International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

# COMPOSITE BEHAVIORAL MODELING FOR IDENTITY THEFT DETECTION IN ONLINE SOCIAL NETWORKS

[1]CHAKINALA SRILEKHA,[2]BURPALLY BHAVANA,[3]KANCHARLA BHARGAV KRISHNA,[4]NANDI KONDA PRANAY VIKRAM REDDY,[5]DR. S.RAJA GOPAL REDDY

[1,2,3,4]Students, Department of computer Science And Engineering, Malla Reddy Engineering College,Hyderabad,Telangana, India 500100

[5]Professor,Department Of Computer Science And Engineering,Malla Reddy Engineering College,Hyderabad,Telangana, India 500100

## ABSTRACT

With the explosive growth of Online Social Networks (OSNs), identity theft has become a pressing cybersecurity concern. Malicious users often impersonate others or steal credentials to conduct fraudulent activities, exploit personal information, or launch phishing campaigns. Traditional detection systems based solely on static features or rule-based mechanisms fall short in capturing complex and evolving user behaviors. This project introduces a Composite Behavioral Modeling (CBM) framework for identity theft detection in OSNs. The model integrates both individual behavioral patterns (such as posting frequency, friend interactions, and login timing) and community-level features (e.g., group dynamics, social interactions) to build a holistic profile of user activity. By leveraging machine learning algorithms—such as Random Forest, Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) networks—our system dynamically identifies anomalous behavior that deviates from a user's typical pattern. The model is trained on labeled datasets from social media activity logs and validated through performance metrics including precision, recall, and AUC. Experimental results demonstrate that the CBM approach significantly enhances detection accuracy and reduces false positives, offering a robust solution to safeguarding digital identities in social platforms.

**Keywords: Identity Theft, Online Social Networks, Composite Behavioral Modeling, Anomaly Detection, Machine Learning, User Profiling, Cybersecurity, Social Media Security, Behavioral Analytics, LSTM, Random Forest, Support Vector Machine (SVM), Feature Engineering, Fraud Detection, User Behavior Modeling**

## I.INTRODUCTION

In the digital era, Online Social Networks (OSNs) such as Facebook, Twitter, Instagram, and LinkedIn have become essential platforms for communication, information sharing, and community building. While these platforms have enhanced global connectivity, they have also introduced significant security risks—most notably, **identity theft**. Cybercriminals exploit user trust by creating fake profiles, hijacking accounts, and impersonating others to gain unauthorized access to personal data or carry out fraudulent activities. Identity theft not only threatens individual privacy and reputation but also undermines the trustworthiness of social platforms. Traditional security mechanisms such as password protection, two-factor

authentication, and manual moderation are often insufficient to detect sophisticated and evolving threats in real time. Moreover, many detection systems rely on static or surface-level data, ignoring deeper behavioral patterns that may signal impersonation or malicious intent. To address this gap, **behavioral modeling** has emerged as a promising approach to detect anomalies based on how users typically interact on a platform. This project proposes a **Composite Behavioral Modeling (CBM)** approach that combines both individual and community-level behavioral features to build dynamic user profiles. By analyzing factors such as login patterns, content engagement, communication frequency, and social graph changes, the system can learn what constitutes normal user behavior and flag deviations that may indicate identity theft. Through the integration of advanced machine learning techniques—such as **Random Forest**, **Support Vector Machines (SVM)**, and **Long Short-Term Memory (LSTM)** networks—our solution aims to detect suspicious activities with high accuracy and low false-positive rates. The proposed system not only enhances **cybersecurity** for OSNs but also contributes to the broader field of user behavior analytics, offering scalable and intelligent solutions to the growing problem of digital identity fraud.

## II.LITERATURE REVIEW

The exponential growth of Online Social Networks (OSNs) has created a fertile environment for cybercriminal activities, especially **identity theft**, which poses severe threats to both individual users and platform integrity. Numerous research efforts have focused on detecting and preventing such threats, with varying degrees of success.

Early studies on identity theft detection relied primarily on **rule-based systems** and **signature detection mechanisms**, which are effective for known attack patterns but struggle with new or evolving threats. For instance, Al-Zahrani et al. (2017) explored anomaly detection using predefined behavioral rules to identify impersonation. However, their approach suffered from high false-positive rates and limited adaptability.

Recent advancements have introduced **machine learning (ML)** into the domain, enabling dynamic and adaptive models capable of learning complex behavioral patterns. Bhargava and Mehrotra (2019) utilized Support Vector Machines (SVM) for identifying suspicious login behaviors in OSNs, demonstrating improved detection accuracy. Similarly, Zhang et al. (2020) employed **Random Forest classifiers** to detect abnormal posting behaviors and content similarities, providing a more robust method to uncover identity misuse.

Other researchers have explored **graph-based models** to examine social relationships and interaction patterns. These models analyze users' social graphs to detect sudden deviations in network structure, such as unusual friend requests or follower spikes. Jiang and Wang (2018) applied graph clustering techniques to identify fake accounts that mimic real users.

More recent approaches emphasize **behavioral biometrics**, where systems learn from users' interaction habits such as typing speed, posting frequency, and browsing patterns. Techniques like **Long Short-Term Memory (LSTM)** networks, as proposed by

Choi et al. (2021), are particularly effective in modeling temporal behavior, making them suitable for real-time detection systems.

In parallel, **composite behavior modeling** has gained traction, as it merges individual behavior features (e.g., activity timing, message patterns) with group-level features (e.g., community interactions, mutual connections). This hybrid approach improves the accuracy of anomaly detection by providing a more holistic view of user activities, as highlighted in the work of Shukla et al. (2022), who demonstrated that combining personal and social behavior metrics significantly enhances detection precision. Despite these advancements, several challenges persist—such as **data sparsity**, **privacy concerns**, and the **adaptive nature of attackers**. Therefore, current research is shifting toward developing lightweight, privacy-preserving, and real-time detection systems using unsupervised learning and **semi-supervised models**. In summary, while multiple strategies exist to combat identity theft in OSNs, **composite behavioral modeling**, empowered by machine learning and deep learning techniques, offers a promising path toward more accurate, scalable, and intelligent identity theft detection systems.

## III.WORKING METHODOLOGY

The working methodology for identity theft detection in online social networks using composite behavioral modeling is structured around a data-driven, machine learning-based framework. Initially, user data is collected from social networking platforms, including attributes such as login times, friend lists, messaging patterns, post frequency, shared content, and device/browser details. This raw data undergoes preprocessing steps like noise removal, missing value imputation, normalization, and feature encoding to ensure consistency and quality. After preprocessing, feature extraction is performed to capture both individual and social behavioral traits—such as user-specific patterns (e.g., login frequency, session duration) and group-level indicators (e.g., community interaction patterns, sudden changes in friend or follower counts). These features are then used to create composite behavioral profiles for each user.

The next phase involves training machine learning models on these behavior profiles. Supervised learning algorithms like Random Forest, SVM, and Gradient Boosting are applied where labeled data is available, while unsupervised models like K-Means and Isolation Forest are used for anomaly detection in unlabeled datasets. For modeling sequential behaviors and detecting real-time deviations, deep learning models such as Long Short-Term Memory (LSTM) networks are implemented. These models help detect inconsistencies in user behavior that may indicate identity theft, such as a sudden shift in login locations, usage hours, or communication style.

Once trained, the models are evaluated using performance metrics such as accuracy, precision, recall, F1-score, and ROC-AUC to ensure reliability and effectiveness. The final system is deployed to continuously monitor user activity, flagging potentially fraudulent behavior in real-time and alerting administrators or triggering automated verification steps. This holistic approach—combining machine learning, behavior profiling, and anomaly detection—ensures high detection accuracy and adaptability,

making it a robust solution for combating identity theft in online social networks.

## IV.CONCLUSION

In this study, we have proposed a comprehensive and dynamic approach for identity theft detection in online social networks by leveraging composite behavioral modeling. The research emphasizes the importance of analyzing both individual and social behaviors to detect potential fraudulent activities. By integrating multiple machine learning techniques, including supervised learning algorithms and unsupervised anomaly detection models, we have created a robust framework capable of identifying inconsistencies and deviations in user behavior that may signal identity theft. The use of deep learning models like Long Short-Term Memory (LSTM) networks has further enhanced the ability to track and predict sequential patterns, improving real-time detection accuracy.

The findings from our experiments indicate that this approach is effective in detecting anomalous behaviors and can significantly reduce the risk of identity theft. Moreover, the proposed methodology is adaptable to various online social platforms, offering a flexible and scalable solution to protect users from fraudulent activities. By incorporating composite behavior profiles, we have advanced the capability of current detection systems, moving beyond simple rule-based or keyword-based methods. As online social networks continue to grow and evolve, this framework offers a promising way forward in securing digital identities and fostering safer online environments.

## V.REFERENCES

1. Anderson, R., & Agarwal, R. (2017). Cybersecurity in online social networks. Journal of Cybersecurity, 3(4), 311-324.
2. Bursztein, E., A. Boneh, & G. Wang. (2018). Web security for online social networks. IEEE Security & Privacy, 16(1), 47-56.
3. Cha, M., & Govindan, M. (2019). Behavior-based anomaly detection in online social networks. Journal of Computer Networks and Communications, 9(2), 101-113.
4. Chen, S., Zhang, Q., & Wang, J. (2020). Identity theft detection using behavioral analytics on social media. Computers in Industry, 121, 101-112.
5. Das, S., & Mitra, S. (2021). A comparative study on machine learning techniques for fraud detection in social networks. International Journal of Data Science and Machine Learning, 6(3), 55-68.
6. Fang, C., Xu, W., & Zhang, H. (2021). Hybrid approaches to identity theft detection in social networks. IEEE Transactions on Information Forensics and Security, 16(7), 1234-1245.
7. Gupta, A., & Jain, P. (2020). Security threats and fraud detection in online social networks: A survey. International Journal of Information Management, 52, 213-225.
8. Jain, V., & Chakraborty, D. (2020). Machine learning-based approach for identifying anomalous behavior in social media. Pattern Recognition Letters, 135, 104-112.
9. Kaminsky, M., & Smith, J. (2018). Real-time identity theft detection using machine learning. Journal of Information Security, 15(3), 102-115.
10. Kim, Y., & Lee, S. (2019). Anomaly detection in online social networks. IEEE Transactions on Cybernetics, 50(2), 588-601.

11. Kwon, M., & Jung, H. (2018). Social network fraud detection via behavioral analysis. International Journal of Advanced Computer Science and Applications, 9(6), 30-42.
12. Lin, Y., & Zhang, Z. (2017). An efficient fraud detection model for social networks. Journal of Computer Science and Technology, 32(5), 901-914.
13. Luo, H., & Chen, F. (2021). Identifying identity theft in social networks using machine learning. Data Science and Engineering, 6(4), 89-103.
14. Meng, S., & Li, Y. (2020). Detecting identity theft and fraud on online social networks. Proceedings of the International Conference on Data Science and Machine Learning, 29, 88-96.
15. Nguyen, T., & Tran, D. (2019). A survey of fraud detection techniques in social networks. International Journal of Computer Science and Information Technology, 11(3), 78-89.
16. Oren, L., & Tov, S. (2020). Detecting identity theft through behavior-based models. Journal of Information Security, 30(6), 205-214.
17. Park, S., & Yang, D. (2021). Real-time anomaly detection for identity theft in social networks. Security and Privacy, 14(2), 111-122.
18. Ren, K., & Li, Z. (2021). A hybrid deep learning approach for identity fraud detection. Journal of Artificial Intelligence Research, 65(2), 321-335.
19. Shankar, M., & Sundaram, S. (2019). Behavioral modeling for identity theft detection in online communities. Journal of Cybersecurity and Privacy, 5(1), 45-56.
20. Singh, R., & Agarwal, N. (2020). Fraud detection and prevention in social media networks: An AI approach. International Journal of AI & Machine Learning, 13(4), 100-112.
21. Smith, L., & Lee, M. (2018). Detecting identity theft in online social networks using machine learning techniques. Computer Networks, 65, 211-222.
22. Tan, X., & Zhou, Y. (2020). Behavior-based anomaly detection in social networks using machine learning. Journal of Machine Learning Research, 21(4), 1097-1110.
23. Thomas, P., & Wang, X. (2021). Anomaly-based detection of identity theft in online social media networks. Journal of Digital Security, 18(2), 76-85.
24. Wang, S., & Xu, T. (2020). Real-time anomaly detection in social media platforms using machine learning. Proceedings of the IEEE Conference on Security and Privacy, 14, 350-362.
25. Wu, Y., & Zheng, Z. (2021). Detecting fraudulent activity in social media through behavioral analytics. Journal of Artificial Intelligence, 6(2), 102-114.
26. Xie, Z., & Hu, B. (2019). Detection of fraud and identity theft in social media networks using a hybrid machine learning framework. IEEE Transactions on Computational Intelligence, 11(1), 45-57.
27. Yang, P., & Zhao, W. (2020). Predictive modeling of fraud detection in online social networks. Journal of Network and Computer Applications, 45, 123-135.
28. Yu, F., & Li, Q. (2020). Machine learning for identity fraud detection in online social platforms. Journal of Cyber Defense, 23(2), 65-74.
29. Zhang, B., & Wang, Z. (2020). Identity theft detection using behavioral anomaly in social networks. Journal of Information Security and Applications, 56, 66-75.
30. Zhao, Y., & Chen, X. (2021). Leveraging machine learning for identity theft detection in social media. Journal of Data Mining and Knowledge Discovery, 19(4), 334-345.