Indonesian Journal of Electrical Engineering and Computer Science
Vol. 10, No. 2, May 2018, pp. 807~816
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i2.pp807-816

An Efficient & Secure Content Contribution and Retrieval Content in Online Social Networks Using Level-level Security Optimization & Content Visualization Algorithm

Kumaran Umapathy, Neelu Khare
School of Information Technology and Engineering, VIT University, Vellore, India

Article Info

Article history:

Received Nov 14, 2017
Revised Jan 26, 2018
Accepted Feb 11, 2018

Keywords:

Controlling & Authentications
Data Contribution & Retrieval
Level-Level Privacy
Privacy Preserving in an Online Social Network
Social Network Organizational Privacy

ABSTRACT

Online Social Networks (OSNs) is currently popular interactive media to establish the communication, share and disseminate a considerable amount of human life data. Daily and continuous communications imply the exchange of several types of content, including free text, image, audio, and video data. Security is one of the friction points that emerge when communications get mediated in Online Social Networks (OSNs). However, there are no content-based preferences supported, and therefore it is not possible to prevent undesired messages. Providing the service is not only a matter of using previously defined web content mining and security techniques. To overcome the issues, Level-level Security Optimization & Content Visualization Algorithm is proposed to avoid the privacy issues during content sharing and data visualization. It adopts level by level privacy based on user requirement in the social network. It evaluates the privacy compatibility in the online social network environment to avoid security complexities. The mechanism divided into three parts namely like online social network platform creation, social network privacy, social network within organizational privacy and network controlling and authentication. Based on the experimental evaluation, a proposed method improves the privacy retrieval accuracy (PRA) 9.13% and reduces content retrieval time (CRT) 7 milliseconds and information loss (IL) 5.33%.

Corresponding Author:

Kumaran Umapathy,
School of Information Technology and Engineering,
VIT University,
Vellore, Tamil Nadu 632014.
Email: solaisbu.phd@gmail.com.

1. INTRODUCTION

Nowadays, Online Social Networks (OSNs) is one of best a popular interactive media to communicate, share, and disseminate a considerable volume of human life information. Daily and continuous communications imply the exchange of many types of data, including free text, image, audio, and video information. Based on statistics average of Facebook, a user creates 90 pieces of data every month. It, whereas becoming more than 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.). The large and dynamic character of these data creates the premise for the employment of web content mining strategies aimed to discover useful information dormant within the data automatically. They are instrumental in providing an active support in complex and sophisticated job involved in OSN management community; such for instance access authentication or information filtering. Information filtering has greatly explored for concerns textual documents and, more recently, web content. However, the objective of the majority of the paper is mainly to offers users a security mechanism to minimize overwhelmed by unwanted data and protects user data from the attacker or unauthorized users. Based on the

result, the vastness and diversity of the field remain mostly inaccessible to externals. Hence, one of the goals of the paper is to apply to best privacy approach in OSNs into to promote social media perspective.

In OSNs, content filtering can also utilize for a different, more sensitive, purpose because in OSNs there is the chance to post or comment other posts on particular public/private areas. It called as general walls content filtering can be used to give users the ability to control the content automatically. They can also be able to remove unwanted contents. It can believe that it is a key OSN service that has not provided before. Nowadays, OSNs provide very less contribution to unwanted content on user walls. In details, Facebook permits candidates to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, there are no content-based preferences supported, and therefore it is not possible to prevent undesired content, such as political or vulgar ones, no matter of the user who posts them. It is not only a matter offering the service of using previously defined web content mining techniques and privacy oriented algorithms for a different application. It requires designing ad-hoc data visualization strategies because the content is constituted by the short text, images, video, etc. for which traditional data visualization methods have serious limitations since short texts do not provide sufficient word occurrences. The existing mechanism could work as a model and analyze access control requirements on collaborative authorization community of shared information in OSNs. The recent work has recognized the requirement of joint management for data sharing, especially photo sharing, in OSNs provided a solution for collective privacy management in OSNs. Their job considered access control policies of content that are co-owned by multiple candidates in an OSN, like that each co-owner may separately specify her/his privacy preference for the shared content.

In [1] suggested a new approach to tackling these privacy problems with a special emphasis on the private lives of users with respect to the application provider in addition to the defense against intruders or malicious users. It is also capable of capitalizing on the trust relationships that are part of social networks in real life to cope with the problem of building trusted and privacy preserving mechanisms. In [2] designed LinkMirage, a system that designed privacy-preserving access to social relations. LinkMirage utilizes users' social relations graph as an input. The method obfuscates the social graph topology and provides untrusted external applications with an obfuscated view of the social relationship graph. In [3] introduced modified an implicit Comparison-based Profile Matching protocol (iCPM) that allows the initiator to obtain directly content instead of the comparison result from the responder. The messages unrelated to user profile can be divided into multiple categories by the responder. It also generalized the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex similarity criteria spanning multiple attributes. In [4] designed a model to evaluate users' behavior in the online environment from third of a million users. It captured by their website choices and Facebook profile features, relates to their personality by the standard Five Factor Model personality questionnaire. In [5] focused on a privacy preservation technique which is applied to graphs to preserve sensitive information present in shortest paths. The privacy preserving technique of edge weight perturbation applied to a social graph in a small user group.

In [6] described a method to preserve the privacy of the published data by modifying the graph by adding a small number of edges. This method provided the quantitative value of lost information due to the generalization of the labels. In [7] explored the privacy-preserving actions regarding information sharing for this demography on one social media platform-Facebook. It also studied the shared information behavior of the elderly by observing the extent. They opt out of the exchange of information publicly about themselves on their profile pages. In [8] investigated the privacy issues of multimedia services by studying a newly emerging multimedia-oriented mobile social network (MMSN). The method also helps users to receive multimedia services not only from their online social communities but also from their social friends in the vicinity. In [9] fulfilled the research gap and uses cultural dimensions to compare the utilization of social media & other information sources for consumer decision-making from 50 countries. The method indicated that the use of information sources that influence online purchase decisions strongly varies by culture. In [10] introduced Best Friend Forever (BFF) method to automatic classification of the friends of a user in communities and assigned a value to the strength of the relationship ties to each one.

In [11] designed novel fine-grained private matching protocols which enable two users to execute profile matching without disclosing any information about their profiles. In contrast to existing coarse-grained special matching techniques for PMSN, protocols permit finer differentiation between PMSN users and can support a wide range of matching metrics at different privacy levels. In [12] developed COSNET (Connecting Heterogeneous Social Networks with local and global consistency), an energy-based model, to address the problem by considering both local and global consistency among multiple networks. An efficient sub-gradient algorithm is developed to train the model by converting the original energy-based objective function into its dual form. In [13] expressed design mechanisms, when given a preference profile submitted by a user that search a person with matching profile in decentralized multi-hop mobile social networks. The mechanisms are privacy-preserving: no participants 'profile and the submitted preference profile are exposed.

In [14] explored the reliably match profiles in practical knowledge, across real-world social networks, by exploiting public attributes, publicly provide about themselves. It also defined a set of properties for profile attributes–Availability, Consistency, non-Impressionability, and Discriminability (ACID)-that are both necessary and sufficient to determine the reliability of a matching scheme. In [15] composed area based informal organization administrations (LBSNS) have been explored; this review constructs a model to analyze the security math, advantage structure, and sex contrasts. In particular, hedonic advantages impact sly effect saw benefits than utilitarian advantages, and there is a communication impact between saw advantages and security dangers.

In [16] actualized Whisper to change the shape and substance of social associations. It demonstrated first huge scale experimental investigation of a mysterious informal community, utilizing an entire 3-month hint of the Whisper arrange covering 24 million whispers composed by more than 1 million one of a kind clients. It saw how obscurity and the absence of social connections influence client conduct. In [17] implemented Quick Community Adaptation (QCA) a perfect system appropriate for investigating substantial scale dynamic informal communities because of its lightweight registering asset necessity. It additionally attempted to distinguish groups in powerful informal organizations and refresh the system group structure given its history rather than re-processing starting without outside help. In [18] constructed a component to describe the substance of Twitter messages, particularly concentrating on well-being experts and their tweets identifying with well-being. It likewise portrayed well-being related tweets on the premise of the kind of explanation made. Particular consideration is given to whether a tweet was close to home (rather than expert) or claimed that clients would hope to upheld by some level of therapeutic proof. In [19] worked towards measuring area protection spillage from MSNs by coordinating the clients 'impacted areas to their genuine versatility follows. It likewise identifies the assault to enable an outer enemy to surmise the socioeconomics (e.g., age, sexual orientation, and training) in the wake of watching clients' uncovered area profiles. In [20] outlined YANA (another way to say "you are not the only one"), a client bunch based security protecting recommender framework for clients in online social groups. Here, clients are sorted out into gatherings with different interests and collaborate with the recommender server using intrigue particular pseudo clients, so that individual client's close to home intrigue data stays escaped the server. A suit is secure multi-party calculation conventions and suggestion techniques to shield client protection from gathering individuals.

In [21] designed Cluster based L-Diversity Privacy Preservation (CLDPP) methods to improve the privacy preservation of anonymized data from many types attacks. The method designed to group similar data together with ℓ-diverse sensitive values and then anonymizer each group individually during data movement in any point and any size. In [22] developed privacy-preserving K-means clustering algorithm to limits information leakage to the untrusted social network providers that perform the clustering. It considered the Homomorphic encryption techniques to improve the state processing encrypted content regarding efficiency by utilization of distributed structure of the system. In [23] explained a collaborative framework for using vertically partitioned co-occurrence parameters in fuzzy co-cluster structure estimation. Here, an object of items is separately stored in several sites to utilize distributed data sets without fear of information leaks. The method worked on co-clustering to simultaneously partition objects and items into co-clusters by estimating two types of fuzzy candidature ships. In [24] explained integration of Adaptive Weight Ranking Policy (AWRP) with intelligent classifiers (NB-AWRP-DA and J48-AWRP-DA) via dynamic aging factor to improve classifiers power of prediction. The methods are used to choose the best subset of features. In [25] introduced a new framework called Fuzzy based contextual recommendation system for classification of customer reviews. It extracts the information from the reviews based on the context given by users. In [26] studied to identify the best classifiers for class imbalanced health datasets through a cost-based comparison of classifier performance. The unequal misclassification costs were represented in a cost matrix, and cost-benefit.

To overcome the issues, Level-level Security Optimization & Content Visualization Algorithm is implemented to avoid the privacy issues during content sharing and data visualization process. The method is implemented with social network framework in the web environment. It utilizes level by level privacy based on OSN's user requirement in the social network. The proposed method determines the privacy compatibility in the online social network environment to avoid security complexities. The mechanism is divided into three parts namely like online social network platform creation, social network privacy, social network within organizational privacy and network controlling and authentication. Initially, it designs the effective social network platform to share and retrieve the many kinds of information. Next, it works to maintain and authenticate the privacy for a user and as well as online social network in an efficient way. It reduces the monitoring burden on OSN providers and as well government. The methods also take the social network privacy organization wise to maintain the privacy of specific organization data contributor and users. It identifies the three types of privacy problems that researchers in computer science tackle. It emerges through the necessary renegotiation of boundaries as social interactions get mediated by OSN services, in short,

called "social privacy." The proposed method reduces the content retrieval time, information loss and improves the privacy retrieval accuracy. The Paper contribution follows as:

a. Propose Level-level Security Optimization & Content Visualization Algorithm is proposed to avoid the privacy issues during content sharing and data visualization process.
b. Apply level by level privacy according to user requirement in social network after evaluation of privacy compatibility of OSN application.
c. To provide efficient full security control and authentication for data contributor and user in social network environments.
d. To offers the organization wise privacy control and endorsement of data contributor and user in social network environments.
e. To minimize the content retrieval time, Information loss and privacy retrieval accuracy of proposed approach compare than existing methods

The rest of paper constructed as Section 2 reviewed all literature which is closest to proposed methodology. Section 3 explains the overview of proposed methodology and algorithm implementation details. Section 4 discusses implemented setup, result and comparative analysis of proposed methodology. Section 5 concludes the overall proposed mechanism feature, implementation and result details with upcoming outcomes.

2. RESEARCH METHOD

The proposed methodology implementation procedure is introduced to understand the implemented framework and their conceptualization. The sections explore the proposed methodology, implementation pre-processing steps and algorithm exploration with functional and logical details. Level-level Security Optimization & Content Visualization Algorithm presents a diagrammatic representation of proposed architecture to display the level by the level privacy of user content and profile in online social networks in Figure 1. The techniques also recommend the user for make friendship or relationship with another user without compromising the privacy of profile and their content details. The pre-processing steps of proposed approach explained in details.

2.1. Implementation Pre-processing Steps

2.1.1. Social Network Construction

The module constructs the efficient and robust social network platform with interactive content to establish the connection with multiple users for many perspectives like the business, academic, research, outsourcing, etc. the main agenda of this platform is making the efficiency of the network with protection connection user data privacy. The system provides complete control in hand of user neither storage server nor online social network service provider.

2.1.2. Online Social Network Security

Online Social Network security relates to the concerns that users raise to the harms. The prior knowledge when technologically mediated communications disrupt social limitations. The users are thus "consumers" of services. Users spend time in public spaces to interact on social media to communicate with family and friends, get access to information and discussions. It also expands matters of the heart as well as those of belonging. These activities are designed publicly to ‘friends, ' or a large number of audiences is seen as a crucial component of Online Social Network. In Access Control, solutions that employ methods from user modeling objective to design strong privacy that is intuitive to use, and that cater to users’ information management requirements.

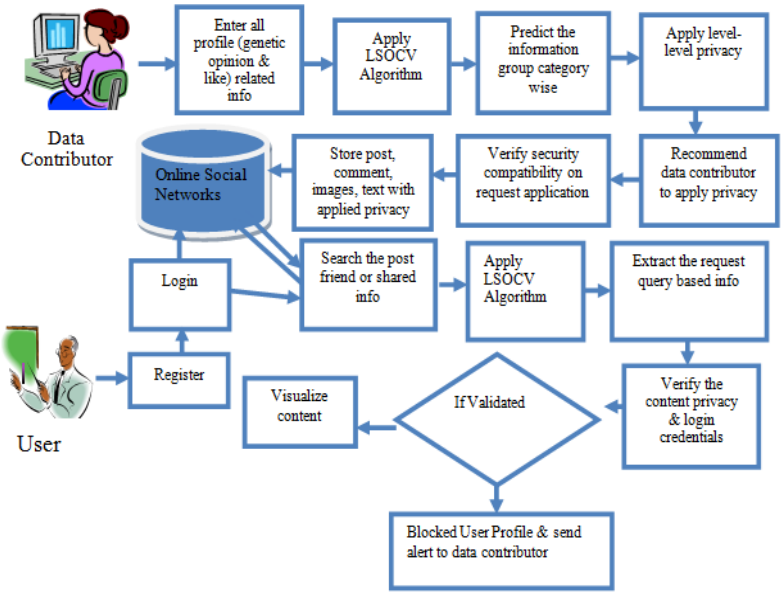

Figure 1. System Architecture Diagram

2.1.3. Controlling and Authentication

Behalf of controlling and authentication in an online social network, the method initializes from the premise that potentially adversarial entities operation or monitoring OSNs. It has an interest in getting the large volume of user details possibility, including user-generated data (e.g., posts, pictures, private content) as well as interaction and behavioral content (e.g., the list of friends, pages browsed, 'likes' 'dislikes'). Once an adversarial entity has acquired user details, it may utilize in unforeseen ways – and possibly to the demerit of the individuals associated with the content.

2.1.4. Organizational Online Social Network Security

The way in which individual control and organization transparency requirements, as defined through legislation, are implemented has an impact on both controlling and as well as online social network security issues or vice versa. Organizational Online Social Network studies all the possible way to improve the privacy of the user and online social network data maintenance for information flow controlling and authentications. The challenges are observed with the combination of controlling and authentication in an online social network to avoid the misleading issues in organization social network security given in fundamental gaps in assumptions and research methodology.

2.2. Level-level Security Optimization & Content Visualization (LSOCV) Algorithms

Level-level Security Optimization & Content Visualization (LSOCV) Algorithm is implemented to avoid the security issues during content sharing and data visualization process. The method is implemented with social network framework in a web environment. It adopts level by level privacy based on user requirement in the social network. The proposed method evaluates the privacy compatibility in the online social network to avoid security complexities. The methods are portioned into three parts namely like online social network platform creation, social network privacy, social network within organizational privacy and network controlling and authentication. The main objective of proposed algorithm is to enable the individual engagement with other users, share, and accountability and contributed information with full control and authentications in online social networks. The user explicitly shares are available to their intended recipients, while the disclosures of any other information to any other users are avoided. It improves the ability of a user to post and retrieve the many more information without hesitation of privacy in OSN. It assures the users about their control and authentication management of profile in the online social network environment. Proposed algorithm reduces the burden of cyber crime branch and service provider to take care the all activity of users by offering the efficient controlling and authentication of user profile and activity. The method also encourages the public to utilize socials media with strong privacy. Proposed method provides strong privacy control and authentication during data contribution & retrieval in the online social network.

The proposed algorithm system dedicates to provide End-End security in an online social network. Proposed algorithm predicts the User profile (UP) or Organizational network user profile (ONUP) in the following group like a genetic information, Interest, opinion, and credential information to apply the privacy. It also classifies the shared information, friend list, comment, post, community shared information group wise. During data contribution in OSN, proposed techniques to ask UP to apply privacy on UDP. It also offers to UP to restrict the user or group based their opinion and creditability of contents. During SCR process, UP can search, retrieve any types of information. Here, proposed LSOCV verified user credentials and requested content privacy setting, if users fulfill the credential ship of content and OSNs then it will proceed the SCR to the respective user. Otherwise, it will treat an unauthorized user or attacker and send alert to respective UP. The proposed LSOCV algorithm reduces the information loss (IL), content retrieval time (CRT), increases privacy retrieval accuracy. The pseudo code of proposed algorithm is explained below in details:

The Input : User Profile (UP) and Organizational Network User Profile (ONUP)
Output : User Data Protection (UDP) and Secure Content Retrieval (SCR)
Procedure :
Start :
Browse the Online Social Networks (OSNs);
Proceed for registration;
Collect the genetic, interest, opinion, and professional information
Store the UP or ONUP in database
Categorize the UP information
Apply level-level privacy based UP credential information
Verify the UP and review the request for application in OSNs
Authenticate the user & offer the application control and authentication;
Contribute and share the information;
Verify the application privacy compatibility and UP;
If accessible
Allow user to the contribution;
Else
Send alert to UP the verify their accessibility or login credentials;
Search the content or UP in OSNs;
Verify the accessibility of content offered data provider;
If applicable
Permits to view the information or UP;
Else
Block the unauthorized User profile and send alert to respective userD0.

3. RESULTS AND ANALYSIS

3.1. Programming Setup

To compare the proposed system with existing approaches, the deployment process is conducted on a laptop with Intel Core i7 7600 processor, 16GB memory, and Window 7 system. Here, this method implemented in JAVA using NetBeans 8.0 with Apache Tomcat 8.0.3 and MYSQL 5.5 Database. The Proposed algorithm is evaluated with many types of social media dataset to evaluate the efficiency of proposed systems. Here, the three types of database namely a 500KB, 1 MB and 100MB with many types of formats.

3.2. Evaluation Parameters

The proposed methods explore the evaluation matrix namely retrieval accuracy, precision, recall, F1 score and retrieval time to evaluate the efficiency of proposed algorithms to overcome the existing methods in online social networks (OSN) environment. The method computes the accuracy and retrieval time during data retrieval and data contribution. It applies the level-level privacy based on compatibility of application. The following evaluation parameters are explained below in details:

3.2.1. Privacy Retrieval Accuracy

This section describes the evaluation parameter for privacy retrieval accuracy to evaluate the privacy efficiency of proposed method which details are expressed in equation (1). The classifier

performance is better if it has higher secure content retrieval accuracy. The retrieval accuracy is calculated as correctly predicted secure user data on overall data.

$$Accuracy(\%) = \frac{T_{NoofpridcedSuer's\,securedata}}{T_{noofrecord}} \text{X100} \quad (1)$$

3.2.2. Content Retrieval (CRT)

It describes evaluation parameter for content retrieval which calculates retrieval time based on system performance and social network responses which details are expressed in equation (2).

$$CRT = T_{UD} \times T_{AR} \quad (2)$$

Where TUD is a total number of candidate data set and TAR is average retrieval time for user data set.

3.2.3. Information Loss (IL)

Information Loss explores the data distortions often to evaluate the data quality in privacy-preserving data sharing. Information loss reduces the quality of the data and affects data utility. When information loss is less, its represents the proposed mechanism is efficient and secure. The information loss is expressed in equation (3).

$$IL = \sum_{k=0}^{n-1} T_k \quad (3)$$

Where IL equals the information latency to complete a given task, n equals the number of steps required, and Tk equals the duration of the Kth step. The information-loss model also assumes that the duration of a processing step increases as the amount of information available decreases.

$$T_k = \frac{D}{I_k} \quad (4)$$

Where Ik equals the proportion of information available at the kth step and D equals the minimum step duration that occurs when the proportion of information available equals, it means that there is no information loss.

Table 1. PRA (Privacy Retrieval Accuracy), CRT (Content Retrieval Time) and IL (Information Loses) for 500KB, 1MB and 10MB Database

Dataset	500KB			1 MB			10 MB		
Algorithms	PRA	CRT	IL	PRA	CRT	IL	PRA	CRT	IL
PPK-MEANS	63.25	16	20	65.47	20	22	67.52	24	24
CFCAF	74.56	14	18	76.54	18	20	78.21	22	22
CLDPP	82.44	9	14	84.56	13	16	86.23	17	14
LSOCV	91.97	7	8	93.33	8	7	95.33	5	13

Table 1 explores the 1 PRA (Privacy Retrieval Accuracy), CRT (Content Retrieval Time) and IL (Information Loses) for 500KB, 1MB and 10MB database to evaluate the privacy efficiency and accuracy in online social network environments. Proposed System is computed with following existing methods namely: Privacy Preserving K-Means Clustering Algorithm (PPK-Means) [22], collaborative fuzzy co-cluster analysis framework (CFCAF) [23] and Cluster-based L-diversity privacy preservation (CLDPP) [21] methods. According to Table1, it noticed that LSOCV have the best score on each respective parameter for all databases.

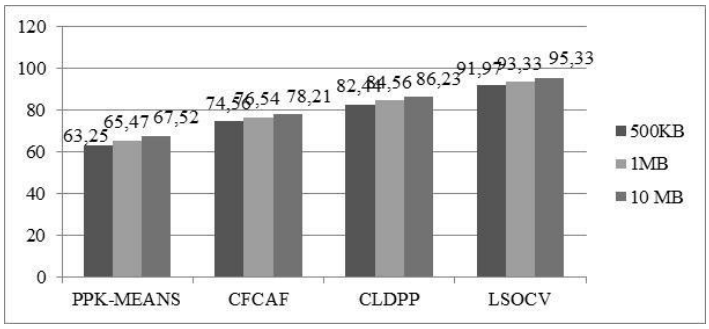

Figure 2. Effect Privacy Retrieval Accuracy (PRA) for 500KB, 1MB, and 10 KB database

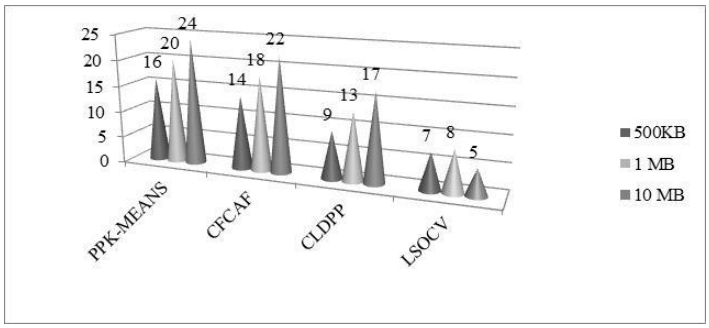

Figure 3. Content Retrieval Time (CRT) for 500KB, 1MB, and 10 KB database

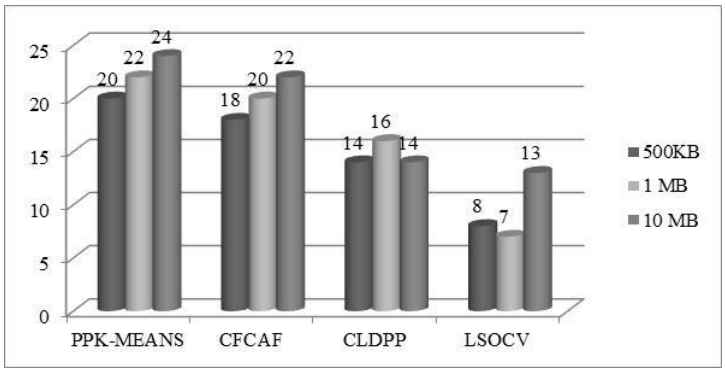

Figure 4. Information Loss (IL) for 500KB, 1MB, and 10 KB Database

According to Figure 2 to 4 evaluations, it observed that proposed LSOCV performed well on 500KB, 1MB, and 10MB database. Proposed LSOCV is evaluated with Privacy Preserving K-Means Clustering Algorithm (PPK-Means)[22], collaborative fuzzy co-cluster analysis framework (CFCAF)[23] and Cluster-based L-diversity privacy preservation (CLDPP)[21] methods behalf of privacy retrieval accuracy (PRA), content retrieval accuracy (CTR) and information loss (IL); . CLDPP is the closest competitor. It improves the privacy preservation of anonymity data to protect from many kinds of attack and also from unauthorized users. It combines the similar group of data with ℓ-diverse sensitive values and proceeds for anonymization. It also works to minimize the information loss in anonymity data during data movements. However, CLDPP fails to adopt level by level privacy based on user requirement in a social network. It does not fit to evaluate the privacy compatibility in an online social network environment for avoiding security complexities. LSOCV improves the privacy retrieval accuracy (PRA) 9.13% and reduces content retrieval time (CRT) 7 milliseconds and information loss (IL) 5.33%. Finally, the paper claims the proposed LSOCV algorithm is best on all respective parameters along with 500KB, 1MB, and 10MB databases).

4. CONCLUSION

In this paper, proposed LSOCV algorithm present Proposed Level-level Security Optimization & Content Visualization Algorithm be proposed to avoid the privacy issues during content sharing and data visualization issues. The method applies level by level privacy according to user requirement in social network after evaluation of privacy compatibility of application. The main motto of proposed technique is to enable the individual engagement with other users, share, accountability and published information with full control and authentications in online social networks. The user explicitly shares are available to their intended recipients, while the disclosures of any other information to any other users are avoided. It improves the ability of a user to post and retrieve the many more information without hesitations of privacy in OSN. It provides effective full security control and authentication for data contributor and user in social network environments. It also offers the organization wise privacy control and authentication of data contributor and user in online social network environments. It improves the privacy retrieval accuracy (PRA) 9.13% and reduces content retrieval time (CRT) 7 milliseconds and information loss (IL) 5.33%. Finally, the research paper said that the proposed LSOCV algorithm is best to approach on all respective parameters with 500KB, 1MB, and 10MB databases.

In future, the paper can be extended to apply privacy preservation techniques in level wise in Big data Hadoop environment for user content without compromising the quality of data accuracy and retrieval time.

REFERENCES

[1] Cutillo, L. A., Molva, R., & Strufe, T., "Safebook: A privacy-preserving online social network leveraging on real-life trust", *IEEE Communications Magazine*, vol. 47, no.12, pp. 1-8, 2009.

[2] Liu, C., & Mittal, P., "*LinkMirage: Enabling privacy-preserving analytics on social relationships*", In 23rd Annual Network and Distributed System Security Symposium, NDSS, pp. 21-24, 2016.

[3] Shewale, K., & Babar, S. D., "An Efficient Profile Matching Protocol Using Privacy Preserving in Mobile Social Network", *Procedia Computer Science*,; vol. 79, pp. 922-931, 2016.

[4] Kosinski, M., Bachrach, Y., Kohli, P., Stillwell, D., & Graepel, T., "Manifestations of user personality in website choice and behavior on online social networks", *Machine Learning*,; vol. 95, no. 3, pp. 357-380, 2014.

[5] Mattani, N., Kumar, J. S., Prabakaran, A., & Maheswari, N., "Privacy Preservation in Social Network Analysis using Edge Weight Perturbation", *Indian Journal of Science and Technology*, vol. 9, no. 37, pp. 1-10, 2016.

[6] Khazali, M. J., Sargolzaei, E., & Keikha, F., "Privacy Preserving Approach of Published Social Networks Data with Vertex and Edge Modification Algorithm", *Indian Journal of Science and Technology*, vol. 9, no. 12, pp. 1-8, 2016.

[7] Chakraborty, R., Vishik, C., & Rao, H. R., "Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing", *Decision Support Systems*, vol. 55, no. 4, pp. 948-956, 2013.

[8] Zhang, K., Liang, X., Shen, X., & Lu, R., "Exploiting multimedia services in mobile social networks from security and privacy perspectives", *IEEE Communications Magazine*, vol. 52, no. 3, pp. 58-65, 2014.

[9] Goodrich, K., & De Mooij, M., "How 'social'are social media? A cross-cultural comparison of online and offline purchase decision influences", *Journal of Marketing Communications*, vol. 20, no. 1-2, pp. 103-116, 2014.

[10] Fogués, R. L., Such, J. M., Espinosa, A., & Garcia-Fornes, A., "BFF: A tool for eliciting tie strength and user communities in social networking services", *Information Systems Frontiers*, vol. 16, no. 2, pp. 225-237, 2014.

[11] Zhang, R., Zhang, J., Zhang, Y., Sun, J., & Yan, G., "Privacy-preserving profile matching for proximity-based mobile social networking", *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 656-668, 2013.

[12] Zhang, Y., Tang, J., Yang, Z., Pei, J., & Yu, P. S., "*Cosnet: Connecting heterogeneous social networks with local and global consistency*", In Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2015, pp. 1485-1494.

[13] Zhang, L., Li, X. Y., & Liu, Y., "*Message in a sealed bottle: Privacy preserving friending in social networks*", In Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on IEEE, 2013, pp. 327-336.

[14] Goga, O., Loiseau, P., Sommer, R., Teixeira, R., & Gummadi, K. P., "*On the reliability of profile matching across large online social networks*", In Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2015, pp. 1799-1808.

[15] Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X., "Location information disclosure in location-based social network services: Privacy calculus, benefits structure, and gender differences", *Computers in Human Behavior*, vol. 52, pp. 278-292, 2015.

[16] Wang, G., Wang, B., Wang, T., Nika, A., Zheng, H., & Zhao, B. Y., "*Whispers in the dark: analysis of an anonymous social network*", In Proceedings of the 2014 Conference on Internet Measurement Conference, 2014, pp. 137-150.

[17] Nguyen, N. P., Dinh, T. N., Shen, Y., & Thai, M. T., "Dynamic social community detection and its applications", *PloS one*, vol. 9, no. 4, pp.1-13, 2014.

[18] Lee, J. L., DeCamp, M., Dredze, M., Chisolm, M. S., & Berger, Z. D., "What are health-related users tweeting? A qualitative content analysis of health-related users and their messages on Twitter", *Journal of medical Internet research*, vol. 16, no. 10, pp. 1-9, 2014.

[19] Li, H., Zhu, H., Du, S., Liang, X., & Shen, X., "Privacy leakage of location sharing in mobile social networks: Attacks and Defense", *IEEE Transactions on Dependable and Secure Computing*, pp. 1-14, 2016.
[20] Li, D., Lv, Q., Shang, L., & Gu, N., "Efficient privacy-preserving content recommendation for online social communities", *Neurocomputing*, vol. 219, pp. 440-454, 2017.
[21] Malaisamy A., Nawaz Kadhar G. M., "Clustering Based L-Diversity Anonymity Model for Privacy Preservation of Data Publishing", *International Journal of Enhanced Research in Science, Technology & Engineering*, vol. 5, no. 11, pp. 55-66, 2016.
[22] Erkin, Z., Veugen, T., Toft, T., & Lagendijk, R. L., "Privacy-preserving distributed clustering", *EURASIP Journal on Information Security*, vol. 1, pp. 1-15, 2013.
[23] Honda, K., Oda, T., Tanaka, D., & Notsu, A., "A collaborative framework for privacy preserving fuzzy co-clustering of vertically distributed cooccurrence matrices", *Advances in Fuzzy Systems*, vol. 1, pp. 1-9, 2015.
[24] Olanrewaju, R. F., & Azman, A. W., "Intelligent Cooperative Adaptive Weight Ranking Policy via dynamic aging based on NB and J48 classifiers", *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 5, no. 4, pp. 357-365, 2017.
[25] Sulthana, R., & Ramasamy, S., "Context Based Classification of Reviews Using Association Rule Mining, Fuzzy Logics and Ontology", *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 6, no.3, pp. 250-255, 2017.
[26] Rao, R. R., & Makkithaya, K.., "Learning from a Class Imbalanced Public Health Dataset: a Cost-based Comparison of Classifier Performance", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 4, pp. 2215-2222, 2017.