International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 4 (2025)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 4, 2025
© 2025 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Composite Behavioural Modelling for Identity Theft Detection in Online Social Networks

[1]Sanga Tulasi, [2]Dr.V. Sudarshan

[1]MCA Student, Department Of Master of Computer Applications, Sri Chaitanya Institute Of Technology (Scit), Ponnekal, Khammam

[1]Email:tulasisanga2@gmail.com

[2]Professor, Department Of Master of Computer Applications, Sri Chaitanya Institute Of Technology (Scit), Ponnekal, Khammam

[2]Email:sudharshan.cse@gmail.com

ABSTRACT

The rapid growth of online social networks has significantly transformed the way people communicate, share information, and interact across the world. Popular social networking platforms such as Facebook, Instagram, X (Twitter), LinkedIn, and other online communities store vast amounts of personal information, making them attractive targets for cybercriminals. One of the most serious security threats in these platforms is identity theft, where attackers gain unauthorized access to legitimate user accounts or create fake profiles by stealing personal information and impersonating genuine users. Such attacks can lead to financial fraud, privacy violations, misinformation, reputation damage, and unauthorized access to confidential information. Traditional identity theft detection techniques mainly rely on password authentication, rule-based security mechanisms, or manual account verification, which are often insufficient to detect sophisticated attacks and evolving behavioral patterns of cybercriminals. This project proposes a Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks, an intelligent security framework that utilizes Artificial Intelligence (AI), Machine Learning (ML), and behavioral analytics to identify compromised or fake user accounts by continuously monitoring multiple behavioral characteristics. The proposed system collects and analyzes various user activities, including login patterns, device information, geographical locations, browsing behavior, posting frequency, messaging habits, friend interactions, profile modifications, and session activities to construct a comprehensive behavioral profile for each user. Instead of depending on a single security feature, the system combines multiple behavioral attributes through composite behavioral modeling to accurately distinguish between legitimate and suspicious activities. Machine learning algorithms such as Random Forest, Support Vector Machine (SVM), XGBoost, Decision Tree, Logistic Regression, and anomaly detection techniques are employed to classify user behavior and identify identity theft attempts with high accuracy. The proposed system aims to improve cybersecurity by providing early detection of suspicious account activities, reducing false alarms, enhancing user privacy, minimizing financial losses, and strengthening trust in online social networking platforms through intelligent behavioral analysis.

Keywords:

Identity Theft Detection, Online Social Networks, Artificial Intelligence, Machine Learning, Behavioral Analytics, Composite Behavioral Modeling, Cyber Security, User Behavior Analysis, Anomaly Detection, Random Forest, Support Vector Machine, XGBoost, Deep Learning, Authentication, Intelligent Security Systems.

I. INTRODUCTION

The rapid advancement of internet technologies and the widespread adoption of online social networking platforms have revolutionized communication, collaboration, and information sharing among individuals across the globe. Millions of users actively participate in social networking platforms such as Facebook, Instagram, X (Twitter), LinkedIn, Snapchat, and many other online communities to communicate with friends, share personal experiences, conduct business activities, and build professional relationships. These platforms store enormous amounts of sensitive user information, including personal details, photographs, conversations, location data, financial information, and social connections. As the popularity of social networks continues to increase, they have become attractive targets for cybercriminals who exploit security vulnerabilities for unauthorized access and malicious activities.

Among various cyber threats affecting online social networks, **identity theft** has become one of the most serious and rapidly growing security challenges. Identity theft occurs when an attacker steals or impersonates the identity of a legitimate user by gaining unauthorized access to their account or creating fake profiles using stolen personal information. Once an attacker successfully compromises an account, they can misuse it to spread false information, perform financial fraud, deceive other users, distribute malicious links, conduct phishing attacks, steal confidential information, or damage the reputation of the legitimate account owner. Such incidents not only affect individual users but also reduce trust in online social networking platforms and create significant cybersecurity concerns.

Traditional identity verification systems primarily rely on passwords, security questions, one-time passwords (OTP), or rule-based authentication mechanisms to protect user accounts. Although these techniques provide an initial level of security, they often fail when attackers obtain user credentials through phishing attacks, malware, social engineering, credential leaks, or password reuse. In many situations, attackers successfully bypass authentication mechanisms because they possess valid login credentials. As a result, conventional security systems are unable to distinguish between genuine users and attackers after successful authentication. This limitation creates the need for intelligent security systems capable of continuously monitoring user activities even after login.

Recent advancements in Artificial Intelligence (AI), Machine Learning (ML), and behavioral analytics have introduced new opportunities for improving identity theft detection. Instead of relying only on authentication credentials, behavioral analysis focuses on understanding how users normally interact with online social networking platforms. Every individual follows unique behavioral patterns, including login timings, frequently used devices, geographical locations, browsing habits, typing speed, messaging behavior, posting frequency, friend interactions, profile update frequency, and overall usage patterns. By analyzing these behavioral characteristics, AI systems can build personalized behavioral profiles for individual users and detect abnormal activities whenever significant deviations occur.

The proposed **Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks** introduces an intelligent framework that combines multiple behavioral characteristics instead of depending on a single feature for identity verification. Composite behavioral modeling integrates login behavior, device information, network characteristics, social interactions, messaging patterns, content posting behavior, session duration, profile modifications, and historical user activities into a unified behavioral profile. Machine

learning algorithms analyze these behavioral features to learn normal user behavior and accurately identify suspicious activities that may indicate identity theft. The system continuously monitors user behavior and automatically generates alerts whenever unusual activities are detected.

II. LITERATURE SURVEY

1. Title: Detecting Identity Theft in Online Social Networks Using Behavioral Profiling

Author: A. K. Sharma and R. Verma

Abstract:
This research proposes a behavioral profiling approach for detecting identity theft in online social networks. The system continuously monitors user activities such as login behavior, browsing history, messaging frequency, and interaction patterns to establish a normal behavioral profile for each user. Machine learning algorithms are applied to compare current user activities with historical behavioral patterns and identify suspicious deviations that may indicate compromised accounts. Experimental results demonstrate that behavioral profiling significantly improves the accuracy of identity theft detection while reducing false alarms compared to traditional authentication methods.

2. Title: Machine Learning-Based Identity Theft Detection in Social Networking Platforms

Author: M. Ahmed, S. Khan, and P. Kumar

Abstract:
This paper presents a machine learning framework for detecting identity theft attacks on online social networking platforms. Various supervised learning algorithms, including Decision Tree, Random Forest, and Support Vector Machine, are evaluated using user behavioral datasets. Features such as login time, device information, geographical location, and posting activities are extracted for classification. The study concludes that ensemble learning models achieve higher detection accuracy and better adaptability against evolving cyber threats.

3. Title: Behavioral Biometrics for Continuous User Authentication

Author: J. Smith and L. Anderson

Abstract:
The authors investigate behavioral biometrics as a continuous authentication mechanism. Unlike traditional password-based authentication, behavioral biometrics monitor typing speed, mouse movements, touchscreen interactions, navigation behavior, and usage patterns throughout the user's session. Experimental analysis shows that continuous behavioral monitoring provides stronger protection against unauthorized access even after successful login. The research highlights the importance of dynamic user profiling for improving cybersecurity.

4. Title: Deep Learning Approaches for Anomaly Detection in Social Networks

Author: X. Li, Y. Wang, and H. Zhao

Abstract:
This study explores deep learning techniques for identifying abnormal user behavior in online social networks. Autoencoders and Long Short-Term Memory (LSTM) networks are utilized to model normal user behavior and detect deviations caused by malicious activities. The proposed framework successfully identifies previously unseen attack patterns and demonstrates high detection accuracy in large-scale datasets. The research suggests that deep learning models can effectively enhance identity theft detection systems.

5. Title: User Behavior Analytics for Cybersecurity Applications

Author: S. Gupta and V. Patel

Abstract:
This paper discusses the role of User Behavior Analytics (UBA) in modern cybersecurity systems. The proposed framework collects user activities from multiple sources and applies machine learning algorithms to build behavioral profiles for anomaly detection. The system effectively identifies insider threats, compromised accounts, and unauthorized access attempts by analyzing deviations from normal user behavior. The research demonstrates the advantages of combining multiple behavioral attributes for improving detection performance.

III. EXISTING SYSTEM

The existing identity theft detection systems used in online social networks primarily rely on traditional authentication mechanisms such as usernames,

passwords, one-time passwords (OTP), security questions, CAPTCHA verification, and multi-factor authentication. These methods verify users only during the login process and provide limited protection after authentication is completed. Once attackers successfully obtain valid login credentials through phishing attacks, malware, credential leaks, or social engineering techniques, they can easily access user accounts without being detected by conventional security systems. Some existing systems use rule-based monitoring techniques that identify suspicious activities based on predefined thresholds such as repeated login failures or unusual login locations. However, these static approaches are unable to adapt to changing user behavior and often generate high false-positive rates. They also fail to detect sophisticated identity theft attacks where attackers imitate normal user activities. Since traditional methods analyze only a limited number of security parameters, they cannot effectively capture the complex behavioral characteristics of individual users. Consequently, there is a need for an intelligent and adaptive behavioral analysis framework capable of continuously monitoring multiple user activities and accurately detecting identity theft in real time.

IV. PROPOSED SYSTEM

The proposed **Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks** introduces an intelligent cybersecurity framework that continuously monitors user behavior to detect compromised accounts and identity theft attempts. Unlike traditional authentication systems that rely only on passwords or login verification, the proposed system analyzes multiple behavioral characteristics including login time, login location, device information, browsing activities, typing behavior, messaging frequency, posting habits, friend interactions, profile modifications, and session duration. These behavioral features are collected from user activities and combined to create a comprehensive behavioral profile through composite behavioral modeling. The collected data undergoes preprocessing to remove inconsistencies, normalize values, and extract meaningful behavioral attributes. Machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Decision Tree, Logistic Regression, and XGBoost are trained using historical user behavior to distinguish legitimate activities from suspicious ones. The system continuously compares current user behavior with previously learned behavioral profiles to identify anomalies that may indicate identity theft. Whenever significant behavioral deviations are detected, the system automatically generates alerts, requests additional authentication, or temporarily restricts suspicious account activities. By integrating multiple behavioral characteristics into a unified decision-making framework, the proposed system improves detection accuracy, minimizes false alarms, enhances user privacy, and provides stronger protection against evolving cyber threats in online social networking environments.

V. SYSTEM ARCHITECTURE

The proposed **Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks** consists of several interconnected modules that work together to continuously monitor user behavior and detect identity theft attempts. The architecture begins with the **User Activity Collection Module**, where behavioral information is collected from online social networking platforms. The collected information includes login history, login location, IP address, device type, browser information, browsing patterns, posting frequency, messaging activities, friend interactions, profile updates, session duration, and user navigation behavior. This raw behavioral data is transferred to the **Data Preprocessing Module**, where missing values are handled, duplicate records are removed, irrelevant attributes are eliminated, and the collected data is normalized into a structured format suitable for machine learning analysis. After preprocessing, the data enters the **Behavioral Feature Extraction Module**, which identifies meaningful behavioral attributes representing individual user activities. Multiple behavioral characteristics are combined through the **Composite Behavioral Modeling Module**, which constructs a comprehensive behavioral profile for each registered user. Instead of analyzing a single feature, this module integrates various behavioral indicators to improve detection reliability. The generated behavioral profiles are then provided to the **Machine Learning Classification Module**, where algorithms such as Random Forest,

Support Vector Machine (SVM), Logistic Regression, Decision Tree, and XGBoost analyze user behavior patterns and classify activities as either legitimate or suspicious. The system also incorporates an **Anomaly Detection Module** that identifies unusual behavioral deviations which may indicate previously unseen identity theft attacks. Finally, the **Decision Support Module** evaluates classification results and generates appropriate security actions such as warning notifications, additional authentication requests, temporary account restrictions, or administrator alerts whenever suspicious activities are detected. The complete architecture provides continuous behavioral monitoring, intelligent anomaly detection, automated decision-making, and enhanced security for protecting online social network users against identity theft attacks.

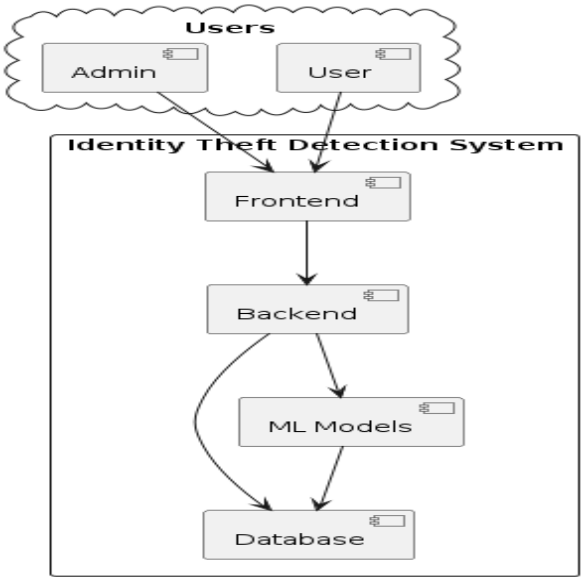


Fig 5.1: System Architecture

VI. IMPLEMENTATION



Fig 6.1 Index page

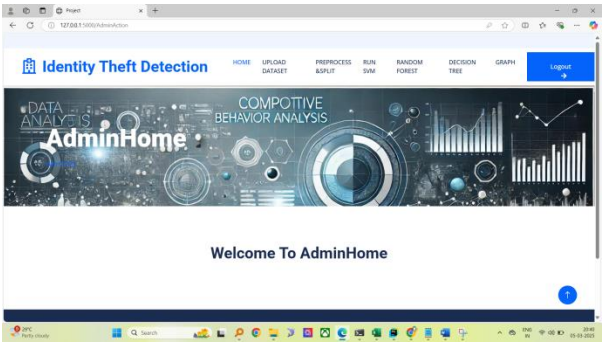


Fig 6.2: Admin home

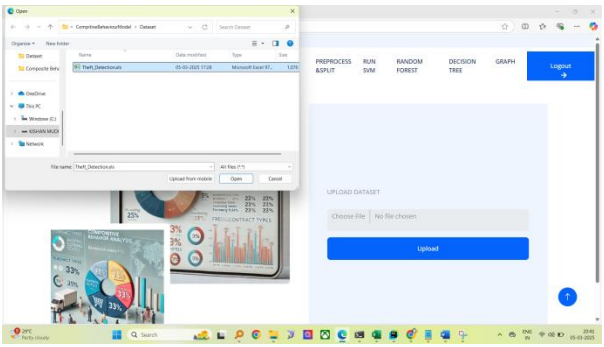


Fig 6.3: Upload dataset

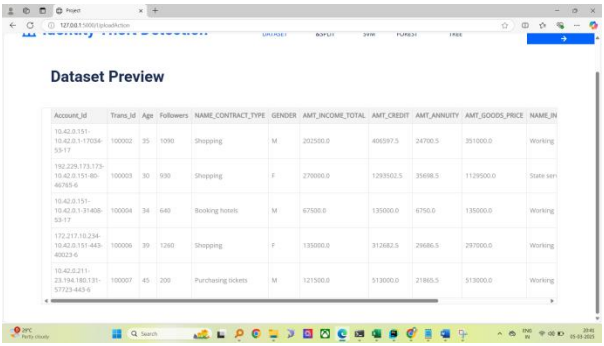


Fig 6.4: Model training

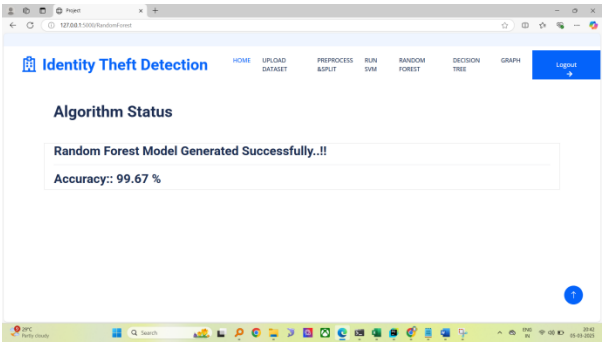


Fig 6.5: Performance

VII. CONCLUSION

The proposed **Composite Behavioral Modeling for Identity Theft Detection in Online Social Networks** provides an intelligent and adaptive solution for detecting identity theft by continuously analyzing multiple user behavioral characteristics. Unlike traditional authentication mechanisms that verify users only during login, the proposed framework performs continuous behavioral monitoring throughout user sessions. By combining login patterns, browsing behavior, device information, messaging activities, posting habits, social interactions, and profile modifications, the system creates comprehensive behavioral profiles that accurately distinguish genuine users from attackers. Machine learning algorithms improve the accuracy of identity theft detection while minimizing false-positive alerts and adapting to changing user behavior over time. The proposed approach enhances account security, protects user privacy, reduces financial losses, and increases user trust in online social networking platforms. Overall, the system demonstrates the effectiveness of integrating behavioral analytics and artificial intelligence to provide proactive cybersecurity against identity theft attacks.

VIII. FUTURE SCOPE

The future scope of the proposed system includes integrating advanced deep learning models such as Long Short-Term Memory (LSTM), Graph Neural Networks (GNN), Transformer-based architectures, and Large Language Models (LLMs) for more accurate behavioral analysis and anomaly detection. The system can be enhanced by incorporating real-time streaming analytics to detect suspicious activities immediately after they occur. Future research may also include multimodal behavioral analysis by combining user behavior with biometric features such as keystroke dynamics, mouse movements, touchscreen interactions, facial recognition, and voice authentication to strengthen identity verification. Blockchain technology can be integrated to improve the security and integrity of user identity information and reduce the risk of identity tampering. Federated learning techniques can also be adopted to enable collaborative model training while preserving user privacy. Furthermore, the proposed framework can be extended to secure online banking systems, e-commerce platforms, healthcare applications, educational portals, cloud computing environments, and enterprise information systems where identity theft remains a significant cybersecurity challenge. These enhancements will contribute toward developing a more intelligent, adaptive, scalable, and secure identity theft detection system capable of defending against sophisticated cyberattacks.

IX. REFERENCES

[1] J. R. Douceur, "The Sybil Attack," *Proceedings of the First International Workshop on Peer-to-Peer Systems*, pp. 251–260, 2002.

[2] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[3] C. Cortes and V. Vapnik, "Support-Vector Networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[4] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

[5] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[6] D. E. Denning, *Information Warfare and Security*. Addison-Wesley, 1999.

[7] M. Bishop, *Computer Security: Art and Science*. Addison-Wesley, 2003.

[8] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[9] T. Fawcett and F. Provost, "Adaptive Fraud Detection," *Data Mining and Knowledge Discovery*, vol. 1, no. 3, pp. 291–316, 1997.

[10] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys*, vol. 41, no. 3, pp. 1–58, 2009.

[11] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed. Morgan Kaufmann, 2012.

[12] W. Stallings, *Network Security Essentials*, 6th ed. Pearson, 2017.

[13] R. Anderson, *Security Engineering*, 3rd ed. Wiley, 2020.

[14] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems," NIST Special Publication 800-94, 2007.

[15] S. Axelsson, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 186–205, 2000.