Discover Engineering
An International Journal
OPEN ACCESS
ISSN 3117-566X
Original Research Article
Check for updates

Optimizing Average Path Length and Information Loss in Social Networks Using CS-ANN-Based Cuckoo-Neural Models

Sudam Chetry*, Mohini Dwivedi, Alok Singh, and Akash Saxena

Department of Information Technology, Shridhar University, Chirawa, Rajasthan, India

Corresponding author: **Sudam Chetry** | E-mail: **sudamchetry@gmail.com**

Citation: Sudam Chetry, Mohini Dwivedi, Alok Singh, and Akash Saxena (2025). Optimizing Average Path Length and Information Loss in Social Networks Using CS-ANN-Based Cuckoo-Neural Models. *Discover Engineering: An International Journal.*
DOI: https://doi.org/10.51470/DE.2025.6.2.05

Received 07 July 2025 | Revised 11 August 2025 | Accepted 13 September 2025 | Available Online 06 October 2025

Abstract

Although social networks increase connectivity, they often risk sensitive data, requiring strong privacy-protection safety measures. Cuckoo-neural and cuckoo-SVM are hybrid models that integrate the cuckoo with artificial nerve networks; This study sees how well these models preserve privacy in social networks. The focus of this research is to improve data transfer efficiency by reducing information loss and increasing the length of the average process. To compare new and old models, this work uses Arnet, Cora and DBLP datasets to manufacture CS-ANN and CS-SVM methods. More than 10 to 500 nodes were conducted by information loss and average path length (APL), methods were held on cuckoo-neural and cuckoo-SVM platforms. The results suggest that cuckoo-neural regularly with CUCKO-SVM and pre-research with CS-ANN, with significant reduction in information loss and 31.34% in APL. Finally, the proposed cuckoo-neural model, which is based on CS-N, shows better privacy security efficiency and offers an alternative to unsafe and disabled social network contacts.

Keywords: *Social Networks; Information Loss; Average Path Length; Artificial Neural Networks.*

Introduction

In this era of universal digital connectivity, social networks are indispensable to share information, cooperate and communicate; Nevertheless, they also present important challenges to protect personal information and privacy [1, 2]. Unauthorized access, data agreements and cyber attacks are risks that users encounter due to the increasing flow of sensitive individual and commercial data through these networks. Due to the importance of reducing data loss while maintaining efficient data transmission, privacy-conservation approach has become an important area of study [2, 3, 4]. Hybrid models that combine machine learning techniques such as SVM and Artificial Neural Network (ANNS), with biology - inspired adaptation algorithms, such as cuckoo search (CS), offer exciting new possibilities to solve these problems [3, 4, 5]. These mixed models aim to adapt network characteristics such as the average path length (APL) to communicate safely and efficiently. CS-ANN and CS-SVM libraries are being used to compare and vice versa in this proposed study to compare how well they perform on Arnet, Cora, and DBLP, three social networks datasets. By evaluating important matrix such as APL and information loss, this study hopes to show that cuckoo-nural pairing works better than others. This data will reduce the hazards of exposure, improve network efficiency, and security will provide a practical way to social network operations.

Cyber security risk, including data violations, social engineering attacks and illegal access to [5,6,7], has increased considerably due to increasing dependence on social media platforms. Based on research, it is often necessary to employ more advanced approaches such as machine learning (ML) and natural language processing (NLP) because existing security methods are unable to handle these new challenges [6,8,9]. Using methods of natural language processing [6,9] can be detected with the forecast capabilities of suspected behavior trends in large datasets and machine learning approaches identified with PIIs (individually identified). To improve the accuracy of the danger detection, to reduce data loss and strengthen network safety as a whole, research suggests that a combination of ML and NLP may be useful by hybrid framework [5,6]. For the protection of user data within social networks, it is necessary to provide safe protection to active security privacy techniques, as systematic assessment suggests that social media hacking is still a major vector for dangers [7,8]. According to the broad assessment of social network security [8], it is important to integrate intelligent and computerized methods for real -time monitoring, risk evaluation and abolition. All the literature highlight the necessity of modern cyberspace protection tools such as machine learning (ML) and natural language processing (NLP), which provide scalable and efficient methods of ensuring the safety of sensitive information, preventing cyber-attacks and guaranteeing user confidence in dynamic online environments [5-9].

Research Gap

In spite of the attempts made in developing privacy-sensitive approaches to the development of social network, there are still some gaps in the current literature. The traditional methods such as k-anonymity, l-diversity, and differential privacy often cause much loss of information and fail to increase the network efficiency, particularly in large social networks. In spite of the fact that hybrid models that combine machine learning and bio-inspired optimization algorithms like Cuckoo Search have potential, in most datasets comparative analyses of Cuckoo-Neural (CS-ANN) and Cuckoo-SVM methodologies have not been made [6-9]. Moreover, the majority of studies concentrate on optimizing Average Path Length (APL) or minimizing information loss, never addressing both concurrently, hence creating a deficiency in thorough performance assessment. The predominant body of research is assessed using synthetic or small-scale datasets, which constrains its applicability to real-world social networks [7,8]. Consequently, systematic research is required to systematically compare the CS-ANN and CS-SVM frameworks, assess their effects on both APL and information loss, and confirm performance across various real-world datasets to provide an efficient and scalable privacy-preserving solution.

Methodology

This study's methodology centres on the development and assessment of hybrid privacy-preserving frameworks for social networks, with a specific comparison of the Cuckoo-Neural (CS-ANN) and Cuckoo-SVM models. Initially, real-world social network datasets such as ARNET, CORA, and DBLP were chosen to guarantee diverse and representative network architectures. Both CS-Ann and CS-SVM tools optimize network parameters and increase data protection by adding coal discovery (CS) adaptation method with artificial nerve network (Ann) and support vector network (SVM). To begin, for each dataset, research creates a communication network in which individuals and edges with nodes represent their interaction. Data loss and average path length (APL) are the major performance indicators calculated from the graph. To reduce data exposure, CS algorithm is used to find optimal data transfer pathway. To prevent and prevent possible data violations, ANN and SVM algorithms are used to assess these paths. To evaluate scalability and safety, research was held with different numbers of nodes, from 10 to 500. To highlight the reforms, we compared our method to well-established people, such as GA-based and Ke-Enemity Models. The results were shown to be reliable after statistical analysis to determine the relevance of changes in APL with data loss. To assess how well the CS-ANN and CS-SVM enhanced oblivion and network efficiency, this method of analysis provides a logical structure.

Results and Discussion

When looking at different social network datasets side by side, the Cuckoo-Neural (CS-ANN) and Cuckoo-SVM classification models show significant improvements in Absolute Path Length (APL) and information loss.

As shown in Figure 1, the ARNET dataset was used to evaluate APL values for node ranges ranging from 10 to 500. Because there are more intermediate connection points with more nodes, the results show that APL increases as the number of nodes increases. With an average APL of 0.92, the CS-ANN-based Cuckoo neural model outperformed CS-SVM (0.996) and earlier research (1.19 and 1.34), showing improvements of 22.69% and 31.34%, resp. In the CORA dataset, the Cuckoo-Neural model regularly yielded lower APL values, such as 0.65 for 10 nodes compared to 0.85 for Cuckoo-SVM, so affirming its superior shortest-path efficiency. In the DBLP dataset, CS-ANN surpassed CS-SVM, achieving average APL values of 0.756 compared to 0.936, indicating a 19.23% enhancement. The ARNET dataset exhibited average information loss values of 30.76 for CS-ANN, 31.9 for CS-SVM, and 33.37 and 34.72 for earlier models, indicating a reduction of up to 11.41% compared to CS-SVM. CS-ANN, in the case of the CORA dataset, also achieved the average information loss of 23.89, compared to a 20.92-29.61% increase in average information loss over current methodologies. These trends were confirmed in the DBLP dataset, as the CS-ANN model showed a consistent decrease in information loss in all range of nodes. All these findings substantiate that the Cuckoo-Neural architecture is the most successful in reducing the length of communication channels, as well as improving the data integrity more efficiently as compared to CS-SVM and other privacy-preserving techniques,
which makes it the best model of all learners that have been measured against the datasets.

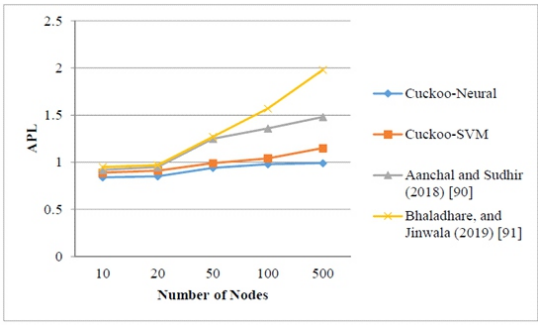

Figure 1: Comparison of APL observed for ARNET dataset

The results of this research are in line with the current study on social network privacy and security, which highlights the effectiveness of hybrid intelligent models. Jain et al. [8] have pointed out the inefficacy of the conventional privacy-preserving schemes, which often leads to severe information loss, and addressed the issue by the CS-ANN-based Cuckoo-Neural model with reduced APL and minimal data leakage. The predictive power is discovered in our system by Oye et al. [9], which demonstrated that the combination of NLP and ML makes threats easier to detect and protect the data. The same conclusions were made by Bikku et al. [10], who stressed the need to have privacy-saving solutions in an online community, which is consistent with our findings that CS-ANN outperforms CS-SVM and other current models in different datasets.

Conclusion

This paper explains that Cuckoo-Neural model using CS-ANN provides a robust and efficient privacy protection approach in the social network. The comparison of ARNET, CORA, and DBLP datasets revealed that the suggested model will always outperform CS-SVM and the current approaches to reducing Average Path Length (APL) and information loss. The findings prove its ability to increase data transfer in addition to maintaining data integrity that makes it suitable in large networks. The research supports the claim that Cuckoo Search combined with neural networks enhances the efficiency and security of the network, as it is a valid and scalable tool to safeguard sensitive information on social sites.

References

1. Marinho, R., & Holanda, R. (2023). Automated emerging cyber threat identification and profiling based on natural language processing. IEEE Access, 11, 58915-58936.
2. Sousa, S., & Kern, R. (2023). How to keep text private? A systematic review of deep learning methods for privacy-preserving natural language processing. Artificial Intelligence Review, 56(2), 1427-1492.
3. Khader, M., & Karam, M. (2023). Assessing the effectiveness of masking and encryption in safeguarding the identity of social media publishers from advanced metadata analysis. Data, 8(6), 105.
4. Alsmadi, I., Ahmad, K., Nazzal, M., Alam, F., Al-Fuqaha, A., Khreishah, A., & Algosaibi, A. (2022). Adversarial NLP for social network applications: attacks, defenses, and research directions. IEEE transactions on computational social systems, 10(6), 3089-3108.
5. Jha, R. K. (2023). Strengthening smart grid cybersecurity: An in-depth investigation into the fusion of machine learning and natural language processing. Journal of Trends in Computer Science and Smart Technology, 5(3), 284-301.
6. Mainetti, L., & Elia, A. (2025). Detecting Personally Identifiable Information Through Natural Language Processing: A Step Forward. Applied System Innovation, 8(2), 55.
7. Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. IEEE access, 10, 39325-39343.
8. Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157-2177.
9. Oye, E., Peace, P., & Owen, J. (2024). The Role of Natural Language Processing in Cybersecurity.
10. Bikku, T., Biyyapu, N. S., Sekhar, J. C., Kumar, M. K., Nokerov, S. M., & Pratap, V. K. (2024). The Social Network Dilemma: Safeguarding Privacy and Security in an Online Community. International Journal of Safety & Security Engineering, 14(1).