Online_Imposters

Fake social media account detector

TEAM MEMBERS

HARSHITHA. RS 22011103018

KAVINI. M 22011103021

PADMAJAA. S 22011103039

USE CASES

Spam and Phishing Prevention with Naive Bayes Classifier:

To effectively safeguard users against unsolicited messages and potential scams, the platform can employ the Naive Bayes Classifier, a robust machine learning algorithm for text classification. This enables the system to discern and promptly address suspicious messages with precision and accuracy.

USE CASES

Preventing Misinformation and Disinformation with Natural Language Processing (NLP):

- By integrating sophisticated Natural Language Processing algorithms, the platform can effectively combat the spread of false or misleading information. This empowers the system to analyze content, discern language patterns, and identify context, thereby mitigating the dissemination of misinformation and disinformation.

Election and Political Campaign Integrity via Network Analysis and Anomaly Detection:

- By employing Network Analysis and Anomaly Detection algorithms, the platform can bolster the integrity of elections and political campaigns. This advanced technology allows for the identification of suspicious accounts engaged in manipulative activities, ensuring a fair democratic process.

USE CASES

Brand Reputation Management with Image Recognition and Text Analysis:

•To safeguard brands and public figures from impersonation, Image Recognition and Text Analysis algorithms can be harnessed. This empowers the platform to swiftly identify and act against fake accounts, thereby preserving reputations and maintaining trust.

User Privacy Protection through Behavioral Anomaly Detection:

•By implementing Behavioral Anomaly Detection, the platform can proactively safeguard user privacy. This algorithm identifies aberrant patterns in user behavior, effectively blocking fake accounts engaged in data collection or stalking.

Ensuring Fair Competitions with Fraud Detection Algorithms:

•To guarantee fair participation in competitions and giveaways, the platform can deploy Fraud Detection algorithms. This technology identifies and eliminates fake accounts, ensuring an equitable and transparent competitive environment.

USE CASES

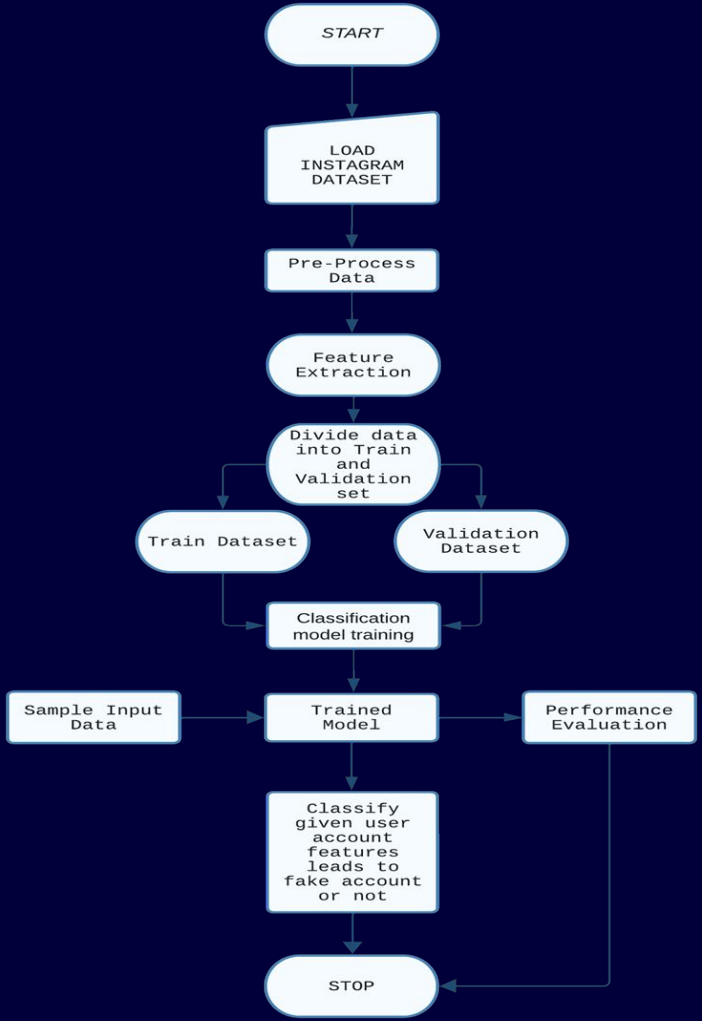
Ad Fraud Prevention using Machine Learning for Anomaly Detection:

•Harnessing Machine Learning for Anomaly Detection, the platform can effectively thwart ad fraud. This algorithm discerns deceptive engagement, providing advertisers with accurate insights and safeguarding against fraudulent activities.

Tracking Online Influence Campaigns using Network Analysis:

•Leveraging Network Analysis, the platform can effectively track and counter online influence campaigns. This enables the identification of fake accounts central to political, social, or economic motivations, safeguarding the integrity of online discourse.

FLOWCHART


START
LOAD INSTAGRAM DATASET
Pre-Process Data
Feature Extraction
Divide data into Train and Validation set
Train Dataset
Validation Dataset
Classification model training
Sample Input Data
Trained Model
Performance Evaluation
Classify given user account features leads to fake account or not
STOP

TECH STACK

Programming Languages:- Python

Machine Learning Libraries: Scikit-learn, TensorFlow or PyTorch

Natural Language Processing (NLP):NLTK (Natural Language Toolkit) or SpaCy

Facial Recognition and Image Analysis: OpenCV

Dlib: Provides tools for facial detection and landmark

DJANGO: For frontend development

DFEATURE EXTRACTION - KEY FEATURES:

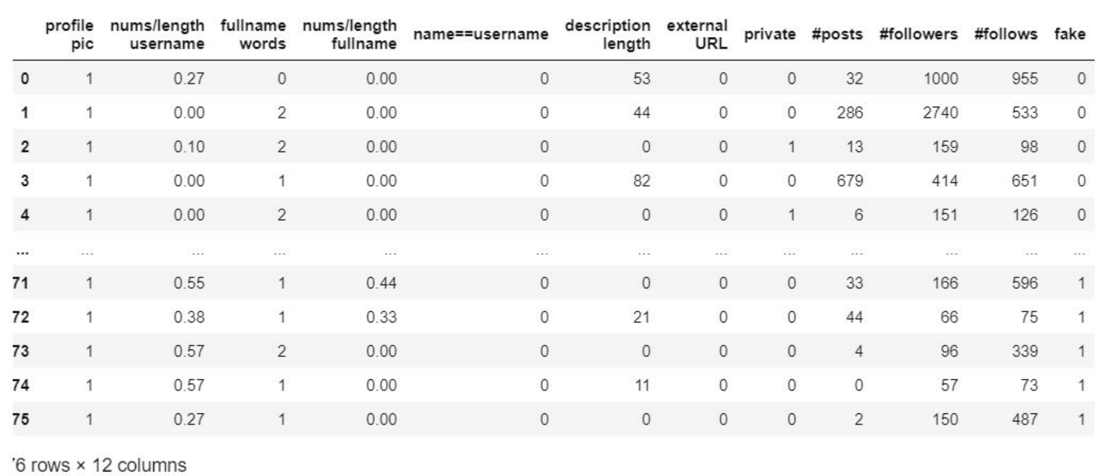
- PROFILE PICTURE - The user has profile picture or not.
- FULLNAME WORDS - Full name in word tokens
- NAME == USERNAME - Are username and full name literally the same?
- DESCRIPTION LENGTH - Bio length in characters.
- EXTERNAL URL - Has external URL or not.
- PRIVATE - Private or not.
- POSTS - Number of posts.
- FOLLOWERS and FOLLOWS

KEY FUNCTIONS IMPLEMENTED FOR THE PROJECT:

- Softmax output layer for multi-class classification.
- ReLU activation in hidden layers as it can accelerate training.
- ANNs good for learning repeating patterns from past data.

This model is trained such that it considers the above given features and determines whether a particular account is fake or not. By resulting the output as either 0 or 1 meaning TRUSTED or FAKE respectively. Our intention is to make this software capable of thinking like a human, based on the data it is given and results in maximum probability of success.

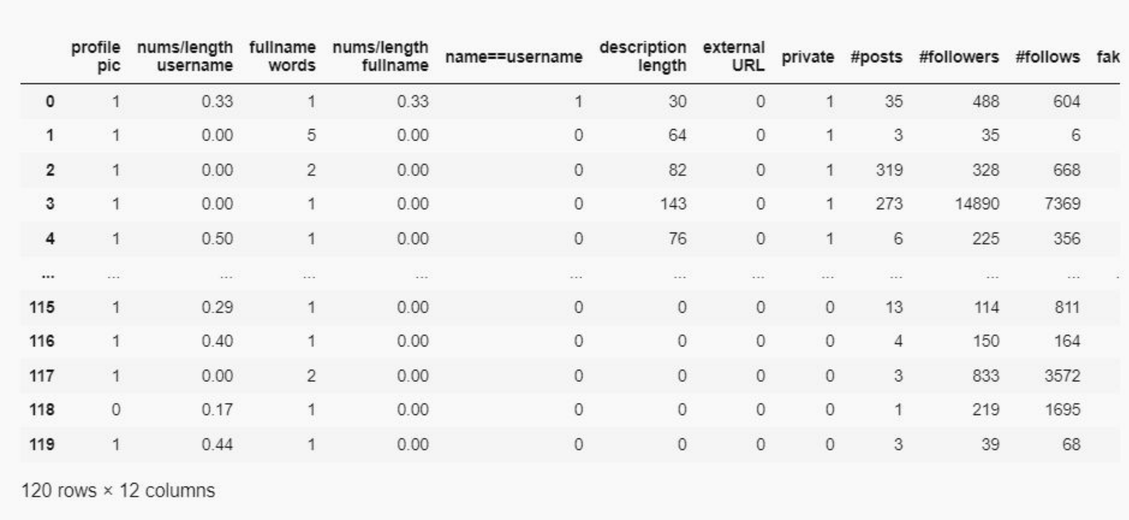
DSample Train dataset description :



	profile pic	nums/length username	fullname words	nums/length fullname	name==username	description length	external URL	private	#posts	#followers	#follows	fake
0	1	0.27	0	0.00	0	53	0	0	32	1000	955	0
1	1	0.00	2	0.00	0	44	0	0	286	2740	533	0
2	1	0.10	2	0.00	0	0	0	1	13	159	98	0
3	1	0.00	1	0.00	0	82	0	0	679	414	651	0
4	1	0.00	2	0.00	0	0	0	1	6	151	126	0
...	...	...	...	...	...	...	...	...	...	...	...	...
71	1	0.55	1	0.44	0	0	0	0	33	166	596	1
72	1	0.38	1	0.33	0	21	0	0	44	66	75	1
73	1	0.57	2	0.00	0	0	0	0	4	96	339	1
74	1	0.57	1	0.00	0	11	0	0	0	57	73	1
75	1	0.27	1	0.00	0	0	0	0	2	150	487	1

’6 rows × 12 columns

Sample Testing dataset description :



	profile pic	nums/length username	fullname words	nums/length fullname	name==username	description length	external URL	private	#posts	#followers	#follows	fak
0	1	0.33	1	0.33	1	30	0	1	35	488	604	
1	1	0.00	5	0.00	0	64	0	1	3	35	6	
2	1	0.00	2	0.00	0	82	0	1	319	328	668	
3	1	0.00	1	0.00	0	143	0	1	273	14890	7369	
4	1	0.50	1	0.00	0	76	0	1	6	225	356	
...	...	...	...	...	...	...	...	...	...	...	...	
115	1	0.29	1	0.00	0	0	0	0	13	114	811	
116	1	0.40	1	0.00	0	0	0	0	4	150	164	
117	1	0.00	2	0.00	0	0	0	0	3	833	3572	
118	0	0.17	1	0.00	0	0	0	0	1	219	1695	
119	1	0.44	1	0.00	0	0	0	0	3	39	68	

120 rows × 12 columns