Journal of Advances in Science and Technology
Vol. 19, Issue No. 1, March-2022, ISSN 2230-9659

Neural Network based Privacy Preservation Data Mining for Social Network Sites

Mr. Vishvas Vitthal Kalunge[1]*, Dr. Amit Jain[2]

[1] Research Scholar, Sunrise University, Alwar

[2] Professor, Department of Computer Science, Sunrise University, Alwar.

Abstract - Due to increasing use of Online Social Networks (OSNs) applications such as Facebook, Twitter, etc., several research challenges related to security and privacy of OSN users introduced. The end users of OSNs expecting that social networks should strong enough to preserve their private data secure from the attackers. In this research work, we introduce the novel data mining based framework to protect the OSNs from various privacy violation concerns. Risk of disclosure of individual's confidential information have risen tremendously due to widening of social network and publication of its data. From security perspective privacy retaining becomes mandatory prior to service providers publish network information. Recently, preservation of privacy in data of social networks has become most challenging and concerning problem as it has caught our lives in a dramatic way. Various methods of anonymizationexist thathelps in retaining privacy of social networking.By developing graph and nodes degree, k-Anonymity and among all available techniques is an utmost one that assist in delivering security of information on internet. With major manipulation in editing of node techniques in this research paper, improvement of K-anonymity has been explained. With integration of same degree in one group, clusters are developed and processes are repeated untillrecognition and identification of noisy data is done. For minimizing node misplacement in groupsan Advanced Cuckoo Search is commenced and processed. To cross verifystructure and for reducing node miss placement in groups outcome of Cuckoo Searches are combined with Feed Forward Back Propagation Neural Networks. We have computed the Information Loss and Average Path Length of proposed model. These results showed that the reduction in these parameters to a good extent compared to other implementations. These values of Information Loss and Average Path Length in case of a network with 9 nodes are obtained as 0.24 and 32.2 respectively.

Keywords - Information loss, K-anonymity, Preservation, Clustering, APL, Neural Networks.

----------X----------

1. INTRODUCTION

Internet is playing a indispensable role in the popularity of social networking. Much of resource in big data, especially social networking sites regularly share large volume data over network. Such information exhibits front and backend characteristics And is basically disseminated with the sole purpose of analysis [1]. Worldwide analysis results of com Score shows that U.S. People use 98% of the available time for surfing over Instagram[2]. The time has shown a tremendous amount of increase in Both scalability and variety of data over network. The statistical Analyses have shown that network sites such as twitter cover 600 million entities with 0.5 billion netizens actively tweets. Similarly, Facebook exhibits at least 1650million users out of which 100 million accounts to most active users. When discussion popularity of Amazon, it is found that it has 0.304 billion users who deal through 9.65 billion items over a single year. With comparatively low popularity Tencent Qaccounts to 829 million active users. This shares huge amount of data though social Networking channels and websites. [3].The stats shows the Growing strength of Social media in connecting people over the Globe. Example of social media is shown in Figure 1.

This big data forms a rich source of information and is very Advantageous for conducting various type of analysis. On the Other hand, the rising numbers of users over the network have Also raised the privacy risk and incidents of various types of theft And attacks. Hence, the social networks have been the major Victims[4, 5]. The users over these networking sites share the Information under various attributes like gender, location, Contact information, etc. This personal information can get Compromised due to malicious act that severely violates the Integrity of the data and privacy protection policy [6].

Figure 1: Social media over globe

As a result, It has become mandatory for a service provider to offer privacy Protection before publishing any kind of data over the network. Data comprising sensitive personal information have been the Mainly focused. The observed inconsistency among the data Instances has raised the foes that keep their eye over the Sensitive information that is integrated in the published records [7].

2. LITERATURE SURVEY

Zhang et al. addressed the privacy issue with the engagement of multi levelled caching and spatial k-anonymity design. Initially next location of the query was predicted based on Markov approach. Further knowledge of location was used by authors to increase the location privacy based on another spatial k-anonymity design. Simulations analysis demonstrated a high magnitude privacy protection and shown success in terms of reduced transparency of location based server [8]. Sharma and Pathak in 2018 employed the advantage of k-anonymity to offer protection to sensitive information disseminated over the social networks. The authors had used the concept of clustering. In this approach clustering is repeated until it encounters a noisy vertex. The evaluation was done in terms of APL and information loss. The results demonstrated a 0.43% reduction in information loss. The authors added that involvement of a classification technique could improve information loss parameter [9].Wei Feng et al. in 2017 has proposed anonymous verification technique that worked on utilizing group signatures in order to deal with privacy outflow while offering Pervasive Social Networking (PSN) communication. Safe levels of endorsement were achieved with the involvement of conditional traceability and anonymity by considering trusted authority (TA) [10]. Bhaladhare et al. in 2016 designed a technique to decrease the information loss due to systematic clustering. In the process 'Greedy k-member' and 'Systematic clustering' were also discussed. The attribute information was used to create anonymized data. Privacy protection of the data was done by using systematic clustering method while disclosure risk was dealt by greedy technique. In the experimental evaluation UCI machine learning data sets comprising of 32561 records having 15 attributes were employed. The evaluation was done in terms of execution time and information loss. The results demonstrated the proposed technique resulted in lesser information loss [11].Tsai et al. in 2015 edge based approach to deal with privacy using k-anonymization in terms of finding the shortest path between the nodes. They believed that there should be a minimum of k number of shortest edges or paths between the two nodes representing a destination node and a data sensitive node. In light of this fact and belief authors proposed three algorithms that were focussed to address three distinct edge categories. This resulted in the k-shortest path based privacy protection with variable degree of information loss and execution time. They offered that their proposed models could be used as a base reference in order to achieve shortest path based anonymization research [12]. Triparty et al. in 2014 focused their research to deal with the privacy concerns of social networks and presented GASNA as an anonymization approach for social networks. The technique was based on greedy algorithm that offers protection of attributes in terms of l-diversity and k-anonymity of the data. Authors had also addressed the issues faced by the existing approaches to deal with the privacy in social network and recommended a few possible solutions. A partial anonymity model was proposed by the authors that successfully addressed the d-neighborhood problem when d>1 [13].Chester et al. in 2013 were majorly concerned by k-anonymization approach in social networks. Their study revolved around higher node degrees with node set modifications preferred over edge set. This approach proved to be very advantageous when real-time node labelled graphs were studied. The authors established that a very little distortion was observed in the clustering coefficients as a result of anonymization [14].

Lin and Chen et al. focussed the issues related to violation of privacy preservation measures and postulated a PPSVC (privacy-preserving SVM Classifier) that could transform traditional SVM into a privacy protecting classifier. The effectiveness of the proposed design was demonstrated by the offered defence against adversarial attacks without compromising the classification accuracy of the classifier [15]. Okada et al.proposed a k-anonymity based technique that appends the noise to edges of social network being studied via k-neighbourhoodsubgraphs. The design was implemented such that it suppressed any change in the magnitude of edge length between nodes. Experimental evaluation had demonstrated that the proposed design could successfully maintain the edge length of the k-anonymity based graphs [16]. Tsai et al. studied the privacy preservation issues of anonymizing the shortest path. The privacy preservation is addressed with the concept utilizing the k-anonymity based identification of k-shortest privacy paths. This is achieved with the modification

of various class of edges. Experimental results demonstrated that proposed modifications successfully achieve the shortest path privacy with vivid levels of information loss [17]. Maheshwarkar et al. analysed the security problem that had risen when a single attribute of the datasets exhibits correlation with multiple attributes. In the process, they proposed K-AMOA model that could successfully solve the issues reacted to overlapping data fields [18]. Tsai et al. combined the association rule hiding techniques to k-anonymity concept to hide out the sensitive information present in the data mining outcomes. The proposed design offers an extension of the k-anonymity to achieve higher level of privacy preservation. Experimental evaluation showed that k-anonymity application to association rule effectively resulted in higher privacy protection with reduces utility loss [20]. Man et al. established that the k-anonymity is not enough to offer complete security of various sensitive data fields. To deal with the issue, they had also evaluated p-sensitive k-anonymity privacy preservation model. The proposed solution significantly decreased the privacy leakage issues and information loss instances thereby improving the data quality [21]. Song et al. proposed a new random k-anonymous method to deal with the privacy issues of the network. The authors had first worked on small data sets and analysed the computational cost. Further k-anonymity is analysed with the addition of noise to the data that offered reduction of information loss along with defending against background, homogeneity and exhaustive attacks [22]. Shailaja et al. developed a Privacy-Preservation Data Mining approach that involved both data restoration and refinement. In both the processes, optimal selection is done using modified cuckoo based opposition intensity method. It has been established that the modified cuckoo search could effectively reduce false rule generation, failure rate while offering higher degree of information preservation rate [24]. Namdarzadegan and Khafaeidesigned a model to address the privacy preservation that combines the strengths of k-anonymity with the Cuckoo based optimization approach. The proposed model was evaluated based on transitivity, clustering coefficient and average path length. Experiments demonstrated that the proposed model is found to be one-unit superior in comparison to k-anonymity method [25].

3. PROPOSEDSOLUTION WITH PROBLEM DESCRIPTION

Definition 1: A graph Get G (N, E, and P) in which there are number of nodes N joined with edges E and consisting number of sensitive labels as P. The issue is to provide equalizing Degree of every node considering that diversity of nodes remains unchanged total number of added noisy nodes remains less. This is to keep in mind that information does not reduces too short that it loses its significance.

Enhanced K-anonymity

This algorithm initiates by determining and identifying friends of root Nodes which follow finding out clusters, clusters in Clusters and appending and subtracting of nodes in information until elements reaches to same degree.

Algorithm: Finding friends of root node

Purpose of this technique is to identify connecting node of each Single unique node present in list. In First column of all three datasets shows main node whereas in third set represents connecting node. For every master node, it first identify all master nodes that is unique nodes in dataset and it searches with whom it has been connected with. Table 1.and Fig.2. is an examples as shown .

Table 1. Sample dataset

1	5644	3
1	5478	4
2	1789	5
2	1788	6
2	1786	3

As shown in table1, there exist 2 master nodes known as 1 and 2,(3, 4) and (5, 6, 3) were their friend nodes respectively. They determines degree of entire unique nodes of dataset. Fig.5 depicts created friend list from Network structure.

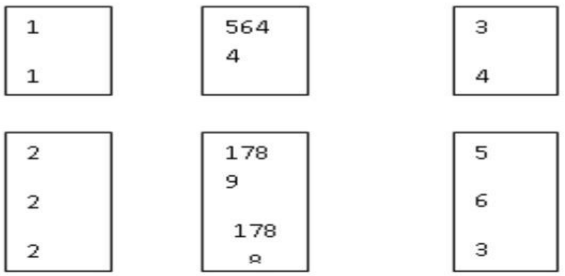

Figure 2. Creation of Friend list

```
Function Node-friend ( )
Read data // upload by user
Master_Nodes= Data (:1); // First row of each column
For each m in Master_node
Previous_value=First Master_node
Previous_Node= Master_Node(n) ;
L=1;
If previous_value=previous_value+1
Node_alteration=1
Node_connection [previous_value ]=Uploaded_data
End
End for
Return:
1 3 4
2 5 6 3
```

After algorithm 1 are three phases that consequentlyproduces 3 clusters known to be as

outer clusters. All node's Average degree (Using algorithm 1 Degree has been evaluated) that would be processed primarily. Cluster 3 consist of those nodes that possesses degree precisely equivalent to average degree, Cluster 2 retains Values that are less than average degree and all those elements having degree Greater than average degree will be in Cluster1.If there exist no node which has an exactly average degree then third cluster might remain entirely empty. As an instance,Following table 2 is taken in to consideration:

Table 2. Indicator of Relationship

1	5644	3
1	5478	4
2	1789	5
2	1788	6
2	1786	3

Node 2 has degree 3 whereas Node 1 has a degree 2. The average degree is (2+3)/n.Average degree here is 2.5, here in the master set (1, 2)as there are only Unique node. Therefore node 1 and node 2 will be considered in cluster 2,while cluster 3 would continue to remain blank. Prediction ofexample set resolved in above mentioned statements is explained in Algorithm written below. Depending on average degree of node Friend function is followed by partitioning phenomenon.

1. $Function\ Create_{cluster}(data_{files})$
2. $Foreach\ dataf\ in\ data_{files}$
3. $Degree_{InOut} = Identify_{degree}$
4. $Average_{Degree} = \sum_{j=1}^{m} \frac{deg}{m}$
5. $Create_{two}group(G1, G2);$
6. $G1 > Degree_{InOut}$
7. $G2 < Degree_{InOut}$

Function Cluster formation ( )

Two different Groups are produced once degree of entire data is computed, one having higher than average degree and other having less than average degree. By keepingnodes in separate group decreases search space however does not make sure exact anonymisation in anetwork. Toanonymize Grouped elements here Cuckoo Search Algorithm is used.

Algorithm 2: Cuckoo Search

1. $Application_{Cuckoo}\ (Group_{Elements})$
2. $Input : Group_{Elements}\ , Output : anonymized$
3. $Current_{Egg} = Key_{parents}(Group_{Elements})$
4. $Other_{Eggs} = Children(Current_{Egg})$
5. $If\ Current_{Egg}.Connection_{Count} < Group_{Elements}.Average_{Degree}$
6. $Add_{Connection_{Cukoo_{Fitness}}} = F_x(Current_{Egg}, Other_{Egg}, 1)\ //flag = 1$
7. $Elseif\ Current_{Egg}.Connection_{Count} > Group_{Elements}.Average_{Degree}$
8. $Remove_{Connection_{Cukoo_{Fitness}}} = F_x(Current_{Egg}, Other_{Egg}, 2)\ //flag = 2$
9. $End\ If$

$Where\ F_x is\ the\ fitness\ function\ of\ Cuckoo_{Search}$

Table 3. Cuckoo Search's Fitness function

Fx Output	$Fitness_{Terms}$
Connections to Add	$Flag = 1\ Intersect_{Common}(Other_{Egg} > G_{Group_{Elements}}, Current_{Egg}$
Connections to Remove	$Flag = 2\ Intersect_{Common}(Other_{Egg} < G_{Group_{Elements}}, Current_{Egg}$

The Cuckoo "Fitness works in two stages as shown in Table 3. The first stage whenthe requires to add connection and the second stage is when the wants to remove the connection. Value 1 denotes that the node wants to increase the degree and value 2 denotes that the node wants to decrease the degree. In the same cluster, if the nodes have similar group connections and other has to decrease its degree then the mutual connection will be removed from the parent and will be added to the child or demanding egg. In a way a similar fashion, the second value is when the parent wants to lose. In this scenario, the common intersected eggs will be added to the child and will be removed from the parent. In addition to Cuckoo Search, the outcome of the Cuckoo Search is cross-validated utilizing Feed Forward Back Propagation Neural Network. The instances of Neural Networks are shown" in Table 4.

Table 4. Neural Architecture

Total Neuron Count	50
Propagation Model	Levenberg
Propagation Type	Feed Forward
Cross validation Parameter	Mean Square Error (MSE)

Algorithm 3: Feed Forward Back Propagation Neural Network

Initialize ANN with parameters *– Epochs (E)*
– Neurons (N)
– Performance parameters: MSE, Gradient, Mutation and Validation Points
– Training Techniques: Levenberg Marquardt (Trainlm)
– Data Division: Random
For *each set of Training Data // Cuckoo search returned data*
Group = Categories of Training data
End
Initialized the FFBPNN using Training data and Group
Net = Newff (T, G, N)
Set the training parameters according to the requirements and train the system
Net = Train (Net, Training data, Group)
Classify = simulate (Net, test properties)
Return: *Output to validate the cuckoo search*
End

For validation of cuckoo search algorithm that depends on training mechanism Algorithm 3 is applied and subsequently used parameters ofFFBPNN are provided in Table 5. Behavior of suggested mechanism became better by implementing FFBPNN, comparatively to existing work that was well explained in next Chapter.

4. RESULTS AND DISCUSSION

This part of research is being classified in two sections. Result of proposed work has been delineated in first section and subsequent section has provided information of comparison of proposed work throughconventional methods. Research study of [19] and [23] has been taken into consideration for comparison, which utilizes Average Path Length and loss of data computing measures in this model.

Proposed Work's Result Analysis

Outcome achieved after first time assessment of proposed work is described in this section .Measures like information loss and Average Path Length has been computed for analysis purposes. Defined below are the description and Mathematical expression of considered Parameter areAverage Path Length.

a) Average Path Length (APL)

Ratio of distance in between two nodes with diverse information to that of total number of Nodes in dataset is described as average path length.

$$APL_{G(L_1 \text{ and } L_2)} = \frac{\sum_{\forall n_{i.s=L_1}, n_{j.s=L_2}} d(n_i, n_j)}{\sum_{\forall n_{i.}=l_{i,}, n_{j,}s=l_{2,}} 1}$$

Total number of nodes and current node is as shown in equation (1).

b) Information loss

Personal information loss is created due to involvement in social networking. Higher level ofencryption is directly proportional to information Loss in less amount. Following are outcome as shown that were computed post Simulation work is done.

Table 5. Average Path Length proposed work's evaluation

Number of nodes	APL
1	0.11
2	0.19
3	0.32
4	0.30
5	0.33
6	0.31
7	0.29
8	0.30
9	0.24
10	0.30

Results of Proposed work forAverage Path Length is shown in table 5 and Fig. 3. For analyzing shortest path among random nodes is assisted by accurate computation of Average Path Length. With respect to privacy protection, attaining intact social network is very complicated processas of privacy and security is concern.

The k value of nodes from 1 to 10 is taken on x-axis in figure as shown whereas obtained values of Average Path Length is taken on Y-axis as illustrated. The Measure for calculating Effectiveness of data or large transmission of information on social networking platforms is defined as Average Path Length. Average Path Length for proposed work is lower with an average of 0.269 as seen from graphical representation.

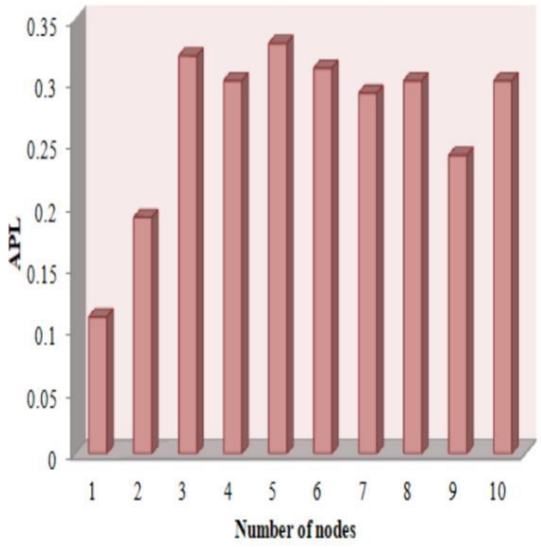

Figure 3. Average Path Length for proposed work

Comparative analysis of "proposed work with the Conventional techniques [19] and[23]This section elaborates the comparison of proposed Mechanism with the existing mechanism to depict the Effectiveness of the work." For the comparison, [19] and [23] has been considered.

Table 6. Proposed work'sevaluation for Information loss

Number of nodes	Information Loss
1	30.5
2	29.6
3	30.3
4	31.5
5	29.3
6	30.4
7	31.7
8	30.4
9	32.2

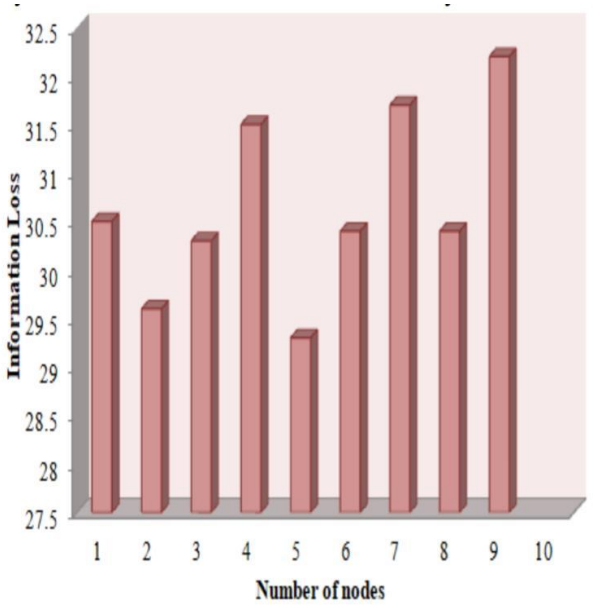

Figure 4. Proposed work's Information Loss

Results of suggested work for Information Loss is shown in table. 6 and Fig. 4.more accurate decision making is achieved with less information loss. When more links or nodes in physical communication network fades away, data loss in communication network takes place.

k value of nodes From 1 to 9 is taken on x-axis in as shown in figure whereasobtained Information loss values is illustrated on Y-axis.

Less reliability of the novel Mechanism is resulted by more information loss, hence, so as to achieve more privacy ofsystemit should be less. By Means of its effectivenessaverage value of information loss forProposed work is 30.65 which are very beneficial.

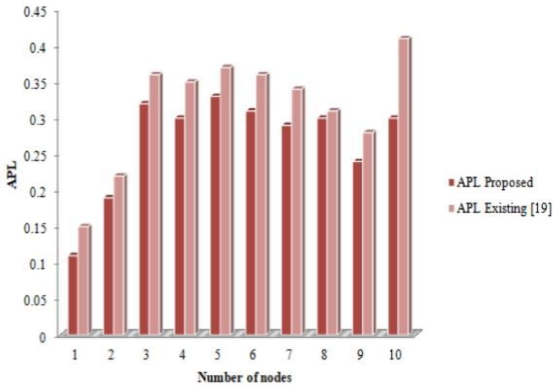

Figure 5. Average Path Length's Comparison

Proposed and existing work's comparison of Average Path Length [19] for k=10 has been delineated in Fig. 5. As contrasted to existing work there is a reduction of 14.6% in Average Path

Length of proposed work. Hence it is clear as shown in graph that proposed work has performed better in terms of Average Path Length comparatively to conventional Methodology.

Table 7. Comparison of proposed and Existing work for Information Loss [19] and [23]

Information Loss		
Proposed	**Existing [19]**	**Existing [23]**
30.5	32	33
29.6	33.1	33.3
30.3	33	33.5
31.5	33.2	33.6
29.3	33.8	34
30.4	33.1	34.2
31.7	34.6	35
30.4	34.1	35.2
32.2	35.8	36

Fig.6represent information loss's comparison for k = 9 has and table 7. Shows values.Comparison has been conducted for proposed and Existing work [19] and [23]. Data loss of conventional method is more as compared to proposed work [19] and [23].

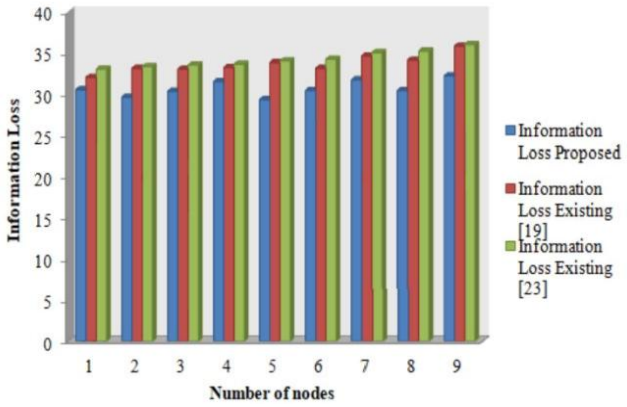

Figure 6: Information loss's comparison

Data lossaverage value for [23]is 34.2 and for [19] is 33.63 which is 8.61%of decrease has been noticed. While in contrast with [23] Information loss of proposed work with [19] was compared which was10.38% of reduction been depicted.With this evaluation conclusion can be drawn that loss of information in case of suggested work is very much low comparative to than of Existing techniques.

5. CONCLUSION

A new mechanism of privacy Preservation in social networking is provided in this article. by taking into account principle of Advanced clustering an improved k-Anonymity technique has been put forth. For designing of a novel fitness Function Cuckoo search optimization Method has been implemented.With the help of Feed Forward Back propagation Neural network results of Cuckoo Search has been cross Verified. For finding the friends of root nodes for cluster IdentificationImproved K-anonymity has been considered and for connecting node of each single Node too.To group Element ofanonymization role of cuckoo search algorithm was significant. To presentresults,QoS parameters likeInformation loss and Average Path Length are considered and comparison has done with preexisting Techniques. . We have computed the Information Loss and Average Path Length of proposed model. These results showed that the reduction in these parameters to a good extent compared to other implementations. These values of Information Loss and Average Path Length in case of a network with 9 nodes are obtained as 0.24 and 32.2 respectively.

REFERENCES

[1] A. Kaur, "A hybrid approach of privacy preserving data mining Using suppression and perturbation techniques", In International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, pp. 306-311,2017.

[2] Keküllüoğlu, D., Kökciyan, N., &Yolum, P. (2016, August). Strategies for privacy negotiation in online social networks.In Proceedings of the 1st International Workshop on AI for Privacy and Security (p. 2).ACM.

[3] D. Patel and R. Kotecha, "Privacy Preserving Data Mining: A Parametric Analysis", In Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory And Applications, Advance in Intelligent Systems and Computing, Vol. 516, pp. 139-149, 2017.

[4] A. Campan and T.M. Truta, "A Clustering Approach for Data And Structural Anonymity in Social Networks," In Privacy, Security, and Trust in KDD Workshop (PinKDD), 2008

[5] Francis, J., & Stokes, M. (2012). U.S. Patent No. 8,140,502.Washington, DC: U.S. Patent and Trademark Offic

[6] P. MohanaChelvan and K. Perumal, “Stable FeatureSelection with Privacy Preserving Data Mining Algorithm”, Advanced Informatics for Computing Research. Communications in Computer and Information Science, Springer. Singapore, Vol. 712, pp 227-237, 2017.

[7] Y. Song, P. Karras, Q. Xiao and S. Bressan, “Sensitive Label Privacy Protection on Social Network Data”, IEEE Transactions on knowledge and data engineering, Vol.25, No.3, pp 562-571, 2013.

[8] Zhang, S., Li, X., Tan, Z., Peng, T., & Wang, G. (2019). A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services. Future Generation Computer Systems, 94, 40-50.

[9] Aanchal Sharma and SudhirPathak, “Enhancement of k- anonymity algorithm for privacy preservation in social media”, International Journal of Engineering & Technology, Vol. 7, No. 2.27, pp.40-45, 2018.

[10] W. Feng, Z. Yan and H. Xie, “Anonymous Authentication on Trust in Pervasive Social Networking Based on Group Signature”, In IEEE Access, Vol. 5, pp. 6236-6246, 2017.

[11] Bhaladhare, P. R., &Jinwala, D. C. (2016). Novel Approaches for Privacy Preserving Data Mining in k -Anonymity Model. J. Inf. Sci. Eng., 32(1), 63 -78

[12] Tsai, Y.-C., Wang, S.-L., Kao, H.-Y., & Hong, T.-P. (2015). Edge types vs privacy in K-anonymization of shortest paths. Applied Soft Computing, 31, 348– 359. doi:10.1016/j.asoc.2015.03.005

[13] Tripathy, B. K., Sishodia, M. S., Jain, S., &Mitra, A. (2014). Privacy and Anonymization in Social Networks. Intelligent Systems Reference Library, 243–270

[14] Chester, S., Kapron, B. M., Srivastava, G., &Venkatesh, S. (2013). Complexity of social network anonymization. Social Network Analysis and Mining, 3(2), 151-166.

[15]. Lin, K. P., & Chen, M. S., “On the design and analysis of the privacy-preserving SVM classifier”, IEEE Transactions on Knowledge and Data Engineering, 23(11), (2010). 1704-1717.

[16]. Okada, R., Watanabe, C., & Kitagawa, H., “A k-anonymization algorithm on social network data that reduces distances between node”, In 2014 IEEE 33rd International Symposium on Reliable Distributed Systems Workshops, (2014). (pp. 76-81). IEEE.

[17]. Tsai, Y. C., Wang, S. L., Kao, H. Y., & Hong, T. P., “Edge types vs privacy in K-anonymization of shortest paths”, Applied Soft Computing, (2015).31, 348-359.

[18]. Maheshwarkar, B., Patidar, P., Rawat, M. K., &Maheshwarkar, N., “K-AMOA: K-Anonymity model for multiple overlapped attributes”, In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. (2016). (p. 83). ACM.

[19] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin and K. Ren, “Real-Time and Spatio-Temporal Crowd-Sourced Social Network Data Publishing with Differential Privacy”, In IEEE Transactions on Dependable and Secure Computing, Vol.15, No. 4, pp. 591-606, 2018.

[20]. Tsai, Y. C., Wang, S. L., Song, C. Y., & Ting, I. H, “Privacy and Utility Effects of k-anonymity on Association Rule Hiding, .(2016).

[21] Meden, Blaž, et al. "k-Same-Net: k-Anonymity with generative deep neural networks for face deidentification." Entropy 20.1 (2018): 60.

[22]. Song, F., Ma, T., Tian, Y., & Al-Rodhaan, M., “A new method of privacy protection: random k- anonymous”, (2019). IEEE Access.

[23] Bhaladhare, P. R., &Jinwala, D. C. (2016). Novel Approaches For Privacy Preserving Data Mining in k -Anonymity Model. J. Inf. Sci. Eng., 32(1), 63 -78

[24]. Shailaja, G. K., &Rao, C. G., “Opposition Intensity-Based Cuckoo Search Algorithm for Data Privacy Preservation”, (2019), Journal of Intelligent Systems.

[25]. Namdarzadegan, M., &Khafaei, T., “Privacy Preserving in Social Networks Using Combining Cuckoo Optimization Algorithm

and Graph Clustering for Anonymization", Asian Journal of Research in Computer Science, (2019).1-12.

Corresponding Author

Mr. Vishvas Vitthal Kalunge*

Research Scholar, Sunrise University, Alwar

E-Mail – vv.kalunge@gmail.com