A Conceptual Anonymity Model to Ensure Privacy for Sensitive Network Data

Conference Paper · December 2021

DOI: 10.1109/ETCCE54784.2021.9689791

6 authors, including:

N H M Arafat
University of Toledo
4 PUBLICATIONS **5** CITATIONS
SEE PROFILE

Abu Jafar Md Muzahid
Universiti Malaysia Pahang
20 PUBLICATIONS **78** CITATIONS
SEE PROFILE

Saydul Akbar Murad
Universiti Malaysia Pahang
18 PUBLICATIONS **50** CITATIONS
SEE PROFILE

2021 International Conference on Emerging Technology in Computing, Communication and Electronics (ETCCE)

2021 Emerging Technology in Computing, Communication and Electronics (ETCCE) | 978-1-6654-8364-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ETCCE54784.2021.9689791

A Conceptual Anonymity Model to Ensure Privacy for Sensitive Network Data

N H M Arafat*
Dept. of Computer Science and Technology
Henan Polytechnic University
454003, Jiaouo, Henan, P.R. China
arafat.nhm@gmail.com

Md Ileas Pramanik
Dept. of Computer Science and Engineering
Begum Rokeya University
5404, Rangpur, Bangladesh
ileas.cse@brur.ac.bd

Abu Jafar Md Muzahid
Faculty of Computing
Universiti Malaysia Pahang
26600, Pahang, Malaysia
mrumi98@gmail.com

Bibo Lu
Dept. of Computer Science and Technology
Henan Polytechnic University
454003, Jiaouo, Henan, P.R. China
lubibo@hpu.edu.cn

Sumaiya Jahan
Dept. of Computer Science and Technology
Henan Polytechnic University
454003, Jiaouo, Henan, P.R. China
sumaiya2110jahan@gmail.com

Saydul Akbar Murad
Faculty of Computing
Universiti Malaysia Pahang
26600, Pahang, Malaysia
saydulakbarmurad@gmail.com

***Abstract*—In today's world, a great amount of people, devices, and sensors are well connected through various online platforms, and the interactions between these entities produce massive amounts of useful information. This process of data production and sharing appears to be on the rise. The growing popularity of this industry, as well as the required development of data sharing tools and technology, pose major threats to an individual's sensitive information privacy. These privacy-related issues may elicit a regularly strong negative reaction and restrain further organizational invention. Researchers have identified the privacy implications of large data collections and contributed to the preservation of data from unauthorised exposure to solve the challenge of information privacy. However, the majority of privacy strategies concentrate solely on traditional data models, such as micro-data. The academe and industry are paying more attention to network data privacy challenges. In this paper, we offer (ℓ, k)-anonymity, a novel privacy paradigm for network data that focuses on maintaining the privacy of both node and link information. Here, original network data will turn to attribute generalization nodes through a complex process, where several algorithms, clustering, node generalization, link generalization and ℓ-diversification will be applied. As a result, (ℓ, k)-anonymous network will be generated and will filter original network data to ensure publishable (ℓ, k)-anonymize data. Hopefully, this anonymity model will have a stronger role against homogeneity attacks of intruders, which will prevent the unauthorized disclosure of sensitive network data for several areas, such as - health sector. This model will also be cost effective and data loss will be controlled using two different ways.**

***Index Terms*—Privacy, k-anonymity, Network-data, Data publishing, Information Loss.**

I. Introduction

With the advancement of computational technology, a massive amount of individual data is generated by various people and collected by numerous organisations on a regular basis, providing tremendous value to our society. These data generate a big data volume, with the majority of datasets being network data. Sociologists and computer scientists agree that social network communication has recently become a very frequent contact tool around the world, and that trend will continue in the future [1], [2]. Because of the emergence of various social networks, data sets have evolved from basic traditional data models to complex ones. Entities and relationships between them indicate social network users. Identifiers, quasi-identifiers, and sensitive information are used to represent entities or nodes, while relationships are used to indicate connections or links [3]. These large datasets also present severe privacy problems, resulting in a regulatory backlash and hindered organizational innovation. Furthermore, social network research focuses on uncovering structures that indicate user relationships [4], [5]. In the last two decades, researchers have looked into privacy preserving approaches to meet the difficulty of social network privacy. Furthermore, research on salable methods for preserving privacy using social network data is gaining traction in academia and industry [6]. The development of effective and efficient solutions for varied data models [7] is a growing trend in data privacy research. Because of the Health Insurance Portability and Accountability Act, the majority of present privacy work focuses on the healthcare domain [8]. However, privacy anxieties have been expanded

to other areas, where data has a variety of characteristics; these areas include location-based services [9], genomic data [10], data streams [11], and social networks [12]–[15]. The goal of privacy-preserving social network analysis is to extract usable business intelligence information from the data of social network in order to ensure that personal information and its relationships are protected in a systematic manner [16], [17]. However, privacy in social networks remains in infancy stage, and applied privacy methods are yet to be developed. A brief overview of existing privacy methods in social networks is stated in the related work section [18]. In this study, we will introduce a new anonymization approach for network data. The key concerns here are:

1. To preserve network data privacy, we mask node information according to the ℓ-diversity model, where sensitive information is ℓ-diverse in any cluster.
2. Relationships are anonymized using the k- anonymity model, where relations are indistinguishable with at least $(k-1)$ other relations in any cluster.

Therefore, we present our privacy approach as the (ℓ, k)-anonymity model. Our anonymization method tries to minimize data distortion in network data, both the quasi-identifiers and sensitive attribute data related to the nodes. As data distortion minimization is very essential to preserve big data privacy with maximum utility, we believe the future extension of this work can contribute in big data privacy. In this research work structural information is associated with the relationships. In our proposed approach, we use generalization and suppression operation-like study [19] to anonymize node information. We apply link generalization approach, where no new links are added into or no existing links are removed from the network datasets, like one other described previous work [20]. Although our proposed approach incorporates some ideas that have already been exposed in related studies, it is novel in several aspects. We extended anonymity approaches [12], [13], [18] to ℓ-diversity approach. Moreover, we planned a set of algorithms with respect to the ideas of top–down specification, local re-coding approaches demonstrated in this study. We also assume a model containing more abundant data than structural information related to social network. Additionally, we will cluster the network and then diversify the nodes via cluster collapsing. Our clustering information process assures ℓ-diversification to the node information and k-anonymization to the nodes' relationships.

The rest of this paper is presented as follows. Section II describes the related works, Section III introduces the conceptual framework with intuition of our proposed method and Section IV presents the conclusion and future work.

II. Related Works

Until recently, the state-of-art on privacy preservation considered the micro-data in which each row represents individual record, and the columns represent attributes [21]–[24]. However, micro-data in the actual world are almost entirely relational in nature, and they are linked to one another and to external information. To enable the introduction of multiple social media, a massive number of people, devices, and sensors [25], [26] are connected via digital networks, and the interactions between these entities generate tremendous amounts of important relational data that enable enterprises to innovate and expand. Besides, the data sharing through social media also raises serious privacy concerns that may cause a regulatory backlash and hinder further organizational innovation [27]. Though, over past two decades, researchers have explored different privacy preserving methodologies to address the challenge of information privacy [28]. The investigation in social network privacy is very recent. Thus, many questions still remain. Now, we briefly present the short overview of the existing literature on social network privacy approaches.

Backstrom et al. studied social network data that have been naively anonymized [29]. Here, intruders' strategy is to develop a highly distinguishable subgraph with edges to a set of target nodes and then to extract the subgraph in the released network. This study plans an algorithm that constructs a distinguished subgraph with high probability. *Hay et al.* proposed another novel anonymization technique based on perturbing the network to assess the privacy risk of sharing anonymized network data [12]. These network anonymization approaches are very close to our study. Moreover, another closest privacy approach is proposed by *Zheleva and Geetor*. The authors consider the problem where associations between different distinct nodes in a network must be secured, and they named this problem as relationships re-identification [20], [30]. This work follows two steps to anonymize network data. First, de-identified nodes' information to achieve k-anonymity or t-closeness [23], without considering relationships between the network nodes. Then, anonymize the network's structure by controlled edge removal or addition in different flavours, each with different success likelihoods. Another similar work is presented by *Campan and Truta*, where a greedy approach uses to anonymize a social network [31]. Their anonymization approach also functions in two steps. In first step, generalized attribute data associated to the nodes which is named as node generalization, and in second step generalize relationships among nodes which is called edge generalization [18], [32]. Campan's privacy model incorporates the k-anonymity model presented by *Hay et al.* [13]. describes k-anonymity with respect to the similarity of neighbourhoods, where every node has no less than k candidate nodes from which it is hard to be distinguished [12], [13]. To achieve k-anonymity property, network data faces some random edge addition and deletion operations. In this privacy approach, nodes are defined by a single identifier, no QI attributes are considered, and all edges are of unique type.

Another similar study was conducted by *Zhou and Pei*, where they consider the nodes to be labelled (having one attribute that can be treated as a QI attribute), and that only the near neighbourhoods (1-radius neighbourhood) of some target records are entirely known to an intruder [33]. Their privacy approach nodes are generalized through adding extra edges to create similar neighbourhoods. Their approach guarantees that no intruders can identify any individual with

a confidence higher than *1/k*, though they have the knowledge of 1-neigborhood. Using the concept of realizability of degree sequence, *Liu and Terzi* proposed another network data anonymization method, where a network is treated as k-degree anonymous if for every node v, at least $k-1$ other nodes exists in the network with the same degree as v [14]. Another approach was introduced by *Ying and Wu* where sensitive link and relationship protection were discussed. They identify the change of graph property with respect to randomly adding and removing edges. Particularly, they focused on the change due to the eigenvalues (spectrum) of the network. The authors additionally discovered how the randomized network could be exploited by the intruders to extract information related to the presence of particular relationships [34], [35].

Our work is related to the above studies. However, in our proposed approach, we used generalization and suppression operation for anonymizing node information similar with the study of *Sweeney* [19]. For relationship anonymization, we applied link generalization approach, where no new links are added into or no existing links are removed from the social network datasets similar to the one described by *Zheleva and Getoor* [20]. Finally, we developed a social network clustering approach followed by node diversification through cluster collapsing. Our clustering mechanism guarantees ℓ-diversification to the nodes' information and k-anonymization to the link information.

III. Conceptual Framework

In this study, we considered a network as an undirected graph $G = (N, L)$. Let graph G be an original graph and G^* be the publishable anonymous graph. Graph G contains some node and link information about a set of individuals existing in the network. At the time of network data anonymization, we have to anonymize node information (micro-data) and relationship information (link data). Each network is presented by some attributes and links. The attributes of a node are classified into three major categories: identifier, quasi-identifier, and sensitive attributes; links represent the structure of the network.

1. An identifier attribute A^{id} (e.g., SSN, e-mail address) which is used to identify an individual from the network data. Identifier attributes must be removed when a network dataset (G) is released to the public.
2. Quasi-identifier (QI) attributes A^{qi} exist in both the released network G^* and the original network dataset G. QI attributes (e.g., Age, Sex) may reveal a personal identity with the aid of external network information. However, they cannot be removed from the released network because of ensuring data utility.
3. Sensitive attribute A^s (e.g., Illness) is confidential for an individual, and so assume it is unknown to intruders and also needs to be protected.
4. Link is mainly a direct relationship that exists in the network released through some modifications. The link information should be anonymized because it is used by intruders to extract node information and such information can be obtained from the network data.

We assumed that all identifier attributes A^{id} are removed and QI attributes A^{qi}, sensitive attributes A^s, and link information L are kept in the released network data. We also expected that collecting sensitive information from any external source (i.e., other network) is not possible. Therefore, intruders cannot use sensitive attributes to increase changes in disclosure. However, intruders can use network linkage approach [18] between QI attributes and external node. Relationship information is then used to conclude the identity of individuals from the released network data, where identifier attributes A^{id} are removed. We used binary links in our proposed privacy model. We considered all links among nodes as identical. Therefore, we denoted these nodes using unlabeled undirected connections that have the same nature to all information (QI and sensitive information) of a node. The link information may be known to an intruder and used by matching them with targeted network information; hence, such information is beneficial to privacy challenges that might lead to node information disclosure (i.e., identity and/or attribute disclosure). To address this privacy challenge, scholars modify node and link information, where intruders are allowed to identify a subgraph but not individuals. This solution enforces the k-anonymity property.

In this study, we assumed that the nodes are labelled by their links. However, clustering process maintains ℓ-diversification among sensitive values within each cluster. Our privacy approach has two main objectives. First, any two nodes within a cluster should be indistinguishable with respect to their link information. Second, nodes within each cluster should be protected against homogeneity attack using external information (e.g., link information).

A. Intuition of proposed model

Most existing network anonymization approaches use k-anonymity models for both node and link anonymization [12], [13], [18]. These methods cannot prevent homogeneity attack if intruders have relationship information of any node in a QI-group, where all nodes have same QI attribute values. Figure 1 shows three k-anonymous networks, where each node contains same sensitive information and has the same relationship structure. If intruders have relationship information, then they can easily identify sensitive information of a node. For example, a person suffers from cancer if any node has one link; meanwhile, an individual has diabetes and flu if the node has two and three links, respectively.

In existing social network anonymization model, sensitive attributes are retained without any modification of the released network data. Based on the example illustrated, only k-anonymity technique cannot provide privacy against some attacks. To protect the privacy for sensitive attributes, we included another privacy model, namely, ℓ-diversity model for preserving privacy in node information. Considering that k-anonymity in relationship information cannot effectively identify individual information, we adopted k-anonymity for

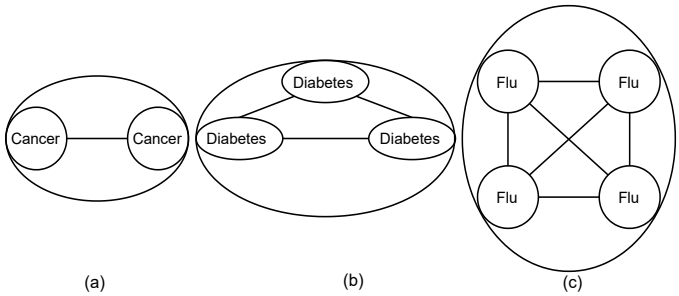

Figure 1: *k*-anonymity: a) 2-anonymity; b) 3-anonymity; and c) 4-anonymity.

relationship anonymization in our proposed approach. Figure 2 shows the network released using our proposed anonymity approach. Suppose an intruder knows the link information of a node (let it be 2), the anonymized network data intruder cannot accurately determine whether or not an individual suffers from diabetes or cancer. Similarly, link 3 intruders cannot declare that any one has flu, cancer, or diabetes.

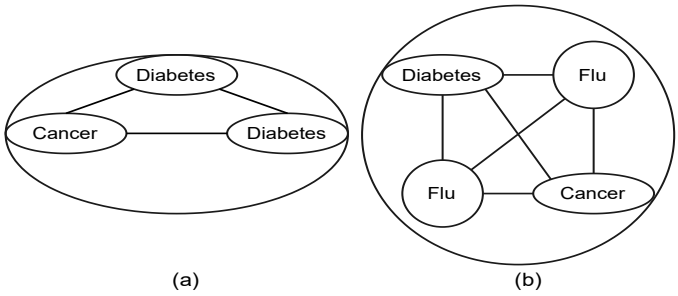

Figure 2: *(l,k)*-anonymity: a) (2,3)-anonymity and b) (3,4)-anonymity.

In the context of network data, the current literature has focused on the application of k-anonymity on both node and link anonymization although privacy preserving approaches should consider diversification among the value of sensitive attributes in the QI group. Therefore, sensitive attributes are affected by different attacks. To resolve this problem, we formalized the concepts that motivated a novel framework for computing privacy-aware information by considering the sensitive value diversification.

B. Privacy model

The privacy model, namely, (ℓ, k)-anonymity model, performs a set of algorithms with respect to the ideas of top–down specification and local recoding approaches to generate the (ℓ, k)- anonymous network, $G' = (N', L')$, from the original network *G=(N,L)*. The quasi-identifier and sensitive attributes are used to present node information (N), and the relationships between nodes and clusters are used to present links (L) that are undirected and unlabelled. In a privacy process, clustering establishes an appropriate partitioning of all nodes from N into clusters, $Cls = cls_1, cls_2, \ldots\ldots, cls_m$, and $\sum_i^m |cls_i| = N$. Here, appropriate partitioning means that each cluster must contain at least k records and minimize information loss during clustering because node and link generalization reduce data utility at the time of data modification. All nodes within a cluster are made similar with respect to the quasi-identifier attributes, and the node relationship is kept diversified with regard to the sensitive attributes. This similar characteristic can be achieved using node generalization for the quasi-identifier attributes and link generalization for node relationship.

Quasi-identifier attributes are modified in each cluster to achieve ℓ-diversification property, where QI attributes of records are similar, but sensitive attributes of records must be ℓ-diverse. In this study, we used top–down specialization approach to cluster data with minimal cost and local recording approach to achieve ℓ-diverse nodes within a cluster. In the local recoding approach, records' values are changed individually. This recoding approach is more suitable and scalable for applying (ℓ, k)-anonymity, and the resulting de-identified node presents less data distortion. To measure data distortion in local recoding, we used a term named privacy cost. For instance, we used a suppression-replace original value by using an unknown value (e.g., *) for recoding any node (N) of network, G. In this case, privacy cost is measured by the whole quantity of suppressions or the number of *'s in the de-identified node information (N'). Our main goal is to find local recoding at minimum privacy cost. This phenomenon is the problem of optimal (ℓ, k) anonymity. The corresponding decision issue is defined as follows:

(ℓ, k)-anonymity: Given a network $G(N, L)$, node information contains some QI attributes (A^{qi}) and sensitive attributes (A^s), local recoding exists for node information (N) by a function f such that after recoding, (ℓ, k)-anonymity is satisfied and the cost of privacy is less than a certain threshold value. In the (ℓ, k)-anonymity technique, our goal is to compute a generalized network (G') such that,

1) it has a generalized node for every node in *G*, and
2) it provides the maximum utility of *G*.

C. Minimize information loss

During anonymization, we should minimize information loss between the original network data and its modified version caused by the subsequent cluster-level nodes and link generalization. To obtain good quality generalized data, we considered two metrics for quantifying information loss in this study. One metric measures how node information is lost through QI attribute generalization, and this measurement approach is called Generalization Node-information Loss (GNiL). Second, metric quantifies the amount of link information lost through the link generalization, and this metric is called Generalization Link-information Loss (GLiL).

1) Generalization Node-information Loss (GNiL): To quantify generalization node-information loss, we measured the data distortion ratio of the anonymized dataset, which is defined as follows:

The distortion ratio is equal to the generalized dataset divided by the fully generalized dataset. The distortion ratio for

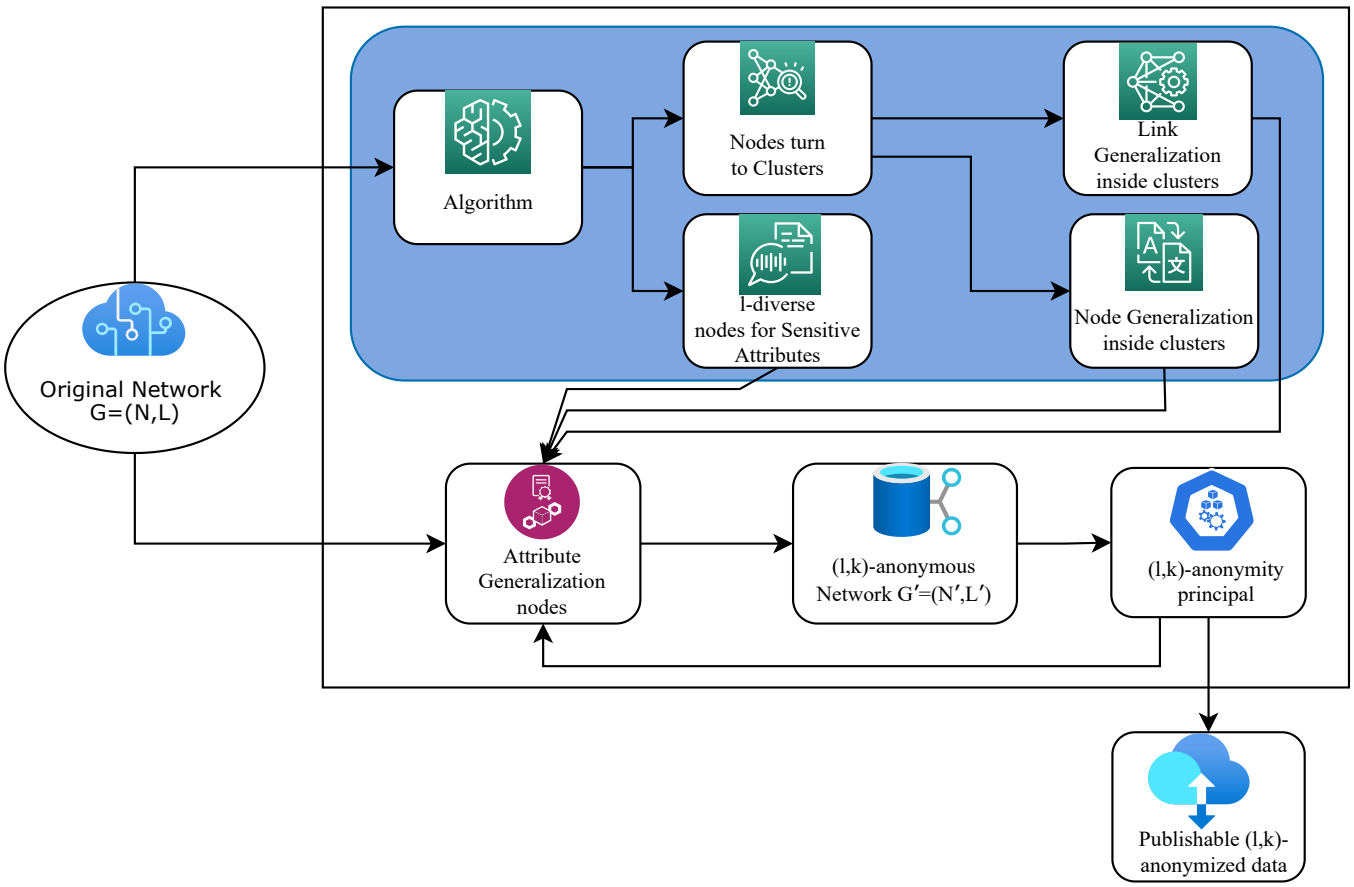

Figure 3: Proposed network data privacy preserving (ℓ, k)-anonymity framework

categorical and numerical attributes is illustrated as follows:
Distortion ratio for categorical attributes:
Let $\mathbb{C}Q$ be a categorical attribute, $\mathbb{C}Q_i \in QI$ and $\mathcal{H}_{\mathbb{C}Q}$ be the height of the tree hierarchy of $\mathbb{C}Q$. Here, $w_{i,i+1}$ is the weight from level i to level $i+1$ where level, $i = 0, 1, 2, 3, 4, \ldots\ldots, .\mathcal{H}_{\mathbb{C}Q}$. If v is the value of attribute $\mathbb{C}Q$, then the distortion ratio between the value of original data (v_o) and the value of anonymized data (v_a) is defined as:

$$Dist\_ratio(v_0, v_a) = \frac{\sum_{i=a+1}^{o} w_{i,i+1}}{height(\mathcal{H}_{\mathbb{C}Q})}$$

2) Generalization Link-information Loss(GLiL): In this section we now introduce a new metric that was first presented in [18] to quantify the loss of link information at the time of anonymizing a network through compressing clusters into nodes, together with their neighboring nodes.

Information loss is measured by the probability of delusion when any intruders want to reconstruct the basic structure of relationships of an original network from its anonymized version. There are two parts for the link information loss: the *intra-cluster link information loss* and the *inter-cluster link information loss* components.

IV. Conclusions and Future Work

In this paper, we studied a novel privacy approach, (ℓ, k)-anonymity, for network dataset. We introduced a node and link generalization method where no nodes and links are added or removed from the social network datasets. We extended k-anonymity approaches to ℓ-diversity through assuring ℓ-diversification to the nodes' information within a cluster. Moreover, we planned to develop a set of algorithms with respect to the ideas of top-down specification and local re-coding approaches to make the model visible in near future. Our privacy approach will provide anonymized networks where any node within a cluster should be indistinguishable with respect to their link information, and nodes within each cluster should be protected against homogeneity attack. The main contribution of this study is the development of a novel, efficient, and effective network privacy method with a conceptual framework, which has great potential to be applied to support real-world business applications through securing network data sharing. This study offers a some theoretical foundation of the protection of records within the network data. However, our proposed privacy approach is bounded to homogeneous network datasets where all relationships have the same meaning. Real-world network data are different as

different relationships have different values. Thus, the current model is not able to provide privacy regarding heterogeneous network data. Nevertheless, we believe that the proposed (ℓ, k)-anonymity approach is amenable to several extensions that will make it practical in real-world applications: incorporating heterogeneous link analytics. We have the intention to investigate these issues further in future work. Moreover, we know currently that we are living in the big data era where a huge number of people, devices, and sensors are connected via digital networks. Though our proposed privacy approach is not ready for use in the big data environment, we will extend our proposed method as a privacy-preserving method for network data analytics in big data environment to address the challenge of information privacy in the near future.

V. Acknowledgment

This work is supported by grants from Bangladesh University Grand Commission (Project: BRUR/RD/2021-22/03).

References

[1] T. Hei-Man, "An ethnography of social network in cyberspace: The facebook phenomenon," *The Hong Kong Anthropologist*, vol. 2, no. 1, pp. 53–77, 2008.

[2] M. A. Rahim, M. Rahman, M. A. Rahman, A. J. M. Muzahid, and S. F. Kamarulzaman, "A framework of iot-enabled vehicular noise intensity monitoring system for smart city," *Advances in Robotics, Automation and Data Analytics: Selected Papers from ICITES 2020*, vol. 1350, p. 194, 2021.

[3] M. I. Pramanik, W. Zhang, R. Y. Lau, and C. Li, "A framework for criminal network analysis using big data," in *2016 IEEE 13th international conference on e-business engineering (ICEBE)*. IEEE, 2016, pp. 17–23.

[4] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163–168, 2018.

[5] M. I. Pramanik, R. Y. Lau, and W. Zhang, "K-anonymity through the enhanced clustering method," in *2016 IEEE 13th International Conference on e-Business Engineering (ICEBE)*. IEEE, 2016, pp. 85–91.

[6] M. I. Pramanik, R. Y. Lau, H. Demirkan, and M. A. K. Azad, "Smart health: Big data enabled health paradigm within smart cities," *Expert Systems with Applications*, vol. 87, pp. 370–383, 2017.

[7] A. J. Md Muzahid, S. F. Kamarulzaman, and M. A. Rahim, "Learning-based conceptual framework for threat assessment of multiple vehicle collision in autonomous driving," in *2020 Emerging Technology in Computing, Communication and Electronics (ETCCE)*, 2020, pp. 1–6.

[8] A. Act, "Health insurance portability and accountability act of 1996," *Public law*, vol. 104, p. 191, 1996.

[9] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in *Proceedings of the 17th international conference on World Wide Web*, 2008, pp. 237–246.

[10] B. A. Malin, "An evaluation of the current state of genomic data privacy protection technology and a roadmap for the future," *Journal of the American Medical Informatics Association*, vol. 12, no. 1, pp. 28–34, 2005.

[11] T. Wang and L. Liu, "Butterfly: Protecting output privacy in stream mining," in *2008 IEEE 24th International Conference on Data Engineering*. IEEE, 2008, pp. 1170–1179.

[12] T. Ji, C. Luo, Y. Guo, Q. Wang, L. Yu, and P. Li, "Community detection in online social networks: a differentially private and parsimonious approach," *IEEE transactions on computational social systems*, vol. 7, no. 1, pp. 151–163, 2020.

[13] M. Hay, G. Miklau, D. Jensen, D. Towsley, and C. Li, "Resisting structural re-identification in anonymized social networks," *The VLDB Journal*, vol. 19, no. 6, pp. 797–823, 2010.

[14] K. Liu and E. Terzi, "Towards identity anonymization on graphs," in *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, 2008, pp. 93–106.

[15] A. Rahman, S. N. Sadat, A. T. Asyhari, N. Refat, M. N. Kabir, and R. A. Arshah, "A secure and sustainable framework to mitigate hazardous activities in online social networks," *IEEE Transactions on Sustainable Computing*, 2019.

[16] T. Wang, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and J. Cao, "Big data reduction for a smart city's critical infrastructural health monitoring," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 128–133, 2018.

[17] M. I. Pramanik, R. Y. Lau, W. T. Yue, Y. Ye, and C. Li, "Big data analytics for security and criminal investigations," *Wiley interdisciplinary reviews: data mining and knowledge discovery*, vol. 7, no. 4, p. e1208, 2017.

[18] A. Campan and T. M. Truta, "Data and structural k-anonymity in social networks," in *International Workshop on Privacy, Security, and Trust in KDD*. Springer, 2008, pp. 33–54.

[19] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 571–588, 2002.

[20] E. Zheleva and L. Getoor, "Preserving the privacy of sensitive relationships in graph data," in *International workshop on privacy, security, and trust in KDD*. Springer, 2007, pp. 153–171.

[21] B. Kenig and T. Tassa, "A practical approximation algorithm for optimal k-anonymity," *Data Mining and Knowledge Discovery*, vol. 25, no. 1, pp. 134–168, 2012.

[22] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *21st International conference on data engineering (ICDE'05)*. IEEE, 2005, pp. 217–228.

[23] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd International Conference on Data Engineering*. IEEE, 2007, pp. 106–115.

[24] M. E. Nergiz and C. Clifton, "Thoughts on k-anonymization," *Data & Knowledge Engineering*, vol. 63, no. 3, pp. 622–645, 2007.

[25] L. C. Kiew, A. J. M. Muzahid, and S. F. Kamarulzaman, "Vehicle route tracking system based on vehicle registration number recognition using template matching algorithm," in *2021 International Conference on Software Engineering Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 2021, pp. 249–254.

[26] M. I. PRAMANIK, M. R. Hasan, B. Karmaker, and T. Alom, "An art of location privacy on social media," *International Journal of Scientific and Engineering Research*, vol. 5, no. 12, pp. 1115–1122, 2014.

[27] M. A. Rahman, A. T. Asyhari, I. F. Kurniawan, M. J. Ali, M. Rahman, and M. Karim, "A scalable hybrid mac strategy for traffic-differentiated iot-enabled intra-vehicular networks," *Computer Communications*, vol. 157, pp. 320–328, 2020.

[28] S. A. Murad, Z. R. M. Azmi, Z. H. Hakami, N. J. Prottasha, and M. Kowsher, "Computer-aided system for extending the performance of diabetes analysis and prediction," in *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*. IEEE, 2021, pp. 465–470.

[29] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography," in *Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 181–190.

[30] M. M. Hasan, M. S. Islam, and S. Abdullah, "Robust pose-based human fall detection using recurrent neural network," in *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*. IEEE, 2019, pp. 48–51.

[31] M. Kowsher, A. Tahabilder, and S. A. Murad, "Impact-learning: a robust machine learning algorithm," in *Proceedings of the 8th international conference on computer and communications management*, 2020, pp. 9–13.

[32] A. Karim, M. A. Islam, P. Mishra, A. J. M. Muzahid, A. Yousuf, M. M. R. Khan, and C. K. M. Faizal, "Yeast and bacteria co-culture-based lipid production through bioremediation of palm oil mill effluent: a statistical optimization," *Biomass Conversion and Biorefinery*, pp. 1–12, 2021.

[33] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," in *2008 IEEE 24th International Conference on Data Engineering*. IEEE, 2008, pp. 506–515.

[34] X. Ying and X. Wu, "Randomizing social networks: a spectrum preserving approach," in *proceedings of the 2008 SIAM International Conference on Data Mining*. SIAM, 2008, pp. 739–750.

[35] A. J. M. Muzahid, S. F. Kamarulzaman, and M. A. Rahman, "Comparison of ppo and sac algorithms towards decision making strategies for collision avoidance among multiple autonomous vehicles," in *2021 International Conference on Software Engineering Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 2021, pp. 200–205.