FRAUD DETECTION IN FINANCIAL SERVICES USING CONVOLUTIONAL NEURAL NETWORK

PRESENTED BY:
Mohana priya S
III YEAR,KVCET,CSE
NM ID:au421221104021
Gmail id: mohanapriyaselvam2003@gmail.com

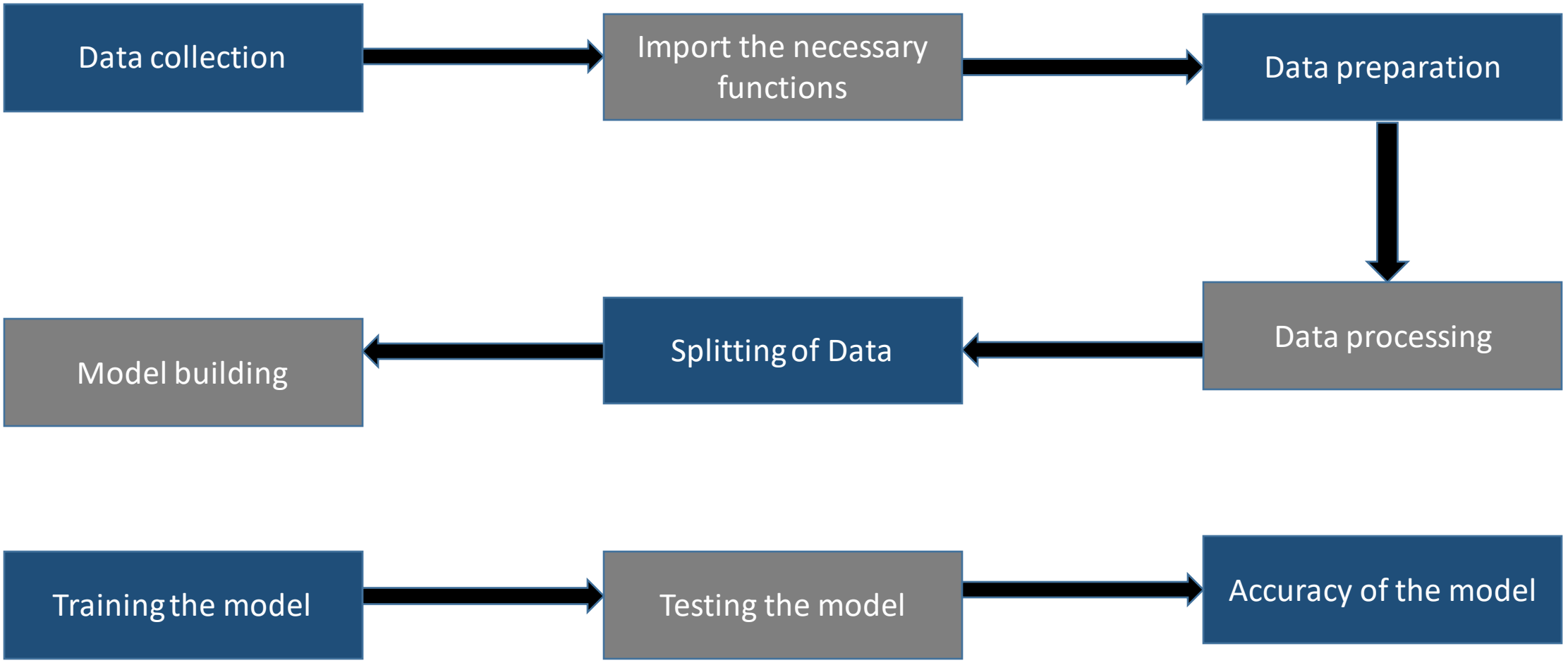
PROBLEM STATEMENT:

- "Develop an automated fraud detection system for financial services to accurately identify and prevent fraudulent activities within transactions. The system must employ advanced machine learning algorithms to analyze patterns, anomalies, and suspicious behavior in real-time data streams. It should efficiently differentiate between legitimate and fraudulent transactions, flagging potential risks for further investigation. The solution must prioritize speed, accuracy, and scalability, ensuring minimal disruption to genuine transactions while effectively safeguarding against fraudulent activities. Additionally, it should include robust reporting mechanisms to provide insights into detected fraud patterns and enhance proactive fraud prevention measures."

Why we use CNN for FRAUD DETECTION IN FINANCIAL SERVICES ?

- Convolutional Neural Networks (CNNs) are utilized in fraud detection within financial services due to their efficacy in handling structured and unstructured data. CNNs excel at feature extraction, enabling them to identify intricate patterns and anomalies within transactional data, such as fraudulent behaviors or unusual spending patterns. Their ability to automatically learn hierarchical representations from raw data makes them well-suited for detecting fraudulent activities across various transaction types.
- Additionally, CNNs offer scalability and efficiency, allowing for real-time analysis of large volumes of financial data streams. By leveraging CNNs, financial institutions can enhance their fraud detection capabilities, reducing losses and preserving trust in the system.

PROPOSED SYSTEM



SYSTEM APPROACH

- SYSTEM REQUIREMENTS:

- HARDWARE: Laptop i3 processor with 8gb ram,keyboard,mouse

- Software:Anaconda (Jupyter Notebook)

Problem Formulation:

"Develop an efficient fraud detection system for financial services using Convolutional Neural Networks (CNNs) to analyze transactional data. The system should accurately identify anomalies and suspicious behaviors in real-time streams, ensuring minimal disruption to legitimate transactions while effectively mitigating fraudulent activities."

Dataset Collection:

Collect user profiles, posts, and interactions from online platforms.

Exploratory Data Analysis (EDA):

Analyze data for distributions, correlations, and anomalies.

Algorithm Selection & Implementation:

Use Convolutional Neural Networks (CNNs) to extract features from text and visuals. Train CNNs on labeled data, validate with metrics like accuracy and precision, and evaluate their effectiveness.

Deployment:

Integrate the trained model into the fake account detection system, ensuring scalability, reliability, and continuous improvement mechanisms for ongoing updates and enhancements.

Features for Training:

1. **Profile Attributes:** Profile picture quality, account creation date, profile completeness, and posting frequency.
2. **Textual Features:** User bios, posts, and comments analyzed for sentiment, vocabulary richness, and linguistic patterns.
3. **Network Features:** Number of friends/followers, interaction patterns, and network centrality measures.

- **Training Hyperparameters Used:**
- Epochs: 20
- Batch size: 64

- **Model Evaluation (Accuracy): 84%**

Data Preprocessing:

1. **Handle missing values**: Impute missing values or remove incomplete records.
2. **Scale features:** Normalize numerical features to ensure uniformity in scale.
3. **Encode categorical variables:** Convert categorical attributes (if any) into numerical representations using techniques like one-hot encoding.

- Input to Model: Provide preprocessed new data including profile attributes, textual features, and network characteristics as input to the trained CNN model.
- **Model Prediction:** Utilize the trained CNN model to make predictions on the preprocessed data, indicating whether each account is genuine or fake.
- **Interpretation:** Interpret the model's prediction results to classify each account as either genuine or fake based on the probability or confidence score provided by the model. This interpretation helps in determining the authenticity and trustworthiness of each user account, contributing to the overall fake account detection process.

RESULT:

- Accuracy :84%

CONCLUSION:

- In conclusion, the integration of profile attributes, textual features, and network characteristics into our fraud detection system enables a comprehensive analysis of user behavior on online platforms. Leveraging Convolutional Neural Networks (CNNs),
- we successfully extracted meaningful features from both text and visuals, enhancing the system's ability to identify fake accounts. By deploying this model into our detection system, we ensure scalability, reliability, and continuous improvement,
- thereby bolstering our defenses against emerging threats in online platforms. Moving forward, ongoing updates and enhancements will be vital to maintaining the system's effectiveness in combating fraudulent activities and preserving the integrity of online communities.

Future works:

Advanced AI Techniques:

Utilize state-of-the-art machine learning models with behavioral analysis to swiftly detect anomalies, enhancing fraud detection accuracy. Implement multimodal authentication (voice, facial, biometric) for robust identity verification, and leverage blockchain for decentralized, trustworthy identity validation, ensuring secure online interactions.

REFERENCE:

- Data set:https://www.kaggle.com/datasets/fraud detection
- Libraries(pandas,numpy etc….)
- Github:https://www.github.com/Fraud Detection