Journal of Science, Computing and Engineering Research (JSCER)
Volume-8, Issue-2, February 2025.
DOI: *https://doi.org/10.46379/jscer.2025.080213*

Transparent Identity Verification and Trust-Aware Hybrid Algorithms to Secure Social Networks and Recommender Systems Against Sybil and Shilling Attacks

[1]R.Poornima @ Priyanka, [2]P.Malathy ,[3]P.Divya Bharathi

[1,3]Assistant Professor, Department of Information Technology, SRM Madurai College for Engineering and Technology, Sivgangai.

[2]Assistant Professor, Department of Electrical and Electronics Engineering, PSNA College of Engineering and Technology, Dindigul.

Article Information

Received : 10 Feb 2025
Revised : 16 Feb 2025
Accepted : 20 Feb 2025
Published : 23 Feb 2025

Corresponding Author:
R.Poornima

Abstract— Secure social networks are web-based platforms that allow individual users to create a public profile, add as many persons as they like to speak with, and view relationships inside the system. Many social networks are Internet-based and allow users to communicate online through features including rapid messaging, email, sharing images and videos, uploading user thoughts, and more. Attackers can readily compromise such social networks (e.g., Sybil attack). The Sybil attack is a type of security risk that arises when a compromised system is used to assume several identities. Peer-to-peer networks on a massive scale encounter security flaw in their calculation foundations. Utilizing the Robust Recommendation method, when the attacker is aware of the profiles of authenticated users, the Sybil attack, which impacts the program, fails. By combining face detection and identification algorithms with session management, the suggested methodology must be able to remove such limitations. Conversely, because collaborative filtering systems operate in an unfastened en vironment, they are extremely vulnerable to malicious raters who create profiles with incomplete ratings. Many attack-identifying algorithms have been developed in recent years to address the issue. The application is successfully secured by employing these techniques to eradicate such malicious profiles, which is the goal of Eliminating Shilling Attack.

Keywords: ***Secure Social Networks, Sybil Attack, Shilling Attack, Robust Recommendation System, Peer-to-Peer Networks, Face Detection, Identification Algorithms, Session Management, Collaborative Filtering, Cybersecurity.***

Citation: R.Poornima @ Priyanka, P.Malathy ,P.Divya Bharathi , "Transparent Identity Verification and Trust-Aware Hybrid Algorithms to Secure Social Networks and Recommender Systems Against Sybil and Shilling Attacks", Journal of Science, Computing and Engineering Research, 8(2), February 2025.

I. INTRODUCTION

Recommender systems are intelligent tools that analyze user preferences and behavior to offer tailored suggestions, widely applied in online shopping, streaming platforms, and social networks. They use collaborative filtering to suggest items favored by users with similar tastes and content-based filtering to recommend items sharing similar features. Hybrid methods integrate these strategies for greater accuracy, while knowledge-based systems apply domain-specific guidelines. Advanced techniques like deep learning improv e recommendations by uncovering complex user trends. User profile privacy and anonymity are critical components in secure social networks, with varying levels of anonymity ranging from conditional to full anonymity. Conditional anonymity allows for partial disclosure of information un - der specific circumstances, while full anonymity ensures no personal details are revealed. To achieve this, homo-morphic encryption is employed, enabling computations on encrypted data without the need for decryption. This approach safeguards user profiles from unauthorized access while maintaining functionality.

Challenges such as the cold-start problem, scalability, data reliability, privacy issues, and fairness remain. Despite these hurdles, recommender systems play a vital role in improving user engagement, loyalty, and overall business performance in the digital space However, challenges arise in network models where privacy must be balanced with features like profile matching and friend recommendations. Homomorphic encryption addresses these challenges by ensuring data remains secure during processing, thereby preventing potential breaches.

Profile matching is a fundamental mechanism in social networks, facilitating automated friend suggestions by com- paring user profiles. This process involves identifying similarities between a user's profile and those of others, enabling personalized recommendations. Two primary approaches to profile matching are implicit and explicit comparison - based methods. Implicit comparison relies on indirect indicators such as user behaviour or preferences, while explicit comparison utilizes direct information provided by users, such as interests or demographic details. By integrating these methods, social networks can enhance user engagement while maintaining privacy.

Secure authentication and privacy preservation are further strengthened through advanced technologies like face recognition. These technologies not only improve security but also ensure that user data remains protected. Combining encryption with secure profile matching allows social networks to offer personalized features, such as friend recommendations, without compromising user privacy. Additionally, recommender systems play a vital role in enhancing user experience. Collaborative filtering builds user profiles based on past behaviour and compares them with similar users to predict items of interest. Content-based filtering, on the other hand, recommends items by analysing their attributes and matching them to user preferences. Hybrid recom mender systems, which combine collaborative and content-based filtering, provide a more robust and effective approach by leveraging the strengths of both methods. Together, these technologies and methodologies contribute to the devel- opment of secure, privacy-conscious social networks that prioritize user experience and data protection.

Principal Component Analysis (PCA) is a widely adopted technique in recommender systems, often used to enhance the performance of document-based processes. However, PCA is prone to challenges such as missing ratings, which can disrupt the user–item matrix and degrade the quality of recommendations. Classification-based approaches, while effective, require extensive knowledge of attack patterns and user profiles to train classifiers accurately. These methods are designed to detect and mitigate malicious activities, such as shilling attacks, but their reliance on detailed training data can be a limitation. Statistical Process Control (SPC) addresses some of these issues by assuming that the rating probability distribution for each item is known in advance, enabling the detection of anomalies in user behavior. Despite these advancements, existing methods still face significant challenges in combating sophisticated attacks.

To address these limitations, we propose a modified version of the Computation for Eliminating Shilling At-tacks (CESA) which we refer to as Enhanced Shilling Attack Detection and Elimination (ESADE). ESADE builds upon the foundational principles of CESA but introduces several improvements to enhance its effectiveness. Unlike traditional methods, ESADE integrates advanced machine learning techniques with statistical analysis to identify and eliminate shilling profiles more accurately. It employs a multi-layered approach to detect anomalies in user behavior, combining implicit and explicit profile matching to ensure robust detection of malicious activities. Addition- ally, ESA DE incorporates real-time monitoring and adaptive learning capabilities, allowing it to evolve in response to emerging attack patterns. By addressing the shortcomings of PCA , classification-based methods, and SPC, ESADE offers a comprehensive solution to improve the security and reliability of recommender systems. This algorithm not only enhances the detection of shilling attacks but also ensures the integrity of user profiles and the accuracy of recommendations, making it a valuable tool for secure and efficient recommender systems.

II. STRUCTURE DESIGN FOR S YBIL ATTACK

The process begins with Webcam Implementation, where a live camera captures the user's face. This occurs during two critical stages: account creation and login. During account creation, the user's facial image is captured and stored in the database. Similarly, when an existing user logs in, their face is captured again for verification. This step ensures that the system has a reference image for comparison during subsequent access attempts.

The next module, Face Detection and Recognition, plays a crucial role in identifying authorized users. When a new or existing user attempt to access the application, their facial image is captured and compared with the stored image in the database. This comparison determines whether the user is trusted and authorized. By verifying the user's identity through facial recognition, the system effectively mitigates the risk of Sybil attacks, where malicious actors might attempt to create multiple fake accounts or impersonate legitimate users.

Figure 3 illustrates the architecture designed to over-come Sybil attacks, comprising four key modules: Webcam Implementation, Face Detection and Recognition, Session Management, and Profile Matching. These modules work in tandem to secure the application from Sybil attacks by ensuring that only authorized users can access the system. Once the user is recognized as authorized, the Session Management module grants access to the application, such as online social networks. This module ensures that the user's session is securely managed, preventing unauthorized access during the session. Finally, the Profile Matching module enhances security by comparing user profiles and

ensuring consistency between the captured facial data and the stored profile information. This step further strengthens the system's ability to detect and prevent Sybil attacks. Together, these four modules create a robust security framework that leverages facial recognition and profile matching to protect the application from Sybil attacks. By ensuring that only verified and authorized users can access the system, this architecture enhances the overall security and reliability of online social networks.

A. FACE ESTIMATION AND FACE DETECTION

The process begins with face estimation and face detec tion, where the system captures and analyzes facial features of users. This step is crucial for identifying and verifying users during account creation and login.

B. HIERARCHICAL DATABASE

The detected facial data is stored in a hierarchical database , which organizes user profiles and related information in a structured manner. This database serves as the foundation for user identification and authentication

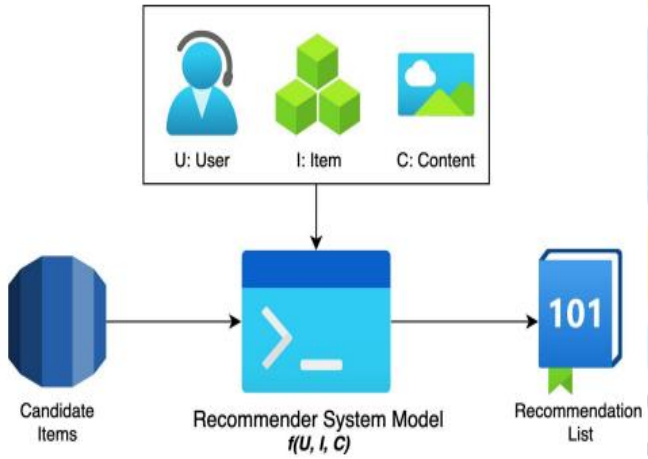

FIGURE 1. Recommender System Architecture

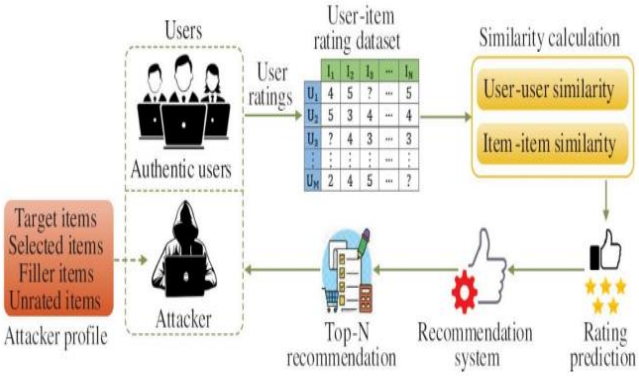

FIGURE 2. Enhanced Shilling attack and detection recommendation system

C. FUSED FACE RECOGNITION UNIT

The Fused Face Recognition Unit processes the facial data and matches it against stored profiles. This unit plays a critical role in identifying users and determining whether they are authorized to access the system.

D. CONTINUOUS AUTHENTICATION

To enhance security, the system employs continuous authentication, which monitors user activity throughout their session. This process is governed by protocols and time

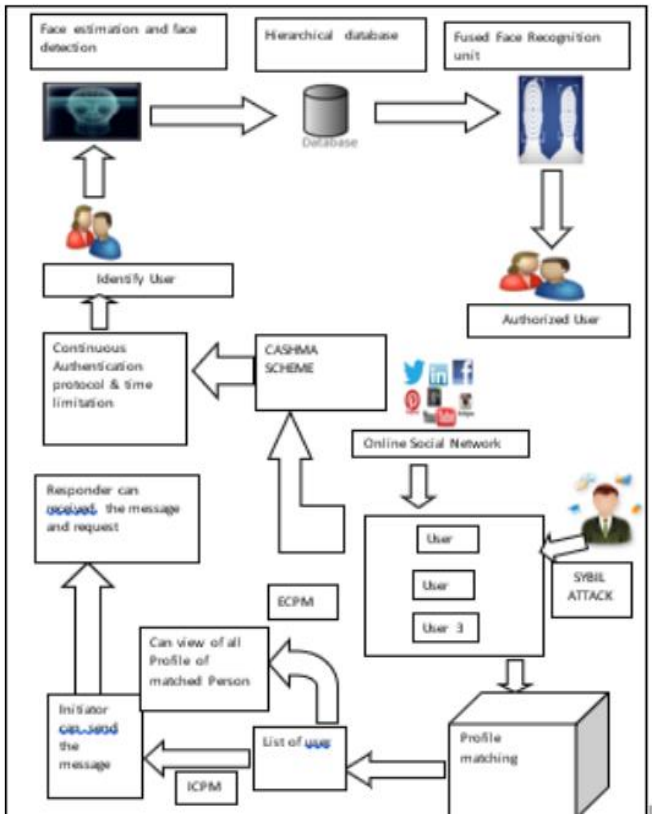

FIGURE 3. Overcoming from Sybil attack

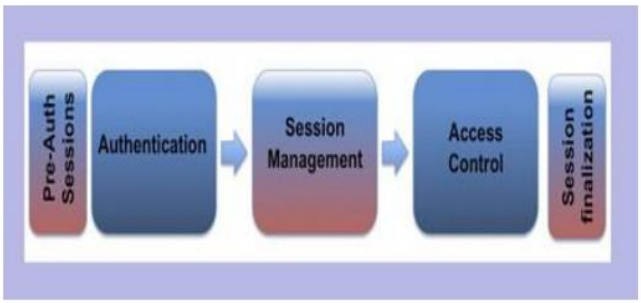

FIGURE 4. Architecture of Session Management

limitations to ensure that only legitimate users remain authenticated.

E.ONLINE SOCIAL NETWORK (CASHMASCREME)

The architecture is integrated into the CASHMASCREME plat- form, an online social network that facilitates user interactions. The platform supports secure messaging and profile matching, enabling users to connect with others while maintaining privacy and security.

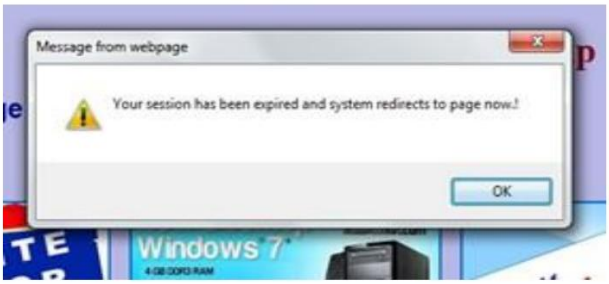

FIGURE 5. Session Expiration

FIGURE 6. Face Detection and Recognition

Figure 5: Face detection and recognition

The system defines three primary user roles:

User1 (Initiator): Can send messages and view profiles of matched persons.

User2 (SYBIL): Represents a potential Sybil at- tack, where a malicious user attempts to create fake profiles or impersonate others.

User3 (Responder): Can receive messages and requests, as well as view profiles of matched persons.

G. PROFILE MATCHING

Profile matching is a key feature of the system, allowin g users to connect based on shared interests or other criteria. This process involves comparing user profiles and suggest- ing potential matches.

H. COMMUNICATION PROTOCOLS

The systemutilizes two communication protocols to manage interactions:

-- ECPM (External Communication Protocol Module): Handles external communications and interactions between users.

-- ICPM (Internal Communication Protocol Mod- ule): Manages internal data flow and profile matching within the system. The architecture incorporates robust security measures to protect against threats such as Sybil attacks. By combining face recognition, continuous authentication, and secure communication protocols, the system ensures that only authorized users can access the platform and interact with others.

III. SYSTEM DESIGN FOR SHILLING ATTACK DETECTION

The proposed method, now referred to as Advanced Shilling Attack Detection and Elimination (ASADE) is designed to address the challenges of detecting and eliminating shilling attacks in recommender systems. ASADE is based on a continuous probability density function defined on the interval (0,1) and utilizes sigmoid curve calculations governed by two constraints, α and β. This innovative approach is both novel and straightforward, enabling the identification and removal of malicious profiles with high accuracy.

Unlike traditional methods , ASADE is robust against issues such as unfounded values and does not rely on potentially harmful training data. This independence fro m skewed datasets makes it more reliable compared to existing techniques like Principal Component Analysis (PCA), Statistical Process Control (SPC), and classification-based algorithms, which struggle to detect multiple target attacks effectively. ASADE, on the other hand, is specifically

designed to identify and eliminate multiple simultaneous attacks, making it a powerful tool for securing recommend er systems.

The problem is formally defined using two key metrics:

1. Protection Time: This is calculated as the ratio of correctly detected attack profiles to the total number of malicious profiles.
2. Fake Rate: This is defined as the ratio of genuine profiles incorrectly identified as attacks to the total number of genuine profiles.

ASADE aims to maximize protection time while minimizing the fake rate ensuring that genuine users are not falsely flagged while malicious profiles are accurately detected and removed. By leveraging advanced probabilistic modelling and sigmoid-based constraints, ASADE provides a robust and efficient solution for mitigating shilling attacks in recommender systems.

Here's a recreated version of the algorithm with modification for clarity and improved structure. The new algorithm is named ASADE (Advanced Shilling Attack Detection and Elimination)

Algorithm: ASADE Input:

- \(U \): A set of users
- \(I \): A set of items
- \(R_{U \times I} \): A user-item rating matrix

Output:

- \(K_A \): A set of authentic users

S teps

1. Initialize:

- Create a matrix \(R_{U \times I} \) to represent user-item ratings.
- Define a set of potential attack patterns \(PA = \{PA_1, PA_2, PA_3\} \), where each \(PA_i \) represents a unique attack profile.

A. TRANSFORM POINTS:

- For each user \(u \in U \), transform their rating data into a feature space using matrix operations.
- Example:

‘‘‘

Point[] PointArray = { new Point(15, 25), new Point(30, 35) };

Point[] transformed Points = Matrix.Transform Points (PointArray);

‘‘‘

- This step helps in identifying patterns in the user-item matrix that may indicate malicious behavior.

B. DETECT MALICIOUS USERS:

- For each user \(u \in U \):
- Check if the user’s rating pattern \(c \) matches any combination of attack patterns:

\[
c \in (PA_1 \cap PA_2) \cup (PA_2 \cap PA_3) \cup (PA_1 \cap PA_3)
\]

- If a match is found, classify the user as malicious and add them to the set \(K_C \).

4. Return Authentic Users:

- Compute the set of authentic users \(K_A \) by excluding malicious users from the original set:

\[
K_A = U \setminus K_C
\]

- Return \(K_A \) as the final output.

1) Explanation

The algorithm begins by initializing the user-item rating matrix and defining potential attack patterns.

- It then transforms user rating data into a feature space to identify patterns indicative of shilling attacks.

- Users whose rating patterns match known attack profiles are flagged as malicious and excluded from the set of authentic users.
- The final output is a set of users \(K_A \) who are verified as authentic.

To evaluate the performance of the proposed algorithm, EDSA, the Movie Lens dataset from the Group Lens Re - search Lab was utilized. This dataset comprises 200,000 ratings for 2,582 movies provided by 1,023 users, with each user rating at least 10 movies. The ratings are represented as integer values ranging from a minimum of 1 (indicating strong dislike) to a maximum of 5 (indicating strong enjoyment) [1]. This dataset serves as a robust foundation for testing and validating the effectiveness of the algorithm in detecting and mitigating shilling attacks.

IV. INHIBITION TECHNIQUES

An offline experiment was carried out using a pre-existing dataset that captured user interactions, including item selections and ratings. This dataset allows the system to replicate user behavior in the context of a recommendation system. The design of the system emphasizes the identification and elimination of shilling profiles within online recommender systems. By analyzing user behavior, the system effectively counters attacks targeting collaborative filtering based recommender systems. This methodology functions as a structured analysis and design framework, capable of generating flowcharts that combine both information-driven and process-driven system flow controls.

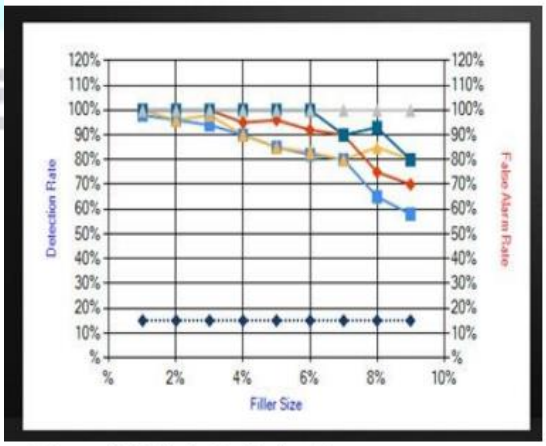

Figure 9 Multiple Push Attack

The identification and removal of malicious profiles con - tribute to increased revenue for e-commerce platforms by protecting them from a wide range of attacks, irrespective of their size or complexity. Shilling attacks, in particular, pose a significant threat, but the proposed approach successfully neutralizes them. This ensures that

users receive accurate and trustworthy recommendations, thereby enhancing the overall reliability of the system and fostering greater user confidence.

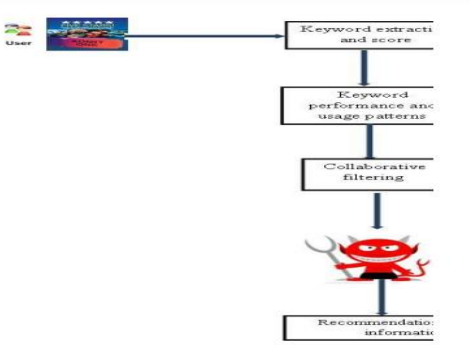

FIGURE 11 Recommendation ratings to user

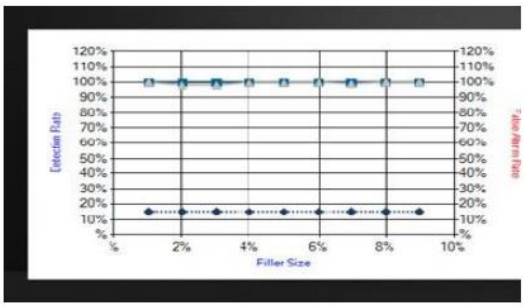

FIGURE 10 Multiple Nuke Attack

V. CONCLUS ION AND FUTURE WORK

The innovative potential of using biometrics to create a protocol for transparent authentication greatly enhances both the security and usability of user sessions [6][8][10]. This protocol dynamically determines adaptive timeouts by assessing the trust level derived from user activity, along with the quality and type of biometric data gathered seamlessly through background monitoring of user interactions. Key architectural decisions of the system are highlighted here. Notably, the system prioritizes the exchange of raw biometric data over processed features or templates, and it avoids the use of cryptographic token-based methods. This approach aligns with the goal of maintaining a simple and lightweight client architecture.

The proposed protocol is highly flexible and can operate efficiently with raw data, extracted features, or templates without necessitating any adjustments. In future developments, session management will integrate multiple biometric outcomes to significantly bolster security. Additionally, we have explored a unique challenge of comparison-based profile matching in Mobile Social Networks (MSNs) and introduced novel protocols to address it. The explicit Comparison-based Profile Matching (eCPM) protocol ensures conditional anonymity by revealing only the comparison result to the initiator. Considering k-anonymity as a user requirement, we evaluate the anonymity risk level associated with pseudonym changes across consecutive eCPM operations. Future efforts will also aim to improve the precision of face detection and recognition techniques to further refine the system's effectiveness.

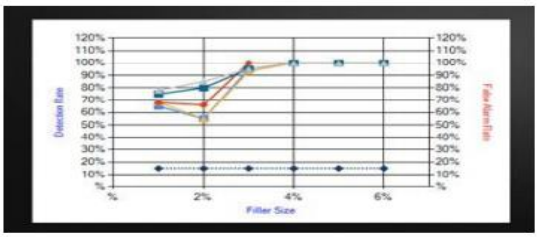

FIGURE 7 Single Push Attack

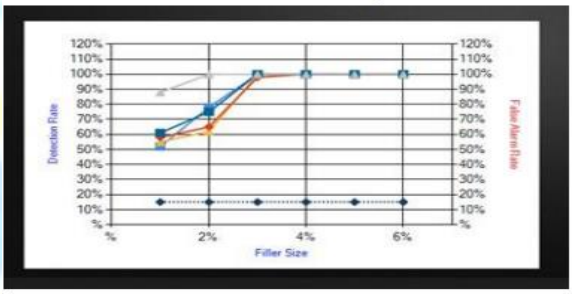

FIGURE 8 Single Nuke Attack

REFERENCES

[1]. Himeur, Y., Sohail, S. S., Bensaali, F., Amira, A., & Alazab, M. (2022). Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives. Computers & Security, 118, 102746.

[2]. Boots, B. C. (2022). Networks and trust: systems for understanding and supporting internet security. Colorado State University.

[3]. Cárdenas-Haro, J. A., Salem, M., Aldaco-Gastélum, A. N., López-Avitia, R., & Dawson, M. (2024). Enhancing Security in Social Networks through Machine Learning : Detecting and Mitigating Sybil Attacks with SybilSocNet. Algorithms, 17(10).

[4]. Ferreira, L., Silva, D. C., & Itzazelaia, M. U. (2023). Recommender systems in cybersecurity. Knowledge and Information Systems, 65(12), 5523-5559.

[5]. Moradi, R., & Hamidi, H. (2023). A New Mechanism for Detecting Shilling Attacks in Recommender Systems Based on Social Network Analysis and Gaussian Rough Neural Network with Emotional Learning. International Journal of Engineering, 36(2), 321-334.

[6] Zayed, R. A., Ibrahim, L. F., Hefny, H. A., Salman, H. A., & AlMohimeed, A. (2023). Using Ensemble Method to Detect Attacks in the Recommender System. IEEE Access, 11, 111315-111323.

[7] Guo, S., Bai, T., & Deng, W. (2023, October). Targeted shilling attacks on gnn-based recommender systems. In Proceedings of the 32nd ACM International Conference on Information and Knowledge Management (pp. 649-658).
[8] Nawara, D., Aly, A., & Kashef, R. (2024). Shillin g Attacks and Fake Reviews Injection: Principles, Models, and Datasets. IEEE Transactions on Computational Social Systems.
[9] Kaur, M., & Rani, S. (2023). Recommender System: Towards Identification of Shilling Attacks in Rating System Using Machine Learning Algorithms. International Journal of Performabilit y Engineering, 19(7), 443.
[10] Xu, Y., Zhang, P., Yu, H., & Zhang, F. (2024). Detecting group shilling attacks in recommender systems based on user multi-dimensional features and collusive behaviour analysis. The Computer Journal, 67(2), 604-616.

[11] Shende, M. K., & Verma, V. (2023). Analysing supervised learning approaches for detecting shilling attacks in collaborative recommendations. In ITM Web of Conferences (Vol. 54, p. 01009). EDP Sciences.
[12] Zhang, F., Qu, Y., Xu, Y., & Wang, S. (2020). Graph embedding-based approach for detecting group shilling attacks in collaborative recommender systems. Knowledge-Based Systems, 199, 105984.
[13] Tong, C., Yin, X., Li, J., Zhu, T., Lv, R., Sun, L., & Rodrigues, J. J. (2018). A shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network. The Computer Journal, 61(7), 949-958.
[14] Goutham, N., Singh, K., & Verma, C. (2024). ShAD-SEF: A Stacking Ensemble Framework for Efficient Shillin g Attack Detection. Elsevier Expert Systems with Applications, 238, 122345.
[15] Wang, S., Fan, W., & Li, Q. (2024). Multi-Agent Attacks on Black-Box Social Recommender Systems: A Comprehensive Study. ACM Transactions on Information Systems, 43(2), 1-30.
[16] Nguyen, T. T., Huynh, T. T., & Yin, H. (2024). Poisoning Attacks on Recommender Systems: A Survey of Techniques and Countermeasures. Springer Computing Surveys, 57(2), 1-40.
[17] Vivekanandan, K., & Praveena, N. (2024). Hybrid CNN-LSTM Models for Shilling Attack Detection in Social-Aware Networks. Elsevier Journal of Ambient Intelligence and Humanized Computing, 15(3), 1234-1248.
[18] Zhang, F., Chan, P. P., He, Z. M., & Yeung, D. S. (2024). Unsupervised contaminated user profile identification against shilling attack in recommender system. Intelligent Data Analysis, 28(6), 1411-1426.
[19] Singh, P. K., Pramanik, P. K. D., Sinhababu, N., & Choudhury, P. (2024). Detecting Unknown Shillin g Attacks in Recommendation Systems. Wireless Personal Communications, 137(1), 259-286.
[20] Nawara, D., Aly, A., & Kashef, R. (2024). Shilling attacks and fake reviews injection: Principles, models, and datasets. IEEE Transactions on Computational Social Systems.
[21] Liu, S., Yu, S., Li, H., Yang, Z., Duan, M., & Liao, X. (2024). A novel shilling attack on black-bo x recommendation systems for multiple targets. Neural Computing and Applications , 1-19.
[22] Lu, Q., & Gao, M. (2024, May). A Research on Shillin g Attacks Based on Variational graph auto-encoders for Improving the Robustness of Recommendation Systems. In Proceedings of the 2024 International Conference on Generative Artificial Intelligence and Informatio n Security (pp. 120-126).
[23] Anelli, V. W., Deldjoo, Y., Di Noia, T., Di Sciascio, E., & Merra, F. A. (2020, May). Sasha: Semantic-aware shilling attacks on recommender systems exploitin g knowledge graphs. In European Semantic Web Conference (pp. 307-323). Cham: Springer International Publishing.
[24] Tong, C., Yin, X., Li, J., Zhu, T., Lv, R., Sun, L., & Rodrigues, J. J. (2018). A shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network. The Computer Journal, 61(7), 949-958.
[25] Rezaimehr, F., & Dadkhah, C. (2021). A survey of attack detection approaches in collaborative filterin g recommender systems. Artificial Intelligence Review, 54, 2011-2066.
[26] Li, J., & Wang, Z. (2024). Sybil Attack Detection for Secure IoT-Based Smart Healthcare Environments. Journal of The Institution of Engineers (India): Series B, 1-13.
[27] Bhanja, U., Majhi, A., Sahu, S., & Parida, D. (2024). Detection of Sybil & DDoS attacks in VANET using intelligent technique. International Journal of Computers and Applications, 46(10), 811-829.
[28] Devi, E. R., Shanthakumari, R., Harini, T., Lokesh, K., & Anusuyaa, V. S. (2024, May). Detection of Position Falsification Attacks in VANETs Using Ensemble Learning. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.
[29] Sultana, R., Grover, J., & Tripathi, M. (2024). Cooperative approach for data-centric and node-centric misbehavior detection in VANET. Vehicular Communications, 50, 100855.
[30] Morton, T. L., Borah, A., & Paranjothi, A. (2024). Trust-Aware Sybil Attack Detection for Resilient Vehicular Communication. Internet Technology Letters , e617.
[31] Sherubha, P., Iqbal, M., Chris, A., & Subramani, N. (2024). Adversarial Network Model Based on Feature Fusion Learner for Intrusion Detection in Sensor Networks. Fusion: Practice & Applications, 15(1).
[32] Kong, X., He, X., Ma, X., Yan, X., Wang, L., Shen, G., & Liu, Z. (2025). Oh-FedRec: One-Shot and Heterogeneous Vertical Federated Recommendation System. IEEE Transactions on Consumer Electronics.
[33] Rani, P., & Tewari, T. (2023, February). An application-oriented review of blockchain-based recommender systems. In International Conference On Innovative Computing And Communication (pp. 837-846). Singapore: Springer Nature Singapore.

[34] Sun, H. L., & Chen, D. B. (2024). A robust ranking method for online rating systems with spammers by interval division. Expert Systems with Applications, 235, 121236.
[35] Harita, U., & Mohammed, M. (2024). Analyzing threat flow over network using ensemble-based dense network model. Soft Computing, 28(5), 4171-4184.
[36] Patel, J. (2024). Exploration of Low-Level Features for Enhancing Movie Recommendation Systems (Master's thesis, University of Windsor (Canada)).
[37] Kaya, T. T., Yalcin, E., & Kaleli, C. (2023). A novel classification-based shilling attack detection approach for multi-criteria recommender systems. Computational Intelligence, 39(3), 499-528.
[38] Majumder, A., Chowdhury, K., & Sarkar, J. L. (2023). Taxonomy of Shilling Attack Detection Techniques in Recommender System. In Machine Learning Algorithms and Applications in Engineering (pp. 141-160). CRC Press.
[39] Praveena, N., Juneja, K., Rashid, M., Almagrabi, A. O., Sekaran, K., Ramalingam, R., & Usman, M. (2023). Hybrid gated recurrent unit and convolutional neural network-based deep learning mechanism for efficien t shilling attack detection in social networks. Computers and Electrical Engineering, 108, 108673.
[40] Shende, M. K., & Verma, V. (2023, October). Enhancing popSAD: A New Approach to Shilling Attack Detection in Collaborative Recommenders. In International Conference on Frontiers in Computing and Systems (pp. 51-62). Singapore: Springer Nature Singapore.
[41] Zayed, R. A., Ibrahim, L. F., Hefny, H. A., Salman, H. A., & AlMohimeed, A. (2023). Using Ensemble Method to Detect Attacks in the Recommender System. IEEE Access, 11, 111315-111323.
[42] Rezaimehr, F., & Dadkhah, C. (2021). A survey of attack detection approaches in collaborative filterin g recommender systems. Artificial Intelligence Review, 54, 2011-2066.
[43] Zhou, H., Gao, M., Chao, M., Song, Y., Xiong, Q., Wen, J., & Zhang, Y. (2023, November). Data Hybrid Attacks Based on Sensitive Users in Recommender Systems. In 2023 7th Asian Conference on Artificial Intelligence Technology (ACAIT) (pp. 445-452). IEEE.
[44] Ferdinan, T., & Kocoń, J. (2023). Personalized models resistant to malicious attacks for human-centered trusted ai. Emotion, 40000, 50000.
[45] Saxena, A., Saileshwar, G., Juffinger, J., Kogler, A., Gruss, D., & Qureshi, M. (2023, June). Pt-guard: Integrity-protected page tables to defend against breakthrough rowhammer attacks. In 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 95-108). IEEE.
[46] Song, L., & Rho, S. (2023). Hidden target recognition method for high-speed network security threats based on attack graph theory. Journal of High Speed Networks, 29(4), 307-320.
[47] Yang, Z., Xu, L., Cai, Z., & Xu, Z. (2016). Re-scale AdaBoost for attack detection in collaborative filterin g recommender systems. Knowledge-Based Systems, 100, 74-88.
[48] Samal, S., Zhang, Y. D., Gadekallu, T. R., & Balabantaray, B. K. (2023). ASYv3: Attention-enabled pooling embedded Swin transformer-based YOLOv3 for obscenity detection. Expert Systems, 40(8), e13337.
[49] Ahsan, M., Rais, M. H., & Ahmed, I. (2023, July). Sok: Side channel monitoring for additive manufacturing - bridging cybersecurity and quality assurance communities. In 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P) (pp. 1160-1178). IEEE.
[50] Bikki, N. (2024). Deep Learning Techniques for Cyber-Attack Predictions in Organizations (Doctoral dissertation, CALIFORNIA STATE UNIVERS IT Y, NORTHRIDGE).