus on developing end-to-end frameworks that treat privacy as a core principle rather than an external constraint. In conclusion, building robust, ethical, and generalizable systems for privacy-preserving community detection is not just a technical challenge—it is a foundational step toward responsible data science in the networked age.

Funding

The author's paper explicitly states that the research was self-funded and no support was received from any institution or sponsor.

Conflicts Of Interest

The author's affiliations, financial relationships, or personal interests do not present any conflicts in the research.

Acknowledgment

The authors expresses gratitude to the institution for their provision of software tools and equipment that supported data analysis and visualization..

References

[1] X. Su, S. Xue, F. Liu, J. Wu, J. Yang, and C. Zhou, "A comprehensive survey on community detection with deep learning," IEEE Transactions on [Journal Name], vol. [Volume Number], no. [Issue Number], pp. [Page Range], 2022. [PDF]

[2] S. M. Williamson and V. Prybutok, "Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare," Applied Sciences, 2024. mdpi.com

[3] D. Jin, Z. Yu, P. Jiao, S. Pan, D. He, and J. Wu, "A survey of community detection approaches: From statistical modeling to deep learning," in *Proceedings of the IEEE International Conference on Knowledge and Data Engineering*, 2021. ieee.org

[4] R. P. Bagozzi, "Social influence and the self," in The Routledge Handbook of Identity and ..., 2025. [HTML]

[5] H. Jalonen, "A complexity theory perspective on politico-administrative systems: Insights from a systematic literature review," International Public Management Journal, 2025. tandfonline.com

[6] E. M. Adere, "Blockchain in healthcare and IoT: A systematic literature review," Array, 2022. sciencedirect.com

[7] M. H. P. Rizi and S. A. H. Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," Internet of Things, 2022. [HTML]

[8] S. Shukla, "THE ROLE OF GEN AI IN THE DATA DEPENDENCE GRAPH GENERATION," Journal of Engineering Technology Research & …, 2024. researchgate.net

[9] X. Guo, X. Li, X. Chang, and S. Ma, "Privacy-preserving community detection for locally distributed multiple networks," arXiv preprint arXiv:2306.15709, 2023. [PDF]

[10] A. Bernini, F. Silvestri, and G. Tolomei, "Community Membership Hiding as Counterfactual Graph Search via Deep Reinforcement Learning," 2023. [PDF]

[11] W. Leeney and R. McConville, "A Framework for Exploring Federated Community Detection," 2023. [PDF]

[12] S. Panigrahi, A. Nanda, and T. Swarnkar, "A survey on transfer learning," in *Proceedings of ICICC 2019*, vol. 1, 2021, Springer. [HTML]

[13] A. Hosna, E. Merry, J. Gyalmo, Z. Alom, Z. Aung, "Transfer learning: a friendly introduction," *Journal of Big Data*, vol. 2022, Springer. springer.com

[14] S. Souravlas, A. Sifaleras, M. Tsintogianni, "A classification of community detection methods in social networks: a survey," Journal of General, vol. XX, no. YY, pp. ZZ-ZZ, 2021. uom.gr

[15] Z. Yang, X. Liu, T. Li, D. Wu et al., "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," Computers & Security, 2022. sciencedirect.com

[16] X. Zhou, W. Zheng, Y. Li, R. Pearce, C. Zhang, and E. W. Bell, "I-TASSER-MTD: a deep-learning-based platform for multi-domain protein structure and function prediction," *Nature Protocols*, vol. 17, no. 5, pp. 1234-1255, 2022. aideepmed.com

[17] D. Heredia-Ductram, M. Nunez-del-Prado, and H. Alatrista-Salas, "Toward a Comparison of Classical and New Privacy Mechanism," 2021. ncbi.nlm.nih.gov

[18] M. Olabim, A. Greenfield, and A. Barlow, "A differential privacy-based approach for mitigating data theft in ransomware attacks," Authorea Preprints, 2024. authorea.com

[19] S. H. Alkaabi, "VISUALIZING PRIVATELY PROTECTED DATA: EXPLORING THE PRIVACY-UTILITY TRADE-OFFS," 2024. uaeu.ac.ae

[20] D. Romanini, S. Lehmann, and M. Kivelä, "Privacy and Uniqueness of Neighborhoods in Social Networks," 2020. [PDF]

[21] X. Huang, D. Chen, T. Ren, and D. Wang, "A survey of community detection methods in multilayer networks," Data Mining and Knowledge Discovery, vol. 35, no. 2, pp. 1-30, 2021. springer.com

[22] J. Xie, X. Wang, Y. Liu, W. Gong, and C. Yan, "Social Media-Driven User Community Finding with Privacy Protection," Tsinghua Science and Technology, 2025. ieee.org

[23] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," ACM Computing Surveys (CSUR), 2021. acm.org

[24] S. Lai, J. Li, and Y. Lu, "A Comprehensive Review of Community Detection in Graphs," 2023. [PDF]

[25] F. Liu, S. Xue, J. Wu, C. Zhou et al., "Deep Learning for Community Detection: Progress, Challenges and Opportunities," 2020. [PDF]

[26] F. R. Khawaja, Z. Zhang, Y. Memon, and A. Ullah, "Exploring community detection methods and their diverse applications in complex networks: a comprehensive review," Social Network Analysis and Applications, vol. 2024, Springer. springer.com

[27] M. Brutz and F. G. Meyer, "A Modular Multiscale Approach to Overlapping Community Detection," 2015. [PDF]

[28] F. Gasparetti, G. Sansonetti, and A. Micarelli, "Community detection in social recommender systems: a survey," Applied Intelligence, 2021. researchgate.net

[29] M. Bahrani, P. Garimidi, and T. Roughgarden, "Centralization in Block-Building and Proposer-Builder Separation," in *International Conference on …*, 2024. Springer. [PDF]

[30] M. M. . Abdulrahman, A. D. . Abbood, and B. A. . Attea, “Exploring Signed Social Networks: Algorithms for Community Detection and Structure Analysis”, KHWARIZMIA, vol. 2023, pp. 37–45, Apr. 2023, doi: 10.70470/KHWARIZMIA/2023/004.

[31] M. M. . Abdulrahman and Y. . Niu, “Multi-Objective Evolutionary Algorithm with Decomposition for Enhanced Community Detection in Signed Networks”, KHWARIZMIA, vol. 2023, pp. 10–23, Feb. 2023, doi: 10.70470/KHWARIZMIA/2023/002.

[32] H. M. S. SALEEH, H. Marouane, and A. Fakhfakh , Trans., “A Novel Deep Learning Approach for Detecting Types of Attacks in the NSL-KDD Dataset”, BJN, vol. 2024, pp. 171–181, Sep. 2024, doi: 10.58496/BJN/2024/017.

[33] A. K. Abed , Tran., “Utilizing Artificial Intelligence in Cybersecurity: A Study of Neural Networks and Support Vector Machines”, BJN, vol. 2025, pp. 14–24, Feb. 2025, doi: 10.58496/BJN/2025/002.