PIP2001 Capstone Project
Final review

Fake Social Media Profile Detection and Reporting Using Machine learning and Blockchain

Batch Number:

Roll Number	Student Name
20211CCS0003	Devatheertha E
20211CCS0005	Shreenidhi G S
20211CCS0007	Nithish V S
20211CCS0010	Hazil Ahammed C
20211CCS0012	Sreerag A

Under the Supervision of,
Ms. Sridevi S
Assistant Professor
School of Computer Science and Engineering
Presidency University

Name of the Program: B.Tech CSE(Cybersecurity)
Name of the HoD: Dr. Anandaraj S P
Name of the Program Project Coordinator: Dr. Sharmasth vali
Name of the School Project Coordinators: Dr. Sampath A K / Dr. Abdul Khadar A / Mr. Md Ziaur Rahman

Introduction

Fake social media profiles have become a significant threat, leading to misinformation, fraud, and security risks. Traditional detection methods, such as manual reporting and rule-based systems, often fail to accurately identify fraudulent accounts.

This project aims to **detect and report fake social media profiles** using a combination of **Machine Learning (ML) and Blockchain technology**.

Machine learning models such as **Random Forest, Support Vector Machines (SVM), Artificial Neural Networks (ANN) and XGBoost** analyze profile features (e.g., follower count, bio length, profile picture) to classify accounts as **real or fake**.

Blockchain ensures **secure, immutable storage** of detected fake profiles and user reports, preventing data manipulation and enhancing transparency. By integrating **ML for detection** and **blockchain for security**, this project provides an **efficient, automated, and trustworthy solution** for combating fake profiles on social media platforms.

- **Problem Statement:** Fake social media profiles contribute to misinformation, fraud, and security risks.
- **Project Objective:** To detect and report fake social media profiles using **Machine Learning (ML) and Blockchain technology**.
- **Machine Learning Approach:** Models such as **Random Forest, Support Vector Machines (SVM), and Artificial Neural Networks (ANN)** and **XGBoost** analyze profile features (e.g., follower count, bio length, isPrivate and has Profile photo) to classify accounts as **real or fake**.
- **Blockchain for Security:** Ensures **secure, immutable storage** of detected fake profiles and user reports, preventing data manipulation and enhancing transparency.
- **Outcome:** Provides an **efficient, automated, and trustworthy solution** for combating fake profiles on social media platforms.

Literature Review

- Fake Profile and Bot Detection:
  Research in the field has focused on detecting fake social media profiles and bots using machine learning techniques. Studies have shown that features derived from user behavior, textual content, and network structure are highly effective for classification.

- Random Forest & SVM in Social Media Analysis:
  Several studies have compared ensemble methods (such as RF) and kernel-based methods (such as SVM) for detecting anomalies in social media data. Both have demonstrated high accuracy and robustness in experimental settings.

- Blockchain for Data Integrity:
  Recent work explores the integration of blockchain with machine learning to ensure the integrity and trustworthiness of data. Blockchain provides a decentralized mechanism to record and verify detection outcomes.

Existing method Drawback

- **Lack of Scalability:** Manual reporting cannot efficiently handle the vast number of fake profiles on large social media platforms.
- **Data Manipulation Risks:** Centralized storage of fake profile reports can be altered or removed, reducing credibility.
- **Slow Detection Process:** Traditional methods rely on user reporting, making fake profile detection reactive rather than proactive.
- **Limited Adaptability:** Rule-based detection struggles to keep up with evolving tactics used by fake accounts.
- **Lack of Transparency:** Users have no way to verify reported fake profiles, leading to distrust in detection mechanisms.
- **No Secure Audit Trail:** Without blockchain, there is no immutable record of reported fake profiles, making tracking difficult.

Proposed Method

This project proposes a hybrid approach that integrates machine learning models with blockchain technology to improve the detection and verification of fake social media profiles.

Key Components of the Proposed System:

- **Machine Learning-Based Fake Profile Detection**
  - Three machine learning models (Random Forest, SVM, XGBoost, and ANN) are used to classify profiles as real or fake based on extracted features.
  - Features such as follower count, following count, bio length, profile photo presence, and privacy status are used for classification.
  - A dataset with labeled fake and real profiles is used to train the models.
- **Blockchain Integration for Security and Transparency**
  - Ethereum blockchain is used to store flagged fake profiles in an immutable ledger.
  - Smart contracts automate the verification and reporting of fraudulent accounts.
  - InterPlanetary File System (IPFS) is used for decentralized storage of reported profiles.
- **User Interface for Profile Verification**
  - A Django-based web application allows users to input profile data and receive real-time predictions.
  - A fraudulent profile reporting system enables users to report suspicious accounts, with all reports being securely stored on the blockchain.

Dataset for the project

For our Fake Social Media Profile detection application, we assembled a dataset comprising real and fake social media profiles.

The dataset includes features such as:

- **Profile Metadata:** Account age, number of friends/followers, frequency of posts, profile picture existence, bio information, and language usage.
- **Behavioral Patterns:** Posting frequency, engagement metrics (likes, comments, shares), and activity time-series data.
- **Textual Data:** Natural language content from posts, comments, and profile descriptions.
- **Network Features:** Connection patterns, friend network clustering, and interaction graphs.
- **Data Sources:**
- **Publicly Available Datasets:** We leveraged open-source datasets (e.g., from research projects on social bot detection) that include labeled examples of genuine and fake profiles.
- **Scraped Data:** With proper ethical guidelines and data usage policies, we also scraped social media platforms using APIs (e.g., Twitter API) to enrich our dataset.
- **Synthetic Data:** In cases where data was imbalanced or under-represented, we applied data augmentation techniques to simulate fake profiles based on known behavioral patterns.

Machine learning algorithms:

RANDOM FOREST(RF):

What is Random Forest?

- An **ensemble learning method** that builds a collection of decision trees.
- Each tree votes, and the **majority class** becomes the final prediction.
- Works by combining multiple models to reduce variance and increase accuracy.

Why Random Forest for Fake Profile Detection?

- **Handles structured/tabular data** very well.
- **Robust to noisy data** and overfitting due to averaging.
- Useful for **feature importance analysis** – helps understand which profile features matter most

Machine learning algorithms:

SUPPORT VECTORE MACHINE(SVM):

What is SVM?

- A **supervised learning algorithm** used for classification tasks.
- Finds the **optimal hyperplane** that best separates two classes (real vs fake profiles).
- Maximizes the **margin** between the nearest data points (support vectors).

How It Works in Our Project

- Feature vectors represent user behaviors and attributes.
- SVM calculates the best boundary that distinguishes fake from genuine profiles.
- Kernel trick used (e.g., RBF) to handle non-linear data.

Machine learning algorithms:

ANN(Artificial Neural Network)

What is an ANN?

- An **Artificial Neural Network** is a computing model inspired by the structure of the human brain.
- Consists of layers of **neurons** (nodes) interconnected through **weights**.
- Capable of **learning complex, nonlinear relationships** in data.

Why ANN for Fake Profile Detection?

- Capable of **capturing subtle correlations** in user behavior that traditional algorithms might miss.
- Learns **nonlinear decision boundaries** that are often present in complex datasets like social media.
- Performs well even when feature importance is not clearly defined.

Machine learning algorithms:

XGBoost

What is XGBoost?

- **Extreme Gradient Boosting** – a powerful boosting algorithm.
- Combines weak learners (usually decision trees) in a **sequential** manner.
- Each new model focuses on **correcting the errors** made by previous ones.
- Uses advanced regularization techniques (L1 & L2) to avoid overfitting.

Why XGBoost?

- Highly efficient and scalable.
- Excellent accuracy and performance.
- Built-in handling of missing values and regularization.

Machine learning algorithm comparisons with other algorithms

Random Forest (RF):

- **Why:** RF is an ensemble learning method that builds multiple decision trees and merges their outputs. It is robust to overfitting, works well with both numerical and categorical data, and can effectively capture complex, non-linear interactions between features.
- **Comparison:**
  - **Versus Logistic Regression:** While logistic regression is faster and easier to interpret, it may struggle with non-linear relationships that RF can capture.
  - **Versus Naïve Bayes:** Naïve Bayes is computationally efficient and works well with text data; however, its strong independence assumptions often do not hold in social network data.

Support Vector Machines (SVM):

- **Why:** SVM is effective in high-dimensional spaces and can handle non-linear boundaries through kernel functions. It works particularly well with text-based features after vectorization.
- **Comparison:**
  - **Versus Decision Trees:** While decision trees are easy to interpret, SVM generally provides a more stable decision boundary when the feature space is complex.

ANN(Artificial neural network)

Why: ANN is inspired by the human brain’s neural structure. It uses layers of interconnected neurons to model and learn complex, nonlinear patterns. In the context of fake profile detection, ANN is especially valuable for capturing hidden patterns in user behavior and engagement metrics.

- **Comparison:**
- **Versus Naïve Bayes:** Naïve Bayes assumes feature independence and often falls short on complex data; ANN thrives on discovering dependencies and nonlinear relationships.

Extreme Gradient Boosting (XGBoost):

Why: XGBoost is a powerful and efficient implementation of gradient-boosted decision trees. It builds models sequentially, where each model corrects the errors of its predecessor. It includes regularization to reduce overfitting and supports parallel computation, making it ideal for high-accuracy, real-world applications.

Comparison:

- **Versus Logistic Regression:** Logistic regression is simple and interpretable but struggles with feature interactions and nonlinearity, which XGBoost handles natively and efficiently.

Purpose of Blockchain Technology & Its Integration

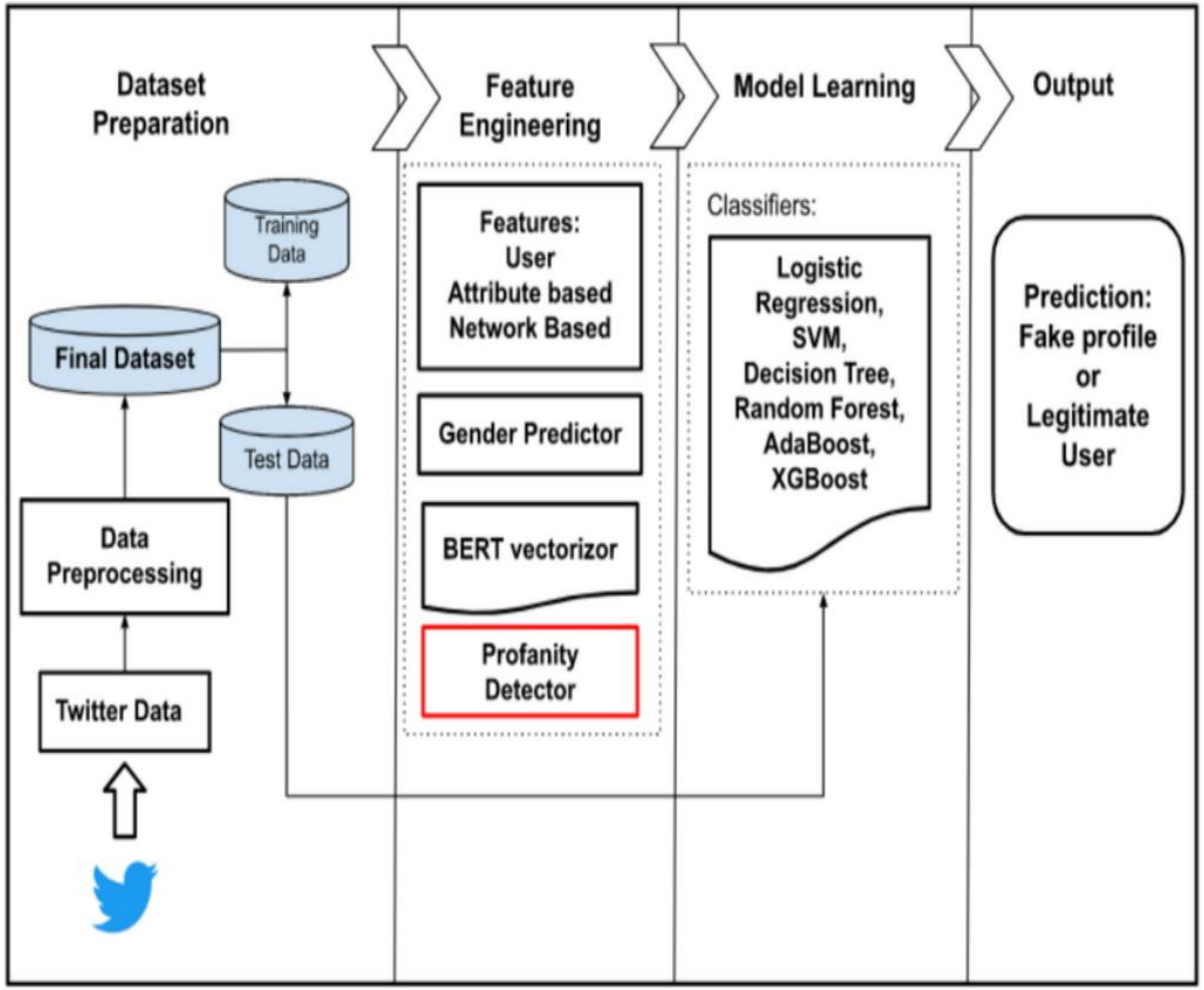
Purpose of Blockchain:

- **Data Integrity & Immutability:** Blockchain ensures that once a profile is flagged as fake and reported, the record is tamper-proof. This is critical when decisions need to be auditable and transparent.
- **Trust & Transparency:** By recording detection outcomes and reports on a blockchain, stakeholders (such as platform moderators, law enforcement, or the public) can verify that the detection and reporting process was conducted in a transparent and unbiased manner.
- **Decentralization:** Blockchain removes single points of failure, ensuring that the report data remains accessible and unaltered even if one part of the system is compromised.

Integration with the Machine Learning Model:

- **Workflow Integration:**
  - **Detection:** The ML models (RF and SVM) process incoming profile data and flag profiles as genuine or potentially fake.
  - **Reporting:** Once a profile is flagged as fake, a report is generated.
  - **Blockchain Logging:** The report—comprising the profile ID, detection score, timestamp, and possibly a cryptographic hash of the profile data—is stored on the blockchain using smart contracts.
- **Smart Contracts:**
  - They automate the reporting process. When the ML model flags a profile, the smart contract is triggered to log the event.
  - This ensures that every detection is recorded in an immutable ledger, which can later be used for audits or further analysis.
- **Interoperability:**
  - The system uses an API layer that interacts with both the ML prediction service and the blockchain network, ensuring smooth data flow and integration.

Architecture



Technologies Used:

Frontend Technologies:
HTML & CSS: Structure and design of the web interface.
JavaScript: Enhances interactivity and handles dynamic updates.

Backend Technologies:
Django (Python Web Framework): Handles user interactions, machine learning model integration, and blockchain transactions.
Python: Used for backend logic, machine learning model execution, and blockchain communication.

Machine Learning Technologies:
scikit-learn: Implements classification algorithms such as Random Forest, Support Vector Machine (SVM), and Artificial Neural Networks (ANN) for detecting fake profiles.
pandas & numpy: Process and structure user data for model prediction.
pickle: Saves and loads trained models for efficient execution.

Blockchain Technologies:
Ethereum Blockchain: Stores immutable records of detected fake profiles and user reports.
Smart Contracts: Automates verification and reporting mechanisms, ensuring transparency and preventing data manipulation.
IPFS (InterPlanetary File System): Decentralized storage for profile reports, preventing unauthorized alterations.

Machine Learning Models:
Random Forest (RF): An ensemble learning method based on decision trees that effectively handles large datasets and captures non-linear relationships.
Support Vector Machine (SVM): A supervised classification algorithm that identifies fake profiles based on feature analysis.
Artificial Neural Network (ANN): A deep learning model that captures complex patterns in user profiles, improving detection accuracy over time.

Timeline of Project

Conclusion

- **Enhanced Detection Accuracy:** Machine learning models effectively classify fake profiles with high precision.
- **Improved Security & Transparency:** Blockchain ensures immutable storage and prevents tampering of reported fake profiles.
- **Automation & Efficiency:** The integration of ML reduces human intervention, making the detection process faster and more reliable.
- **Scalability:** The system can handle large amounts of social media data, making it suitable for real-world applications.
- **Reduction in Fraud & Misinformation:** By detecting fake profiles accurately, the system helps improve the integrity of social media platforms.
- **Future Scope:** The project can be expanded with deep learning models and real-time detection capabilities for even better accuracy and performance.

Github Link

The Github link provided should have public access permission.

Github Link
https://github.com/shreeeeeeeeeeeeeeeee/Fake-Profile-Detection-on-Social-Networking-Using-Machine-learning-and-Blockchain-.git

References

[1]. "Fake Media Detection Based on Natural Language Processing and Blockchain Approaches", ZEINAB SHAHBAZI AND YUNG-CHEOL BYUN IIST, Department of Computer Engineering, Jeju National University, Jeju-si 63243, South Korea

[2]. "FAKE PROFILE IDENTIFICATION USING MACHINE LEARNING",T.Sudhakar

[3]. "Machine learning-based social media bot detection: a comprehensive literature review", Malak Aljabri · Rachid Zagrouba · Afrah Shaahid · Fatima Alnasser · Asalah Saleh · Dorieh M. Alomari

[4]. "Using Machine Learning to Detect Fake Identities: Bots vs Humans",ESTÉE VAN DER WALT AND JAN ELOFF Department of Computer Science, University of Pretoria, Pretoria 0002, South Africa

[5]. "Fraud detections for online businesses: a perspective from blockchain technology" ,Zicklin School of Business, Baruch College, City University of New York, New York, NY, USA. 2 College of Business, Iowa State University, Ames, IA, USA.

Project work mapping with SDG

SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

The Project work carried out here is mapped to SDG-9: Industry, Innovation, and Infrastructure

The use of AI and blockchain promotes innovation in cybersecurity and digital infrastructure. It enhances technological resilience in online platforms by automating fake profile detection.

Thank You