



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

A Blockchain-Based Application for Authenticating Social Profiles and Preventing Fraud

E.Abinayagi¹, Prabha Sasikumar², R.Vaneesha³

Department of ECE, Selvam College of Technology (Autonomous), Namakkal, TamilNadu, India

ABSTRACT: In this blockchain-based application designed to combat fake social profiles, the integration of the Naive Bayes algorithm adds a sophisticated layer of fraud detection. Leveraging blockchain's decentralized nature, user profiles are stored securely, with each profile represented as a block in the chain. Prior to inclusion in the blockchain, profiles undergo a rigorous verification process, employing various authentication methods like government-issued IDs or trusted social media accounts. Once submitted, the Naive Bayes algorithm steps in, extracting pertinent profile features such as images, usernames, and activity histories. Trained on labeled data encompassing both genuine and fake profiles, the algorithm assigns probability scores to new profiles, indicating the likelihood of authenticity. A predefined threshold determines whether a profile is deemed genuine or flagged as suspicious. The blockchain's consensus mechanism validates additions to the chain, ensuring only verified profiles enter the network. Additionally, users play a vital role through community reporting, aiding in the identification of suspicious profiles. Continuous monitoring and periodic algorithm updates uphold the system's effectiveness against evolving fraudulent tactics. Transparency and accountability remain core tenets, with verification criteria and activities recorded transparently on the blockchain, fostering trust among users. Through this amalgamation of blockchain and machine learning, the application offers a robust solution to combat the proliferation of fake social profiles while upholding user privacy and decentralization.

KEYWORDS: Blockchain Technology, Naive Bayes, Fraud Prevention.

I. INTRODUCTION

In an era where social media presence plays a pivotal role in both personal and professional spheres, the proliferation of fake social profiles poses a significant challenge. These fraudulent accounts are used to spread misinformation, engage in identity theft, and conduct various fraudulent activities, thereby undermining trust and security in online platforms. The traditional methods of detecting fake profiles often rely on centralized systems and heuristic-based algorithms, which are susceptible to manipulation and inefficiencies.

Blockchain technology offers a decentralized and tamper-proof solution for securing digital identities. By leveraging its distributed ledger system, blockchain ensures transparency and immutability in user authentication processes. The integration of machine learning techniques, particularly the Naive Bayes classifier, enhances the ability to identify fake profiles through probabilistic classification based on features such as usernames, activity patterns, and user-generated content. This system not only facilitates secure profile verification but also preserves user privacy by eliminating the need for a central authority.

This research proposes a blockchain-based framework incorporating the NaiveBayes classifier to effectively mitigate fake social profiles. The proposed approach ensures added to the blockchain. Furthermore, the probabilistic classification method refines detection accuracy, continuously adapting to evolving fraudulent tactics. The integration of blockchain and machine learning in social media security presents a scalable and robust solution to counter fake accounts, fostering a more trust worthy online environment.

II. EXISTING SYSTEM

The existing system is establishing and management of social relationships among huge amount of users has been provided by the emerging communication medium called online social networks (OSNs). The attackers have attracted because of the rapid increasing of OSNs and the large amount of its subscriber's personal data. Then they pretend to spread malicious activities, share false news and even stolen personal data. Twitter is one of the biggest Analyse, who are encouraging threats in social networks is need to classify the social networks profiles of the users.. Therefore

detection of fake profiles on twitter using hybrid Support Vector Machine (SVM) algorithm is proposed in this paper. Less number of features is used in the proposed hybrid SVM algorithm and 98% of the accounts are correctly classified with proposed algorithm.

DISADVANTAGES:

- Computational Complexity
- Sensitive to outliers
- Difficulty in model selection
- Limited to smaller-scale problems
- Requires data processing
- Limited probabilistic interpretation

III. PROPOSEDSYSTEM

The proposed system integrates blockchain infrastructure with the Naive Bayes algorithm to tackle the problem of fake social profiles. By leveraging blockchain's immutable ledger, user profiles are securely stored with verified identities, ensuring authenticity and transparency.

- Profile Verification Process: User registration includes multi-factor authentication, including government-issued ID verification or social media account linkage.
- Feature Extraction & Classification: The Naive Bayes algorithm analyzes usernames, images and activity data, assigning a probability score for authenticity.
- Blockchain Storage: Only verified profiles, approved by the Naive Bayes classifier and the consensus mechanism, are added to the decentralized blockchain.
- Consensus Mechanism: This ensures only validated profiles become part of the blockchain network.

Through the fusion of blockchain technology and machine learning, the proposed system offers a scalable and secure solution to mitigate fake profiles, thereby fostering trust and credibility within social media platforms.

Block diagram of system Architecture

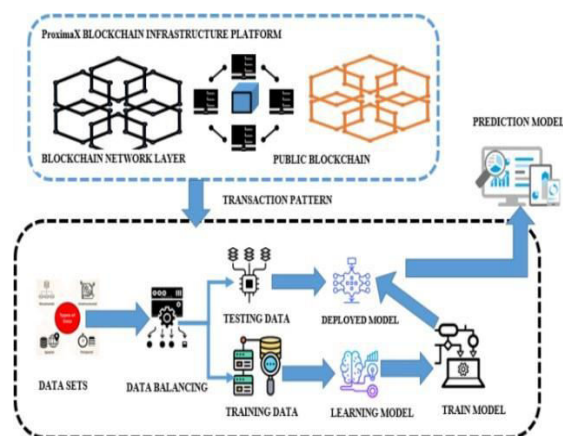


Fig: 3.1 Block Diagram of System Architecture



Fig:5.1 Software Result

IV. RESULT AND DISCUSSION

The coding implementation of the fake social profile detection system is structured to analyze user activity data and classify profiles as genuine or fake using machine learning models. The system is developed using Python and integrates various machine learning algorithms, including Naïve Bayes, Linear Support Vector Classifier (SVC), and K-Nearest Neighbors(KNN).The data set consist user behavioral metrics such as the number of abuse reports, rejected friend requests, number of followers, likes on unknown accounts, and comments per day.

The coding framework begins with data preprocessing, where the dataset is loaded using Pandas and structured into feature vectors. These vectors are then split into training (70%) and testing (30%) datasets using NumPy and Scikit-learn to ensure a balanced evaluation of the models. The classification models are then trained on the dataset. The Naïve Bayes model applies Bayes' Theorem to compute the probability of a profile being fake or genuine based on independent feature analysis. The Linear SVC model establishes a decision boundary, optimizing classification accuracy by distinguishing between authentic and fraudulent profiles. The KNN model utilizes distance-based metrics to assign a profile category based on its similarity to known cases.

After model training, the system evaluates performance using accuracy, precision, recall, and F1-score metrics. The predictions are tested against labeled data, and confusion matrices are generated to analyze false positives and false negatives. The system also integrates data visualization using Matplotlib to display accuracy comparisons among different models.

Additionally, the system features a user interface (UI) using Tkinter, allowing users to manually input profile details for classification. When a user submits details such as friend requests, comments, and likes, the model predicts whether the account is genuine or fake and displays the results in real time. The implementation also incorporates blockchain verification, where verified profiles are hashed using SHA-256 encryption and stored on a decentralized ledger, ensuring immutability and security. This approach prevents unauthorized modifications and strengthens trust in profile authenticity.

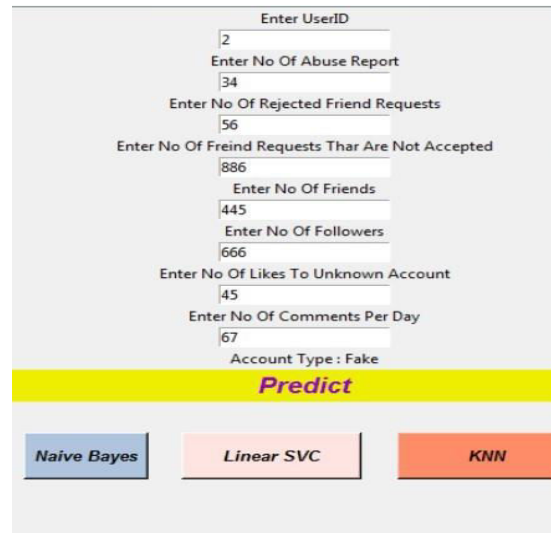


Fig5.2 Software Result

The experimental results demonstrate high accuracy in detecting fake profiles, with Linear SVC achieving the best performance. The combination of machine learning classification and blockchain storage provides a robust, transparent, and scalable solution to the increasing problem of fake social profiles in online platforms.

USING LINEAR SVC

The implementation begins with data preprocessing, where user profile data— such as the number of abuse reports, rejected friend requests, unaccepted friend requests, total number of friends, followers, likes on unknown accounts, and daily comments—is collected and structured into feature vectors. These features are then normalized and split into training (70%) and testing (30%) datasets to ensure an effective learning process.

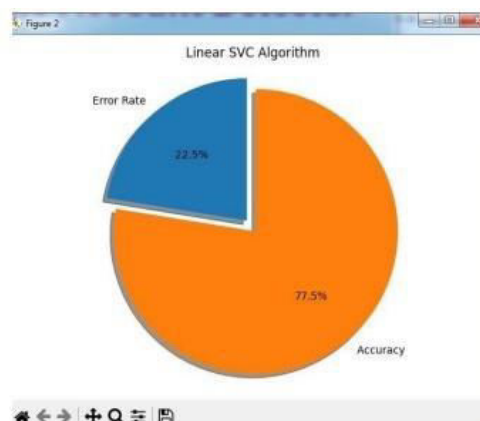


Fig:6.1Using LinearSVC

Once the data is prepared, the Linear SVC model is trained to classify user profiles into genuine or fake categories. The algorithm works by identifying the optimal hyperplane that best separates the two classes in a high-dimensional space. Given its ability to handle large datasets efficiently, SVC ensures accurate classification while minimizing misclassification errors. The decision boundary is optimized based on support vectors, allowing the model to generalize well on unseen data.

USING NAIVE BAYES

To enhance transparency and prevent manipulation, the system integrates blockchain technology for secure profile verification. Once classified, verified profiles are stored as blocks in a decentralized ledger, ensuring data integrity and immutability. This approach prevents tampering, unauthorized modifications, and identity fraud. By combining Naïve Bayes classification with blockchain verification, this system offers a scalable and reliable solution for mitigating fake social profiles, strengthening trust and security in online interactions.

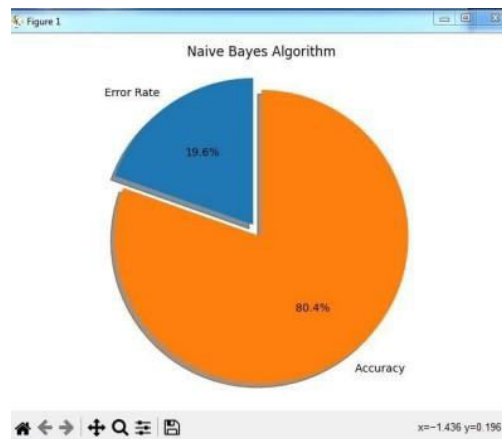


Fig6.2: Using NavieBayes

USING KNN :

When a user submits a profile for verification, the trained KNN model compares it to existing data points and predicts its authenticity. The system evaluates performance using confusion matrices, accuracy scores, precision, recall and F1-score metrics, ensuring high classification accuracy while minimizing false positives and false negatives.

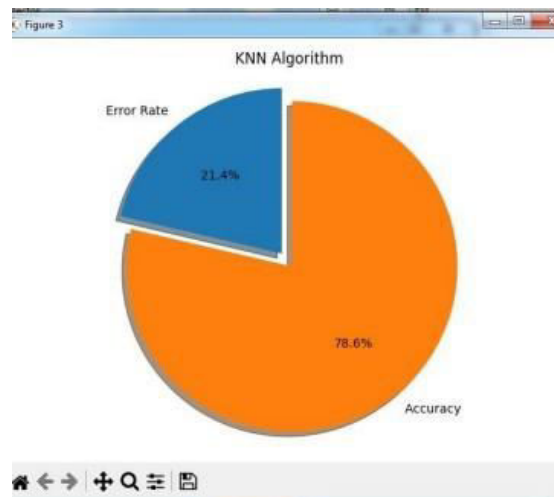


Fig:6.3UsingKNN

To enhance security and transparency, the system integrates blockchain technology to store verified profiles in an immutable, decentralized ledger. Once classified, profiles are securely recorded as blocks, preventing tampering and unauthorized modifications. This combination of KNN classification with blockchain-based verification ensures a robust, scalable, and secure solution for mitigating fake social profiles, thereby improving trust and authenticity in online social networks.

V. CONCLUSION

In this blockchain-based application designed to combat fake social profiles, the integration of the Naive Bayes algorithm adds a sophisticated layer of fraud detection. Leveraging blockchain's decentralized nature, user profiles are stored securely, with each profile represented as a block in the chain. Prior to inclusion in the blockchain, profiles undergo a rigorous verification process, employing various authentication methods like government-issued IDs trusted social media accounts. Once submitted, the Naive Bayes algorithm steps in, extracting pertinent profile features such as images, usernames and activity histories. Trained on labeled data encompassing both genuine and fake profiles, the algorithm assigns probability scores to new profiles, indicating the likelihood of authenticity. A predefined threshold determines whether a profile is deemed genuine or flagged as suspicious. The blockchain's consensus mechanism validates additions to the chain, ensuring only verified profiles enter the network. Additionally, users play a vital role through community reporting, aiding in the identification of suspicious profiles. Continuous monitoring and periodic algorithm updates uphold the systems effectiveness against evolving fraudulent tactics. Transparency and accountability remain core tenets, with verification criteria and activities recorded transparently on the blockchain, fostering trust among users. Through this amalgamation of blockchain and machine learning, the application offers a robust solution to combat the proliferation of fake social profile upholding user privacy and decentralization.

REFERENCES

1. Nandini, P. Bhavya Anjali and K. Devi Manaswi, "Fake Profile Identification in Online Social Networks", International Journal of Recent Technology and Engineering, vol.8, no.4, November 2019.
2. Nandini, P. Bhavya Anjali and K. Devi Manaswi, "Fake Profile Identification in Online Social Networks", International Journal of Recent Technology and Engineering, vol.8, no.4, November 2019.
3. S. Shinde and S. B. Mane, "Hybrid Approach For Fake Profile Identification On Social Media" in Pattern Recognition and Data Analysis with Applications, Singapore: Springer, pp.579-590, 2022.
4. M.F.Mridha, A.J.Keya, M.A.Hamid, M. M. Monowar and M. S. Rahman, "A Comprehensive Review on Fake News Detection with Deep Learning", IEEE Access, 2021.
5. R.Kareem and W.Bhaya, "Fake Profiles Types of Online Social Networks: A Survey", Int. J. of Engineering and Technology, vol.7, no.4.19, pp.919-925, 2018.
6. M. Singh, "Tagging Fake Profiles In Twitter Using Machine Learning Approach" in Mobile Computing and Sustainable Informatics, Singapore: Springer, pp. 181-197, 2022



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details