Optimized Multi-Level Security for Content Contribution and Retrieval in Online Social Networks using a Content Visualization Mechanism

S. Nasira Tabassum
Department of Computer Science & Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
nasira.tabassum@gmail.com (corresponding author)

Gangadhara Rao Kancherla
Department of Computer Science & Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
kancherla123@gmail.com

Received: 10 September 2024 | Revised: 9 October 2024 and 13 October 2024 | Accepted: 14 October 2024

ABSTRACT

Online social networks have become an integral part of modern communication, providing platforms for users to share personal information, media, and opinions. However, these platforms face significant challenges in preserving user privacy while ensuring efficient data retrieval and maintaining data integrity. Existing privacy preservation methods, such as PPK-MEANS, CFCAF, and CLDPP, are limited in their ability to handle the growing complexity and scale of user data, often leading to inefficiencies such as high Content Retrieval Time (CRT), increased Information Loss (IL), and compromised data accuracy. These inefficiencies are crucial to address, as they can degrade the user experience by causing delays, compromising data integrity, and limiting system scalability. High CRT frustrates users, while increased IL reduces data accuracy, undermining trust and system reliability. The primary issue addressed in this study is the need for an advanced privacy-preserving mechanism that can provide multilevel security while maintaining optimal system performance. To overcome these limitations, the Layered Secure Online Collaborative Verification (LSOCV) algorithm is proposed, designed to offer a scalable solution with tiered privacy controls based on user requirements. LSOCV enhances Privacy Retrieval Accuracy (PRA), significantly reduces CRT, and minimizes IL. The experimental results show that LSOCV achieved a PRA of 91.97%, reduced CRT to 7ms, and decreased IL by up to 8% for 500KB files, outperforming existing approaches. This method provides robust privacy protection and efficient data handling on social networks, with the potential for future application in big data environments, such as Hadoop, to ensure scalable, secure, and efficient privacy-preserving solutions.

Keywords-social networks; complexity; information retrieval; privacy

I. INTRODUCTION

Privacy-preserving strategies are crucial in the modern digital landscape, particularly within Online Social Networks (OSNs) and Web-based platforms where users share vast amounts of personal and sensitive information. These strategies are designed to protect user data from unauthorized access while ensuring the integrity of interactions among users. However, despite their effectiveness in certain environments, such strategies face challenges when it comes to managing the different levels of access control required by OSN users [1]. Public, private, and protected privileges are essential for customizing access to content based on the sensitivity of the shared information. Balancing user convenience with the need for robust security becomes a complex task, as users expect seamless experiences without compromising their privacy. Machine learning techniques, such as those used for predictive maintenance in rotating machinery fault detection, can be adapted to enhance the efficiency of online social network security by identifying anomalies in content retrieval and user interactions [2]. This study proposes the LSOCV algorithm to address these complexities. This algorithm offers a solution to manage privacy during content sharing and data visualization, providing a structured approach to determine the privacy compatibility of OSN frameworks. Efforts to reduce authentication computational time, as demonstrated in MANETs [3], are crucial to improving the performance and security of OSNs. By doing so, LSOCV helps mitigate common privacy concerns that arise in social network environments, particularly during interactions that involve multimedia sharing and large-scale data transmissions.

A. Applications and Benefits of LSOCV in OSNs

The LSOCV algorithm has a range of applications in OSNs, especially as these networks continue to grow in scale and complexity. One of its primary functions is to secure multimedia content sharing, including images, videos, text, and audio, which are transmitted between users on these platforms. OSNs such as Facebook, Twitter, and Instagram generate significant amounts of user-generated content daily, necessitating advanced methods to safeguard user privacy. The ability of LSOCV to optimize security based on different access levels allows for personalized privacy settings, ensuring that each piece of content is shared according to user-defined preferences. Cybersecurity awareness models, such as those developed to protect specific populations from social media attacks, emphasize the importance of user education and secure platform design in preventing privacy breaches [4]. The algorithm not only enhances security during data transmission but also facilitates content visualization, allowing users to access shared content without risking unauthorized exposure. This dual focus on content sharing and visualization makes LSOCV versatile, improving both the privacy and efficiency of OSN interactions while maintaining user trust and satisfaction.

B. Challenges and Issues in Implementing LSOCV

Despite its advantages, the implementation of the LSOCV algorithm is not without challenges. One of the key issues is the complexity involved in balancing privacy and usability. Users demand platforms that provide seamless and intuitive experiences, but the introduction of multiple levels of access control can potentially complicate the user experience. Decentralized privacy-preserving services, such as the one proposed in [5], provide an alternative solution that allows users to easily navigate and manage privacy settings in OSNs while maintaining control over their data. Another issue is that the scalability of large social networks with millions of users may face difficulties in deploying the algorithm at scale, particularly when handling massive amounts of multimedia content. The algorithm needs to manage and optimize privacy settings for diverse types of content while minimizing any delays or inefficiencies. Techniques for detecting malicious behavior, such as those utilizing Windows audit logs [6], are critical for adapting privacy-preserving methods to evolving cybersecurity threats in OSNs. With hackers continually developing new methods to breach privacy, the algorithm must be updated regularly to combat emerging vulnerabilities. Finally, as data privacy laws and regulations become stricter worldwide, ensuring that the LSOCV algorithm complies with all legal requirements across different jurisdictions adds another layer of complexity to its implementation.

This study introduces the LSOCV algorithm to address privacy challenges related to content sharing and visualization in OSNs. This method leverages tiered privacy settings based on user requirements, ensuring privacy compatibility within the network environment. The proposed system addresses security complexities by dividing its implementation into three main components: OSN platform creation, privacy management in social networks, and organizational privacy control, including network management and authentication. Recent studies have highlighted advanced retrieval techniques that improve data accuracy and minimize IL [7, 8]. These methods incorporate optimized algorithms that significantly reduce content retrieval time, thus providing a more efficient and secure user experience on large-scale OSNs. The contributions of this study are:

- Proposes the LSOCV algorithm, offering a scalable, multi-level privacy solution tailored to OSNs.
- Improve key performance metrics by demonstrating significant advances in Privacy Retrieval Accuracy (PRA), reduced Content Retrieval Time (CRT), and minimized Information Loss (IL).
- Highlights the potential for LSOCV to be applied in big data environments, ensuring scalable, efficient privacy-preserving solutions.

II. LITERATURE REVIEW

In recent years, the volume of multimedia content including images, text, audio, and video generated and transmitted worldwide through various social network platforms has grown exponentially [7]. Privacy-preserving data publication methods, such as those described in [9], provide crucial frameworks for ensuring the secure dissemination of user data in social networks while complying with privacy regulations. Daily, millions of users worldwide share vast amounts of private information across platforms such as blogs, wikis, and OSNs. Techniques such as exploiting OSNs to provide privacy in personalized web searches, as demonstrated in [10], offer effective ways to balance user privacy with the need for personalized content in online social networks.

Dynamic privacy-preserving mechanisms enhance the protection of user data in dynamic OSNs, ensuring secure data sharing and reducing privacy risks [11]. However, privacy concerns arise in this process, as sensitive information, such as user content preferences, can be collected and exposed to third-party servers [12]. Current privacy-preserving methods for collaborative filtering often compromise either accuracy or efficiency, making them inadequate for large-scale social networks with substantial user bases. In the digital age, the surge in multimedia content, ranging from images, text, audio, and videos shared on social networking platforms, has increased dramatically. As experts highlight, the exponential growth of this content brings significant privacy concerns, particularly in the way it is transmitted and shared across platforms. Users are increasingly sharing sensitive personal information daily through platforms such as blogs, Wikis, and OSNs, and these interactions must be safeguarded to prevent misuse or unauthorized access [13]. In response, governments, corporations, and online communities are focusing on providing more secure and privacy-oriented services, often enforced through stricter regulations.

Technological innovations such as big data, cloud computing, and the semantic web have paved the way for the advancement of more sophisticated social web services. These technologies allow for more efficient data storage and processing, fostering the growth of social networks but also intensifying concerns regarding the privacy of users' shared content. In particular, cloud computing, with its distributed nature, raises questions about data ownership, jurisdiction, and compliance with regional privacy laws, such as the General Data Protection Regulation (GDPR).

Many social networks use recommender systems that rely on collaborative filtering techniques to provide personalized content to users. This method examines user behaviors and preferences to suggest content based on what users with similar interests like. However, this process raises privacy concerns, as it involves the collection and processing of potentially sensitive user data. The recommendations are generated by collecting information such as users' browsing habits, interactions, and preferences, which are stored and analyzed, creating privacy risks. If this data is mishandled or accessed by unauthorized parties, it can lead to breaches of personal information.

Despite the benefits of collaborative filtering, privacy-preserving techniques remain a challenge, particularly in large-scale networks. Privacy-preserving distributed clustering techniques, such as the one proposed in [14], offer a scalable and efficient method of protecting data in large-scale networks, balancing both accuracy and privacy. Maintaining a balance between privacy, efficiency, and accuracy remains a significant hurdle. Advanced techniques such as homomorphic encryption or differential privacy are explored to address these concerns, but they still face scalability and computational resource challenges when applied to large OSNs. As a result, research on collaborative privacy-preserving filtering continues to be an evolving area that aims to offer better protection to users without compromising the performance of recommendation systems. The existing literature lacks a comprehensive privacy-preserving solution that efficiently balances accuracy, retrieval speed, and information loss in large-scale OSNs. Although methods such as PPK-MEANS and CFCAF address specific aspects, they fall short in scalability and adaptability, underscoring the need for an advanced, multi-layered approach such as LSOCV.

III. PROPOSED SYSTEM

This section details the proposed method, outlining the preprocessing steps required for implementation and exploring the algorithm with both functional and logical details. Figure 1 shows the LSOCV algorithm, providing a diagrammatic representation of its architecture and demonstrating the step-by-step privacy management of user content and profiles in OSNs. The method also includes techniques that allow users to form friendships or relationships with others without compromising their privacy or revealing sensitive profile and content information. This figure depicts the process where a data contributor enters user profile information, including preferences and insights, which are then categorized and grouped based on their characteristics. Tiered privacy settings are applied to the grouped data, ensuring that sensitive information is protected according to the required level of privacy. The system suggests appropriate privacy settings to the contributor and checks their security compatibility to ensure that they align with the platform's security protocols. Once verified, the content and its corresponding privacy settings are saved in the OSN. Meanwhile, users can register or log in to the platform, where they can access the available content, depending on the privacy settings defined by the data contributor.

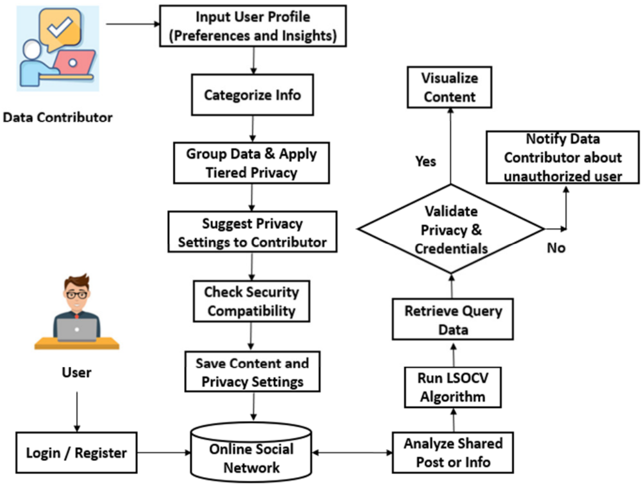
Data Contributor
Input User Profile (Preferences and Insights)
Categorize Info
Group Data & Apply Tiered Privacy
Suggest Privacy Settings to Contributor
Check Security Compatibility
Save Content and Privacy Settings
User
Login / Register
Online Social Network
Analyze Shared Post or Info
Run LSOCV Algorithm
Retrieve Query Data
Validate Privacy & Credentials
Yes
No
Visualize Content
Notify Data Contributor about unauthorized user

Fig. 1. Architecture of the proposed model.

Additionally, the figure illustrates the process of data categorization, privacy setting application, and security validation within the LSOCV framework. It provides a step-by-step overview from user registration to content retrieval, with mechanisms to notify contributors in case of unauthorized access attempts. This section highlights how LSOCV dynamically manages privacy based on user input and security checks.

Before a user can visualize the content, the system validates its privacy level and credentials. If the user meets the required criteria, the content is retrieved for visualization. However, in case of an unauthorized access attempt, the system promptly notifies the data contributor. The platform also incorporates an LSOCV algorithm to analyze shared data, ensuring that only valid and appropriate content is presented to the user. This final analysis ensures that user access aligns with the content's privacy settings, and only then the user can interact with the shared information. The entire process emphasizes a balance between data sharing and privacy, safeguarding the contributor's content through layered security and validation mechanisms.

The system targets users with a high trust score who unexpectedly exhibit malicious behavior, optimizing security levels to mitigate such users under privacy controls. The user's trust is derived from their profile, which incorporates various social attributes. Suppose denoting the users as U_i for the i^{th} user, V_j the j^{th}, and $Q(U_i, V_j)$ the similarity between the profiles of users U_i and V_j. Here, T_j represents the total reputation of user V_j, while G_j is the global trust level of V_j. Parameters

β_1, β_2, β_3 are used to assign different weights to various factors. The trust based on the user profile is computed using:

$$P_{ij} = \beta_1 . Q\left(U_i, V_j\right) + \beta_2 . T_j + \beta_3 . G_j \qquad (1)$$

The similarity between users U_i and V_j is calculated using:

$$Q\left(U_i, V_j\right) = \sum_{\sigma=1}^{n} Q\left(U_{i,\sigma}, V_{j,\sigma}\right) \qquad (2)$$

The total reputation of user V_j is expressed using:

$$T_j = \gamma_1 . p\left(U_i, V_j\right) + \gamma_2 . s\left(u_j\right) \qquad (3)$$

Here, γ_1 and γ_2 represent weights on different aspects, where $p\left(U_i, V_j\right)$ indicates V_j user's reputation from user's U_i viewpoint, and $s\left(u_j\right)$ refers to the user's standing within the group. The global trust level for user V_j across all groups is given by:

$$G_j = \sum_{k=1}^{m} h_k\left(v_j\right) \qquad (4)$$

where $h_1\left(v_j\right), h_2\left(v_j\right), \ldots, h_m\left(v_j\right)$ correspond to user's V_j trust level in various social circles. In social bookmarking, this framework is commonly applied, modeling trust through content interactions. The content-level trust model incorporates multiple features to evaluate trust within social networks. Let CT_k represent the k^{th} content and CT_{ij} denote the trustworthiness of V_j concerning content CT_k from user's U_i perspective. The trust level on content is computed using:

$$Trust_{ij,k} = PT_{ij,k} . Trust_j(CT_k) \qquad (5)$$

where $PT_{ij,k}$ is a parameter that describes the influence of U_i's perception of V_j's trustworthiness on content CT_k.

```
Algorithm: Layered Secure Online
Collaborative Verification (LSOCV)
Browse(OSN)
Register(User)
Collect($U_i$:interests, opinions,
    professional data)
Store(UP $\vee$ ONUP) → Database
Categorize(UP)
ApplyPrivacy(UP) = $\sum_{i=1}^{n} P_i . Level(i)$
Verify(UP) $\wedge$ Request(OSN)
Authenticate(UP) →
    ControlAccess(Application)
Contribute($U_i$ → InformationShare)
VerifyPrivacy(Application,UP)
If PrivacyValid(UP) ⇒ Allow(Access)
Else Alert($U_i$) → VerifyCredentials($U_i$)
Search(OSN,Content,UP)
If ContentAccessValid(UP)
    ⇒ GrantAccess(Information)
Else BlockUnauthorizedUser $\vee$
    NotifyDataProvider
EndProcedure
```

The proposed LSOCV algorithm ensures comprehensive end-to-end security within an OSN environment. It predicts the User Profile (UP) or Organizational Network User Profile (ONUP) by considering attributes such as genetic data, preferences, opinions, and credentials to enforce privacy measures. The algorithm processes shared content in OSNs and applies privacy settings based on these user profiles. During the data submission process, it prompts the user to apply specific privacy rules on User Data Protection (UDP) and also provides restrictions for the user or group based on the credibility and opinions surrounding the shared content.

In the Secure Content Retrieval (SCR) phase, users can search and retrieve data of any type, provided that their credentials are validated. If the user satisfies the verification criteria required, the algorithm proceeds with SCR for content retrieval. Otherwise, it flags the user as unauthorized and alerts the data provider. This approach not only reduces IL and improves CRT but also enhances the accuracy of privacy settings.

The LSOCV algorithm optimizes security through layered privacy, ensuring that access permissions align with user-specific requirements on the social network. The process actively verifies privacy compatibility to prevent potential security complexities, allowing information to be shared only with the intended recipients while protecting other sensitive data. Additionally, the method allows users to explore and retrieve content without risking their privacy, reinforcing secure access and authentication mechanisms across the platform. The algorithm also mitigates cyber-crime risks by giving the data owner control over monitoring and managing user activities. It also encourages responsible data-sharing practices, ensuring that users and data contributors operate under secure, monitored conditions in the network environment.

IV. RESULTS AND DISCUSSIONS

Various evaluation metrics were used to measure the efficiency of the proposed algorithm compared to existing methods in an OSN environment. Key evaluation parameters include:

- Accuracy: Evaluates how well the method predicts user data accurately, with higher scores indicating better performance.
- Content Retrieval: Measures the time required for content retrieval, incorporating both system performance and user network responses.
- Information Loss (IL): Assesses data distortions that impact data quality during privacy-preserving data sharing. Lower information loss signifies better efficiency and security of the proposed mechanism.

Table I presents PRA, CRT, and IL metrics for data sizes of 500KB, 1MB, and 10MB to evaluate privacy efficiency and accuracy within OSN environments. The proposed LSOCV method was evaluated in comparison with the following existing techniques: Privacy-Preserving K-Means Clustering Algorithm (PPK-Means), Collaborative Fuzzy Co-cluster Analysis Framework (CFCAF), and Cluster-based L-diversity Privacy Preservation (CLDPP). The evaluation of the four algorithms PPK-MEANS, CFCAF, CLDPP, and LSOCV was carried out using MATLAB. The tests were performed on a high-performance computing system with Intel Xeon processors and 64 GB of RAM. MATLAB's robust capabilities enabled efficient handling of large-scale data and computations. All algorithms were executed under the same network conditions to ensure fairness in comparing metrics such as PRA, CRT, and IL. The bar graph in Figure 2 presents the PRA for different file sizes (500 KB, 1 MB, and 10 MB) across four algorithms: PPK-MEANS, CFCAF, CLDPP, and LSOCV. As file size increases, PRA also shows a general upward trend for all algorithms, with LSOCV consistently achieving the highest accuracy across all file sizes, followed by CLDPP, CFCAF, and PPK-MEANS. This comparison highlights the efficiency of LSOCV in handling various data sizes in terms of privacy retrieval accuracy.

TABLE I. PERFORMANCE ANALYSIS OF LSOCV

Dataset/ Algorithms	File size (500 KB)		
	PRA (%)	**CRT (ms)**	**IL (%)**
PPK-MEANS	63.25	15	22
CFCAF	74.55	15	19
CLDPP	82.43	10	16
LSOCV	91.96	8	9
Dataset/ Algorithms	**File size (1 MB)**		
	PRA (%)	**CRT (ms)**	**IL (%)**
PPK-MEANS	65.49	22	23
CFCAF	76.56	19	22
CLDPP	84.55	17	17
LSOCV	93.37	12	12
Dataset/ Algorithms	**File size (10 MB)**		
	PRA (%)	**CRT (ms)**	**IL (%)**
PPK-MEANS	67.53	26	26
CFCAF	78.25	23	22
CLDPP	86.23	18	16
LSOCV	95.38	14	14

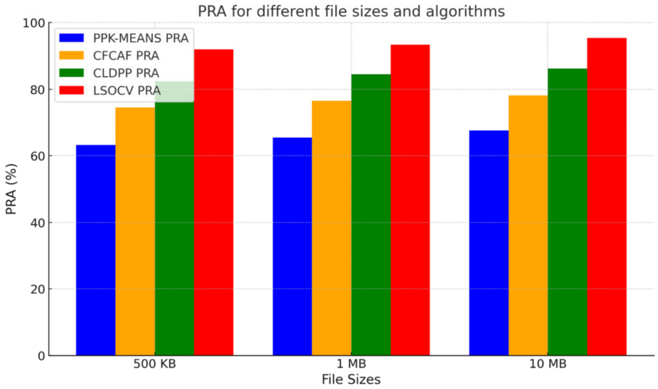

Fig. 2. Comparison of PRA with varying file sizes.

Figure 3 illustrates the performance of the four algorithms across three file sizes (500 KB, 1 MB, and 10 MB). Accuracy was measured on a scale of 0 to 100%, and the results show that LSOCV consistently outperformed the other methods, with a slight increase in accuracy as the file size increased. CLDPP and CFCAF followed a similar trend with moderate performance, while PPK-MEANS showed the lowest accuracy overall.

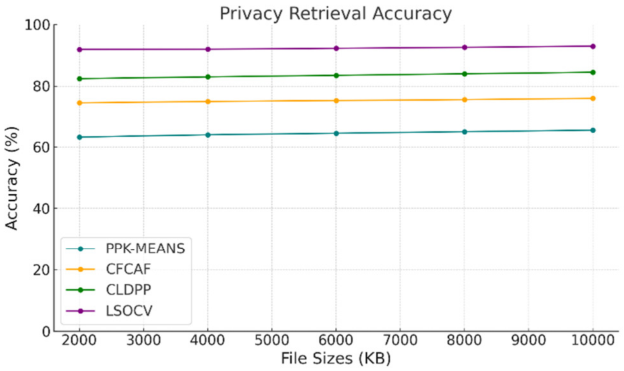

Fig. 3. Accuracy comparison with varying file sizes.

Figure 4 shows the CRT for different file sizes (500KB, 1MB, and 10MB) for the four algorithms. LSOCV consistently demonstrated the lowest retrieval time, indicating better performance, while PPK-MEANS had the highest retrieval times, especially as the file size increased. Overall, LSOCV was the most efficient in terms of CRT.

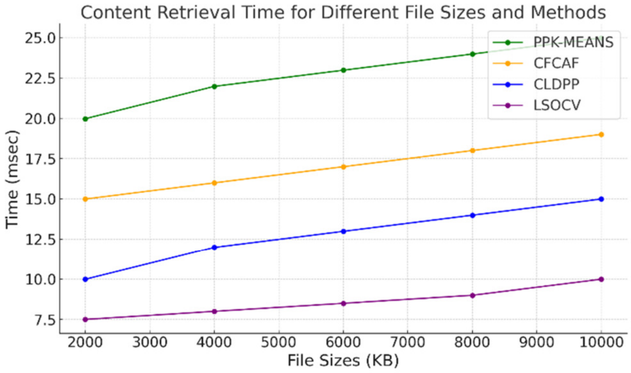

Fig. 4. Comparison of Content Retrieval Time (CRT) with varying file sizes.

Figure 5 shows the IL (%) for different file sizes for the four algorithms. PPK-MEANS had the highest information loss, which increased with file size, while LSOCV demonstrated the lowest IL, making it the most efficient algorithm for preserving data quality. CLDPP and CFCAF were between the two, with moderate levels of IL. This graph highlights LSOCV's superior performance in minimizing IL across all file sizes. The LSOCV algorithm consistently outperformed previous algorithms such as PPK-MEANS, CFCAF, and CLDPP across several key metrics. In terms of PRA, LSOCV achieved the highest accuracy, demonstrating its effectiveness in retrieving sensitive data while maintaining privacy. Furthermore, LSOCV had the fastest CRT, indicating greater efficiency in accessing data compared to other methods, which experienced slower performance as file sizes increased. Additionally, LSOCV exhibited the lowest IL, ensuring better data quality during privacy-preserving processes. This method proves to be a superior solution for privacy-preserving tasks in online environments, balancing accuracy, speed, and data integrity better than other approaches.

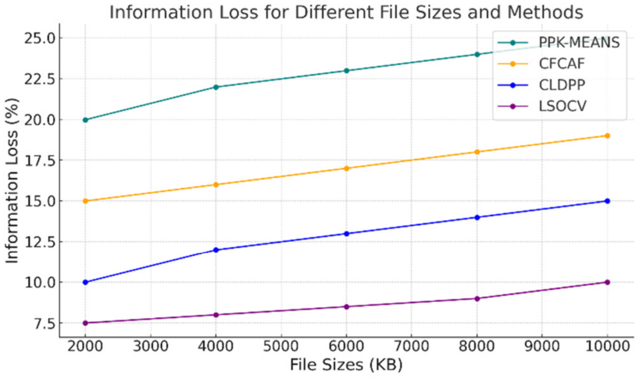

Fig. 5. IL (%) comparison with varying file sizes.

The LSOCV algorithm offers a robust alternative to existing privacy-preserving techniques for OSNs. Unlike traditional methods such as PPK-MEANS, which cluster data without adapting to user needs, LSOCV integrates a multilevel security framework that customizes privacy settings based on content sensitivity. This adaptability yields a higher PRA, with LSOCV achieving 95.38% accuracy for larger files compared to 86.23% by CLDPP. Additionally, CFCAF uses fuzzy co-clustering, which can introduce complexity and slow retrieval, while LSOCV optimizes CRT by associating access controls with predefined privacy levels, reducing CRT to 14 ms for 10 MB files compared to CFCAF's 23 ms. By focusing on layered privacy and customized content management, LSOCV minimizes IL to 9% for smaller datasets, outperforming other methods and providing a balanced solution in terms of security, efficiency, and accuracy for managing privacy in OSNs.

V. CONCLUSION

The proposed LSOCV method was designed to address privacy concerns during content sharing and data visualization. It implements a multilevel privacy approach tailored to user requirements within social networks, following an assessment of the application's privacy compatibility. The LSOCV algorithm enables users to experience tiered security in OSNs, with access varying by level. At the public level, general and non-personal information is accessible, while at the private and protected levels, personal and sensitive data can also be accessed. This method provides organization-specific privacy controls and authentication mechanisms for data contributors and users in social networking environments. In addition, it effectively decreases IL and CRT while improving PRA. Specifically, the proposed method achieved a PRA of 91.97%, which exceeded that of existing methods for file sizes of 500 KB. In terms of CRT, LSOCV recorded 7 ms, significantly lower than other approaches used for the same file size. Furthermore, the method reduced IL by up to 8% compared to competing algorithms. In general, LSOCV improved PRA by 9.13%, decreased CRT by 7 ms, and reduced IL by 5.33%. Future work may extend the application of privacy-preserving techniques to big data environments, such as Hadoop, without compromising data accuracy or retrieval speed.

REFERENCES

[1] H. K. Bhuyan and N. K. Kamila, "Privacy preserving sub-feature selection in distributed data mining," *Applied Soft Computing*, vol. 36, pp. 552–569, Nov. 2015, https://doi.org/10.1016/j.asoc.2015.06.060.

[2] A. F. Khalil and S. Rostam, "Machine Learning-based Predictive Maintenance for Fault Detection in Rotating Machinery: A Case Study," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13181–13189, Apr. 2024, https://doi.org/10.48084/etasr.6813.

[3] A. S. Q. Syed, C. Atheeq, L. Ali, and M. T. Quasim, "A Chaotic Map-based Approach to Reduce Black Hole Attacks and Authentication Computational Time in MANETs," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 13909–13915, Jun. 2024, https://doi.org/10.48084/etasr.7073.

[4] G. Alotibi, "A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13787–13795, Apr. 2024, https://doi.org/10.48084/etasr.7123.

[5] L. Bahri, B. Carminati, and E. Ferrari, "Decentralized privacy preserving services for Online Social Networks," *Online Social Networks and Media*, vol. 6, pp. 18–25, Jun. 2018, https://doi.org/10.1016/j.osnem.2018.02.001.

[6] K. Berlin, D. Slater, and J. Saxe, "Malicious Behavior Detection using Windows Audit Logs," in *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security*, Denver, CO, USA, Oct. 2015, pp. 35–44, https://doi.org/10.1145/2808769.2808773.

[7] S. Khalid, S. Wu, A. Alam, and I. Ullah, "Real-time feedback query expansion technique for supporting scholarly search using citation network analysis," *Journal of Information Science*, vol. 47, no. 1, pp. 3–15, Feb. 2021, https://doi.org/10.1177/0165551519863346.

[8] S. Khalid, S. Khusro, I. Ullah, and G. Dawson-Amoah, "On The Current State of Scholarly Retrieval Systems," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3863–3870, Feb. 2019, https://doi.org/10.48084/etasr.2448.

[9] J. H. Abawajy, M. I. H. Ninggal, and T. Herawan, "Privacy Preserving Social Network Data Publication," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1974–1997, 2016, https://doi.org/10.1109/COMST.2016.2533668.

[10] A. Erola, J. Castellà-Roca, A. Viejo, and J. M. Mateo-Sanz, "Exploiting social networks to provide privacy in personalized web search," *Journal of Systems and Software*, vol. 84, no. 10, pp. 1734–1745, Oct. 2011, https://doi.org/10.1016/j.jss.2011.05.009.

[11] T. Zhu, J. Li, X. Hu, P. Xiong, and W. Zhou, "The Dynamic Privacy-Preserving Mechanisms for Online Dynamic Social Networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 6, pp. 2962–2974, Jun. 2022, https://doi.org/10.1109/TKDE.2020.3015835.

[12] S. Weifeng, S. Mingyang, L. Xidong, and L. Mingchu, "An Improved Personalized Filtering Recommendation Algorithm," *Applied Mathematics & Information Sciences*, vol. 5, no. 5–2, pp. 69–78, 2011.

[13] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 3015–3045, 2017, https://doi.org/10.1109/COMST.2017.2718178.

[14] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Privacy-preserving distributed clustering," *EURASIP Journal on Information Security*, vol. 2013, no. 1, Nov. 2013, Art. no. 4, https://doi.org/10.1186/1687-417X-2013-4.

[15] K. Honda, T. Oda, D. Tanaka, and A. Notsu, "A Collaborative Framework for Privacy Preserving Fuzzy Co-Clustering of Vertically Distributed Cooccurrence Matrices," *Advances in Fuzzy Systems*, vol. 2015, no. 1, 2015, Art. no. 729072, https://doi.org/10.1155/2015/729072.