Unveiling the Veiled: Leveraging Deep Learning and Network Analysis for De-Anonymization in Social Networks

Rutba-Aman[1*], Rahnuma Tasmin[1], Poly Rani Ghosh[1]

Abstract

Online anonymity allows individuals to safeguard their personal information. It provides the freedom for anyone to express themselves without being concerned about censorship, discrimination, or retaliation. This pseudonym also provides opportunities for individuals to promote open discourse and diverse viewpoints. However, in today's digital age, this online anonymity has become a growing concern. Although the safeguarding of people's rights, the advancement of free speech, and the development of a more diverse and democratic online community all depend heavily on the anonymity of online users, there are risks as well, such as cyberbullying, harassment, and the propagation of false information. Because of their anonymity, predators, groomers, and other unscrupulous individuals may be able to take advantage of vulnerable individuals, especially children and adolescents. In order to trick victims into hazardous or abusive situations, adversaries can hide their identities. Deep learning and network analysis can be used to reveal the true identities of anonymous social media users in order to combat this. Deep learning algorithms are capable of analyzing a wide range of social network data, including user behavior, relationships, and content, in order to find patterns and correlations that can lead to the true identities of users that go anonymous. The proposed system includes examining network topology and group dynamics to identify potential anomalies and connections that could lead to de-anonymization. This paper proposes a novel module for de-anonymization integrating deep learning and network analysis in social networks.

Keywords: online anonymity, free speech, cyberbullying, de-anonymization, social networks.

Significance | Online anonymity enables free expression but raises concerns like cyberbullying; de-anonymization techniques aim to balance safety and openness online.

*Correspondence. Rutba-Aman, Department of Computer Science and Engineering, Primeasia University, Banani, Dhaka, Bangladesh
E-mail: tasnimul.islam@primeasia.edu.bd

Editor A. B. M. Abdullah, Ph. D., And accepted by the Editorial Board Feb 13, 2023 (received for review Jan 03, 2023)

Introduction

The widespread use of social networks in today's digital era has raised concerns about user privacy and anonymity (Sharad, 2016). While anonymity fosters freedom of expression, it also provides opportunities for malicious activities such as misinformation, cyberbullying, and harassment (Kourtis et al., 2021). The issue of online anonymity is complex, acting as both a protective measure and a tool for harm (Deanonymization: Blurring the Boundaries of Social Network Privacy, n.d.). In response, de-anonymization has become crucial, particularly in fields such as cybersecurity and law enforcement (Wondracek et al., 2010). For example, it aids in identifying cybercriminals, including those involved in financial fraud (Narayanan & Shmatikov, 2009). In addition to security, de-anonymization is valuable for research and marketing purposes by offering insights into user behavior (Lee et al., 2017). The balance

Author Affiliation.
[1] Department of Computer Science and Engineering, Primeasia University, Banani, Dhaka, Bangladesh

Please cite this article.
Rutba-Aman, Rahnuma Tasmin et al. (2023). Unveiling the Veiled: Leveraging Deep Learning and Network Analysis for De-Anonymization in Social Networks, Journal of Primeasia, 4(1), 1-6, 40042

between user privacy and anonymity remains challenging, with deep learning and network analysis being key in de-anonymization techniques (Jiang et al., 2021). Advanced algorithms such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are essential in identifying hidden patterns within large datasets (Gu et al., 2018). Furthermore, methods like community detection and centrality measures in network analysis provide structural insights into user relationships (Xie & Zheng, 2016).

By combining deep learning and network analysis, modern de-anonymization efforts aim to address malicious behavior on social networks while maintaining ethical standards for privacy (Sahoo & Gupta, 2021). The use of these innovative approaches continues to evolve, contributing to safer online environments (Goodfellow et al., 2020). The tension between maintaining privacy and preventing harmful exploitation of anonymity underscores the importance of ethical considerations in this research (Razavi-Far et al., 2022).

Materials and Methods

The study utilizes a combination of deep learning techniques and network analysis to address the issue of de-anonymization in social networks (Sharad, 2016; Wondracek et al., 2010; Narayanan & Shmatikov, 2009; Jiang et al., 2021). The data collection phase involves the use of datasets from various platforms like Twitter, Facebook, and Reddit, along with synthetic datasets created using models such as Barabási–Albert, Watts–Strogatz, and Erdős–Rényi (Kourtis et al., 2021; Wondracek et al., 2010). Ethical considerations were ensured, and all datasets were anonymized at the beginning of the analysis (Deanonymization: Blurring the Boundaries of Social Network Privacy, n.d.; Introduction to deanonymization and encryption, n.d.).

Feature extraction included key user attributes like demographics and interaction patterns, which were processed using techniques such as one-hot encoding and standardization (Mondal, Correa, & Benevenuto, 2020; Lee et al., 2017). The deep learning model was further enhanced by utilizing convolutional neural networks (Gu et al., 2018; Simonyan & Zisserman, 2014), with additional techniques drawn from recent advancements in anomaly detection (Ma et al., 2019; Khraisat et al., 2019; Wang et al., 2017). Finally, the evaluation of the de-anonymization model's performance was carried out, drawing on techniques from previous work in social network privacy and encryption (Narayanan & Shmatikov, 2009; Hsu, Liau, & Wang, 2014; Ying & Wu, 2011; Xie & Zheng, 2016).

Deep learning techniques were applied to uncover patterns in data and aid de-anonymization. Various models like Convolutional Neural Networks (CNNs) analyzed textual data, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models captured sequential behaviors (Yu et al., 2019). Generative Adversarial Networks (GANs) simulated real network activity (Goodfellow et al., 2020), and Siamese Networks compared user behaviors for identity similarities (Melekhov et al., 2016). Autoencoders reduced data dimensionality, highlighting key characteristics (Alalmaie et al., 2022). Hierarchical Attention Networks prioritized essential attributes for de-anonymization (Gu et al., 2017).

Network analysis methods complemented these models by analyzing structural and relational aspects of social networks (Narayanan & Shmatikov, 2009). Centrality measures helped identify prominent users (Sharad, 2016), while community detection grouped users with similar behaviors (Hsu et al., 2014). Link prediction estimated potential relationships (Fu et al., 2017), and homophily analysis identified shared traits aiding identity inference (Kourtis et al., 2021). Structural and temporal analyses examined network topology and user behavior over time (Wondracek et al., 2010), with role discovery identifying anonymous users through interaction patterns (Jiang et al., 2021).

Anonymity Score Calculation

A key component of the methodology was the development of an Anonymity Score Calculation Module, which measured the likelihood of a user's identity being revealed. This module integrated deep learning and network analysis outputs, assigning each user a score ranging from 0 (high de-anonymization risk) to 1 (high anonymity likelihood). The scores were computed based on interaction patterns, user attributes, and network centrality.

Model Evaluation

The performance of the proposed de-anonymization framework was evaluated using metrics such as accuracy, precision, recall, and ROC AUC. Visualization tools such as heatmaps and network graphs were employed to depict the distribution of anonymity scores and identify users or communities at higher de-anonymization risk. Finally, interpretability measures were developed to explain the factors influencing user anonymity and to ensure transparency in the model's decision-making process.

Ethical Considerations

Throughout the study, ethical concerns regarding user privacy and consent were meticulously addressed. The de-anonymization techniques were applied in accordance with data protection regulations, and efforts were made to minimize potential privacy infringements.

Results and Discussion

In our exploration of de-anonymization within social networks, we have employed deep learning techniques and network analysis to reveal hidden patterns of user behavior. By utilizing various datasets and advanced algorithms, we were able to develop a robust understanding of online anonymity and create methods for de-anonymizing users. This section provides a detailed examination of the findings, which emphasize both the effectiveness and the

potential ethical implications of these methods (Kumar & Kumar, 2013; Sharad, 2016; Wondracek et al., 2010; Narayanan & Shmatikov, 2009a).

Deep learning techniques, particularly Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Generative Adversarial Networks (GANs), have proven to be effective in detecting and analyzing user activities within social networks. Through rigorous analysis of user-generated textual data, interactions, and behavior patterns, these models were able to uncover previously hidden connections between anonymous users and real-world identities (Goodfellow et al., 2020; Jiang et al., 2021; Simonyan & Zisserman, 2014).

For instance, CNNs were able to analyze textual data from social media comments, recognizing patterns such as writing style, vocabulary usage, and sentiment. This enabled the identification of users who attempt to remain anonymous behind pseudonyms (Deanonymization, n.d.; Lee et al., 2017). RNNs were particularly useful for processing user interaction sequences over time, revealing temporal behavior patterns that are unique to specific users (Xie & Zheng, 2016; Ma et al., 2019). LSTM networks, designed to handle long-term dependencies, captured the recurring behavioral trends of anonymous users, which further contributed to de-anonymization (Yu et al., 2019; Wang et al., 2017).

In our experiments, we used GANs to generate synthetic user data, simulating anonymous behavior in social networks. The adversarial learning process allowed us to improve the detection of fake or anonymous accounts (Goodfellow et al., 2020), while also refining our models' ability to distinguish real users from synthetic ones (Razavi-Far et al., 2022). Siamese networks and deep autoencoders were utilized to extract user profile embeddings (Melekhov et al., 2016; Guo et al., 2017), providing a more refined understanding of similarities between user accounts (Chicco, 2021). This enabled us to compute the likelihood of de-anonymizing users based on their interaction patterns (Bo et al., 2019; Alalmaie et al., 2022).

Network analysis methods have complemented the deep learning models by focusing on the structural relationships within social networks. Through the use of centrality measures, community detection, and link prediction, we were able to gain insights into how users interact within the network and identify central players (Sharad, 2016; Kourtis et al., 2021; Narayanan & Shmatikov, 2009). Centrality measures like degree and betweenness centrality helped us identify the most influential users within the network (Narayanan & Shmatikov, 2009; Wondracek et al., 2010). These users were often highly connected and more likely to be involved in illicit activities, making them prime targets for de-anonymization efforts (Jiang et al., 2021; Narayanan & Shmatikov, 2009). Community detection algorithms allowed us to identify clusters of users with similar interests and connections, further narrowing down our targets for de-anonymization (Lee et al., 2017; Fu et al., 2017).

Link prediction techniques were used to predict the likelihood of future interactions between users, revealing hidden connections between anonymous and known individuals (Xie & Zheng, 2016; Ying & Wu, 2011). This was particularly useful in identifying users who may have been attempting to evade detection by limiting their social interactions (Sharad, 2016; Fu et al., 2017).

In combination, these network analysis methods significantly improved the ability to uncover anonymous users, especially when paired with deep learning models that could analyze user behavior at a more granular level (Kourtis et al., 2021; Mondal et al., 2020; Wang et al., 2017).

The choice of dataset was crucial to the performance of both deep learning and network analysis models (Sharad, 2016; Kourtis et al., 2021; Narayanan & Shmatikov, 2009). The research utilized datasets from various online social networks such as Twitter, Facebook, and Reddit (Wondracek et al., 2010; Deanonymization: Blurring the Boundaries of Social Network Privacy, n.d.; Lee et al., 2017), along with synthetic datasets generated by models like Barabási–Albert and Watts–Strogatz (Goodfellow et al., 2020; Razavi-Far et al., 2022). The synthetic datasets allowed testing of de-anonymization techniques under controlled conditions (Jiang et al., 2021; Fu et al., 2017; Ma et al., 2019). These datasets provided a wide range of social interactions and behavioral patterns, which enhanced model training and generalization (Narayanan & Shmatikov, 2009; Mondal et al., 2020).

Additionally, the Anonymity Score Calculation module was central to the evaluation of the system (Hsu et al., 2014; Xie & Zheng, 2016; Gross & Acquisti, 2005), with the module assessing features such as user attributes and interaction patterns to compute anonymity risk scores (Ying & Wu, 2011; Liu et al., 2008; Qian et al., 2019). Lower scores were associated with a higher risk of de-anonymization (Korolova et al., 2008; Arachchige et al., 2019; Xu et al., 2020). The analysis further emphasized the importance of robust privacy-preserving methods in social network research (Jiang et al., 2021; Wang et al., 2017; Sahoo & Gupta, 2021).

To evaluate the performance of our models, we utilized standard metrics such as accuracy, precision, recall, and ROC AUC. The models consistently achieved high accuracy rates, with de-anonymization success rates exceeding 85% for some datasets (Narayanan & Shmatikov, 2009; Sharad, 2016; Wondracek et al., 2010). Visualization tools, such as heatmaps and graphs, were used to analyze the distribution of anonymity scores across the network, helping to identify groups of users who were at risk of being de-anonymized (Lee et al., 2017; Jiang et al., 2021).

While the results of our study demonstrate the effectiveness of deep learning and network analysis techniques for de-anonymizing users, the ethical implications of such actions must be carefully

considered (Kourtis et al., 2021; Xie & Zheng, 2016; Hsu et al., 2014). The potential for misuse of these techniques, particularly in violating user privacy, cannot be ignored (Narayanan & Shmatikov, 2009). It is imperative that any application of de-anonymization techniques follows strict ethical guidelines, ensuring that user consent and data privacy are respected (Gross & Acquisti, 2005; Mondal et al., 2020).

Researchers and law enforcement agencies must strike a balance between the need for de-anonymization to prevent illegal activities and the protection of users' rights to privacy (Fu et al., 2017; Ying & Wu, 2011). As such, robust safeguards must be implemented to prevent the abuse of de-anonymization technologies (Gu et al., 2018; Wang et al., 2017).

Conclusion

The rise of social networks has heightened the demand for privacy and anonymity, but this has also allowed for malicious activities such as cyberbullying and fraud. De-anonymization, which aims to uncover hidden identities in these networks, has become an essential research area. Deep learning techniques, such as CNNs, RNNs, and GANs, along with network analysis approaches like centrality measures and community detection, offer powerful tools to reveal user identities and combat online abuse. However, ethical concerns regarding privacy must be addressed. By calculating anonymity scores, these methods help identify users at higher risk of de-anonymization, enabling better resource allocation for investigation. Ultimately, while de-anonymization can enhance security and protect intellectual property, it is crucial to balance these efforts with the need to safeguard user privacy and maintain ethical standards.

Author contributions

R.A. conceptualized the project, developed the methodology, conducted formal analysis, and drafted the original writing. R.T. contributed to the methodology, conducted investigations, provided resources, visualized the data. P.R.G. contributed to the reviewing and editing of the writing.

Acknowledgment

Author thanks the Department of Computer Science and Engineering, Primeasia University, Banani, Dhaka, Bangladesh

Competing financial interests

The authors have no conflict of interest.

References

Alalmaie, A. Z., Nanda, P., & He, X. (2022, December). Zero Trust-NIDS: Extended multi-view approach for network trace anonymization and auto-encoder CNN for network intrusion detection. In 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 449-456). IEEE.

Arachchige, P. C. M., Bertok, P., Khalil, I., Liu, D., Camtepe, S., & Atiquzzaman, M. (2019). Local differential privacy for deep learning. IEEE Internet of Things Journal, 7(7), 5827-5842.

Bayot, R. K., & Gonçalves, T. (2018). Age and gender classification of tweets using convolutional neural networks. In Machine Learning, Optimization, and Big Data: Third International Conference, MOD 2017, Volterra, Italy, September 14–17, 2017, Revised Selected Papers (Vol. 3, pp. 337-348). Springer International Publishing. https://doi.org/10.1007/978-3-319-73603-7_27

Bo, H., Ding, S. H., Fung, B., & Iqbal, F. (2019). ER-AE: Differentially private text generation for authorship anonymization. arXiv Preprint arXiv:1907.08736.

Chicco, D. (2021). Siamese neural networks: An overview. Artificial Neural Networks, 73-94.

Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2015). Analyzing Android encrypted network traffic to identify user actions. IEEE Transactions on Information Forensics and Security, 11(1), 114-125. https://doi.org/10.1109/TIFS.2015.2482927

Deanonymization: Blurring the Boundaries of Social Network Privacy. (n.d.). https://fastercapital.com/content/Deanonymization--Blurring-the-Boundaries-of-Social-Network-Privacy.html

Faralli, S., Stilo, G., & Velardi, P. (2015). Large scale homophily analysis in Twitter using a twixonomy. In IJCAI International Joint Conference on Artificial Intelligence (Vol. 2015, pp. 2334-2340). International Joint Conferences on Artificial Intelligence.

Fu, X., Hu, Z., Xu, Z., Fu, L., & Wang, X. (2017, December). De-anonymization of networks with communities: When quantifications meet algorithms. In GLOBECOM 2017 - 2017 IEEE Global Communications Conference (pp. 1-6). IEEE.

Geetha, R., Karthika, S., & Kumaraguru, P. (2021). Tweet-scan-post: A system for analysis of sensitive private data disclosure in online social media. Knowledge and Information Systems, 63(9), 2365-2404. https://doi.org/10.1007/s10115-021-01513-7

Gleize, M., Shnarch, E., Choshen, L., Dankin, L., Moshkowich, G., Aharonov, R., & Slonim, N. (2019). Are you convinced? Choosing the more convincing evidence with a Siamese network. arXiv preprint arXiv:1907.08971. https://arxiv.org/abs/1907.08971

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2020). Generative adversarial networks. Communications of the ACM, 63(11), 139-144.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80).

Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., ... & Chen, T. (2018). Recent advances in convolutional neural networks. Pattern Recognition, 77, 354-377.

Gu, X., Luo, W., Ryoo, M. S., & Lee, Y. J. (2020, August). Password-conditioned anonymization and deanonymization with face identity transformers. In European Conference on Computer Vision (pp. 727-743). Cham: Springer International Publishing.

Guo, Q., Feng, W., Zhou, C., Huang, R., Wan, L., & Wang, S. (2017). Learning dynamic siamese network for visual object tracking. In Proceedings of the IEEE International Conference on Computer Vision (pp. 1763-1771). https://doi.org/10.1109/ICCV.2017.194

Havinga, I., Marcos, D., Bogaart, P., Massimino, D., Hein, L., & Tuia, D. (2023). Social media and deep learning reveal specific cultural preferences for biodiversity. People and Nature, 5(3), 981-998.

Hernandez, N., Rahman, M., Recabarren, R., & Carbunar, B. (2018, October). Fraud de-anonymization for fun and profit. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 115-130).

Himelboim, I., Sweetser, K. D., Tinkham, S. F., Cameron, K., Danelo, M., & West, K. (2016). Valence-based homophily on Twitter: Network analysis of emotions and political talk in the 2012 presidential election. New Media & Society, 18(7), 1382-1400.

Hsu, T. S., Liau, C. J., & Wang, D. W. (2014). A logical framework for privacy-preserving social network publication. Journal of Applied Logic, 12(2), 151-174.

Introduction to deanonymization and encryption. (n.d.). https://fastercapital.com/topics/introduction-to-deanonymization-and-encryption.html

Jiang, H., Gao, Y., Sarwar, S. M., GarzaPerez, L., & Robin, M. (2021, December). Differential privacy in privacy-preserving big data and learning: Challenge and opportunity. In Silicon Valley Cybersecurity Conference (pp. 33-44). Springer International Publishing.

Jiang, H., Pei, J., Yu, D., Yu, J., Gong, B., & Cheng, X. (2021). Applications of differential privacy in social network analysis: A survey. IEEE Transactions on Knowledge and Data Engineering, 35(1), 108-127.

Jiang, H., Yu, J., Cheng, X., Zhang, C., Gong, B., & Yu, H. (2021). Structure-attribute-based social network deanonymization with spectral graph partitioning. IEEE Transactions on Computational Social Systems, 9(3), 902-913.

KDD 2023 TOC. (2023, August). https://kdd.org/kdd2023/wp-content/uploads/2023/08/toc.html

Khanam, K. Z., Srivastava, G., & Mago, V. (2023). The homophily principle in social network analysis: A survey. Multimedia Tools and Applications, 82(6), 8811-8854.

Khazbak, Y., & Cao, G. (2017, October). Deanonymizing mobility traces with co-location information. In 2017 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1), 1-22.

Korolova, A., Motwani, R., Nabar, S. U., & Xu, Y. (2008, October). Link privacy in social networks. In Proceedings of the 17th ACM conference on Information and knowledge management (pp. 289-298).

Kourtis, M. A., Oikonomakis, A., Papadopoulos, D., Xylouris, G., & Chochliouros, I. P. (2021, December). Leveraging deep learning for network anomaly detection. In 2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 1-6). IEEE.

Kumar, G., & Kumar, K. (2013). Design of an evolutionary approach for intrusion detection. The Scientific World Journal, 2013.

Lane, N. D., Xie, J., Moscibroda, T., & Zhao, F. (2012, November). On the feasibility of user de-anonymization from shared mobile sensor data. In Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones (pp. 1-5).

Lee, W. H., Liu, C., Ji, S., Mittal, P., & Lee, R. B. (2017, October). Blind de-anonymization attacks using social networks. In Proceedings of the 2017 on Workshop on Privacy in the Electronic Society (pp. 1-4).

Li, K., Lu, G., Luo, G., & Cai, Z. (2020, October). Seed-free graph de-anonymization with adversarial learning. In Proceedings of the 29th ACM International Conference on Information & Knowledge Management (pp. 745-754). https://doi.org/10.1145/3340531.3411897

Lindemann, B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). A survey on anomaly detection for technical systems using LSTM networks. Computers in Industry, 131, 103498. https://doi.org/10.1016/j.compind.2021.103498

Liu, L., Wang, J., Liu, J., & Zhang, J. (2008). Privacy preserving in social networks against sensitive edge disclosure. Technical Report CMIDA-HiPSCCS 006-08, Department of Computer Science, University of Kentucky.

Luceri, L., Braun, T., & Giordano, S. (2019). Analyzing and inferring human real-life behavior through online social networks with social influence deep learning. Applied Network Science, 4(1), 1-25.

Ma, C., Du, X., & Cao, L. (2019). Analysis of multi-types of flow features based on hybrid neural network for improving network anomaly detection. IEEE Access, 7, 148363-148380.

Mao, J., Tian, W., Jiang, J., He, Z., Zhou, Z., & Liu, J. (2018). Understanding structure-based social network de-anonymization techniques via empirical analysis. EURASIP Journal on Wireless Communications and Networking, 2018, 1-16.

Mao, J., Tian, W., Jiang, J., He, Z., Zhou, Z., & Liu, J. (2018). Understanding structure-based social network de-anonymization techniques via empirical analysis. EURASIP Journal on Wireless Communications and Networking, 2018, 1-16.

Melekhov, I., Kannala, J., & Rahtu, E. (2016, December). Siamese network features for image matching. In 2016 23rd International Conference on Pattern Recognition (ICPR) (pp. 378-383). IEEE. https://doi.org/10.1109/ICPR.2016.7899667

Mondal, M., Correa, D., & Benevenuto, F. (2020, July). Anonymity effects: A large-scale dataset from an anonymous social media platform. In Proceedings of the 31st ACM Conference on Hypertext and Social Media (pp. 69-74).

Narayanan, A., & Shmatikov, V. (2009). De-anonymizing social networks. arXiv preprint arXiv:0903.3276.

Narayanan, A., & Shmatikov, V. (2009, May). De-anonymizing social networks. In 2009 30th IEEE Symposium on Security and Privacy (pp. 173-187). IEEE.

Narayanan, A., & Shmatikov, V. (2009, May). De-anonymizing social networks. In 2009 30th IEEE Symposium on Security and Privacy (pp. 173-187). IEEE.

Ombabi, A. H., Lazzez, O., Ouarda, W., & Alimi, A. M. (2017, November). Deep learning framework based on Word2Vec and CNN for users interests classification. In 2017 Sudan Conference on Computer Science and Information Technology (SCCSIT) (pp. 1-7). IEEE. https://doi.org/10.1109/SCCSIT.2017.8293031

Qian, J., Li, X. Y., Jung, T., Fan, Y., Wang, Y., & Tang, S. (2019). Social network de-anonymization: More adversarial knowledge, more users re-identified?. ACM Transactions on Internet Technology (TOIT), 19(3), 1-22.

Qian, J., Li, X. Y., Zhang, C., Chen, L., Jung, T., & Han, J. (2017). Social network de-anonymization and privacy inference with knowledge graph model. IEEE Transactions on Dependable and Secure Computing, 16(4), 679-692.

Qian, J., Li, X. Y., Zhang, C., Chen, L., Jung, T., & Han, J. (2017). Social network de-anonymization and privacy inference with knowledge graph model. IEEE Transactions on Dependable and Secure Computing, 16(4), 679-692.

Razavi-Far, R., Ruiz-Garcia, A., Palade, V., & Schmidhuber, J. (Eds.). (2022). Generative adversarial learning: Architectures and applications. Springer International Publishing.

Sahoo, S. R., & Gupta, B. B. (2021). Multiple features based approach for automatic fake news detection on social networks using deep learning. Applied Soft Computing, 100, 106983.

Sharad, K. (2016). Learning to de-anonymize social networks (No. UCAM-CL-TR-896). University of Cambridge, Computer Laboratory.

Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.

Sopuru, J., Sari, A., & Akkaya, M. (2019). Modeling a malware detection and categorization system based on seven network flow-based features. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(7).

Su, J., Shukla, A., Goel, S., & Narayanan, A. (2017, April). De-anonymizing web browsing data with social networks. In Proceedings of the 26th International Conference on World Wide Web (pp. 1261-1269).

Umar, P., Akiti, C., Squicciarini, A., & Rajtmajer, S. (2021). Self-disclosure on Twitter during the COVID-19 pandemic: A network perspective. In Machine Learning and Knowledge Discovery in Databases. Applied Data Science Track: European Conference, ECML PKDD 2021, Bilbao, Spain, September 13–17, 2021, Proceedings, Part IV (pp. 271-286). Springer International Publishing.

Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2017). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access, 6, 1792-1806.

Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2017, January). Malware traffic classification using convolutional neural network for representation learning. In 2017 International Conference on Information Networking (ICOIN) (pp. 712-717). IEEE.

Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010, May). A practical attack to de-anonymize social network users. In 2010 IEEE Symposium on Security and Privacy (pp. 223-238). IEEE.

Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010, May). A practical attack to de-anonymize social network users. In 2010 IEEE Symposium on Security and Privacy (pp. 223-238). IEEE.

Wu, X., Hu, Z., Fu, X., Fu, L., Wang, X., & Lu, S. (2018, April). Social network de-anonymization with overlapping communities: Analysis, algorithm and experiments. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications (pp. 1151-1159). IEEE.

Xie, Y., & Zheng, M. (2016). A differentiated anonymity algorithm for social network privacy preservation. Algorithms, 9(4), 85.

Xu, Y., Meng, X., Li, Y., & Xu, X. (2020). Research on privacy disclosure detection method in social networks based on multi-dimensional deep learning. Computers, Materials & Continua, 62, 137-155.

Ying, X., & Wu, X. (2011). On link privacy in randomizing social networks. Knowledge and Information Systems, 28, 645-663.

Yu, Y., Si, X., Hu, C., & Zhang, J. (2019). A review of recurrent neural networks: LSTM cells and network architectures. Neural Computation, 31(7), 1235-1270. https://doi.org/10.1162/neco_a_01199

Zhang, X., Qi, C., Wei, X., & He, W. (2023). Identifying intimacy of self-disclosure: A design based on social penetration theory and deep learning. Applied Soft Computing, 100, 106983.

Zhou, J., Hu, C., Chi, J., Wu, J., Shen, M., & Xuan, Q. (2022). Behavior-aware account de-anonymization on Ethereum interaction graph. IEEE Transactions on Information Forensics and Security, 17, 3433-3448.