FAKE ACCOUNT DETECTION FROM URL FEATURES USING MACHINE LEARNING AND DEEP LEARNING

Sofian Khan[1], Mohammad Ilyas[2], Shaik Sarfaraz[3], Dr. Mohammed Rahmat Ali[4]

[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.

[4]Assistant Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

ABSTRACT: Currently, social media has a significant impact on the lives of individuals. On a daily basis, the bulk of individuals are dedicating their time to social media sites. The number of accounts on these social networking sites has been steadily expanding on a daily basis, and a significant portion of users are engaging with others regardless of their time and place. These social media platforms offer advantages and disadvantages, and they also pose security risks to our personal information. In order to identify the individuals responsible for making threats on these social networking sites, it is necessary to categorize the accounts into authentic and fraudulent ones. Historically, many categorization approaches have been used to identify counterfeit accounts on social media. However, it is essential to enhance the precision of spotting counterfeit accounts on these platforms. Our work utilizes Machine Learning technologies, namely Deep Learning and Natural Language Processing (NLP), to enhance the accuracy of identifying bogus accounts based on URL attributes. We choose to use the Random Forest tree classifying technique.

INTRODUCTION

Social media has emerged as the most captivating medium in the modern world, captivating consumers who spend countless minutes on these services. These social media platforms effectively address a wide range of issues, from little inconveniences to major challenges. [1]. Enhancing security measures and safeguarding against malicious websites are crucial factors that have become more challenging. Through the usage of social media, individuals engage with unfamiliar users and disclose their personal information. This may potentially give rise to various forms of dangers. Several social media strategies have been suggested; however, they often depend on non-publicly accessible data for LinkedIn profiles. The user's text is "[2]." An approach based on features to identify fraudulent Twitter profiles The input consists of the numbers 3 and 4 enclosed in square brackets. Social media platforms are susceptible to several forms of assaults, with file theft being the most significant. When a someone appropriates someone else's knowledge for their own personal gain, it is theft and poses a significant concern. Victims may be subject to consequences. For instance, individuals may assume the identity of others and commit errors that have a negative impact on the affected person's reputation within society. Indeed, several Social Network programs have the default setting for data protection at the minimum level.Thus, the Social Network has emerged as the most effective platform for perpetrating fraud and engaging in abusive behavior.Social media facilitates the execution of identity theft and phishing attempts by both sophisticated and inexperienced perpetrators.Furthermore, users are required to establish an account on the social networking platform, exacerbating the situation.The potential consequences of loss, particularly in the event of unauthorized access to such accounts.The configuration file information in the internet network might

be either static or dynamic.During the profile time, individuals have the opportunity to contribute comprehensive information.Creation is referred to as static knowledge.Static knowledge include a person's demographic information and hobbies, while dynamic knowledge pertains to a person's leadership practices and present place in studies. These studies are conducted using both static and dynamic data.The network often consists of both static and dynamic configuration files. This innovative study has put forward many methodologies to detect counterfeit identities and dangerous information on social networking sites.Each approach has its own set of advantages and disadvantages.Instances of bullying, abuse, and trolling, among other similar behaviors.False personal information is often used on specialized platforms, resulting in the presence of both male and female accounts with inaccurate data.False personal information on Facebook is mostly used for nefarious purposes targeting users inside social networks.Individuals fabricate deceptive social engineering materials with the intention of engaging in phishing, which seeks to undermine or belittle an individual, as well as to advocate for or motivate a collective group of individuals.The term "Facebook Immune System (FIS)" is often used to describe the system that deals with issues such as spam and fraudulent identities on Facebook.Currently, the ability to thoroughly examine the fraudulent user accounts generated for Facebook consumers is not yet available. Artificial intelligence (AI) refers to the cognitive capacity of a computer program or machine to engage in thinking and learning processes.Additionally, it is a field of study that seeks to enhance the intelligence of computers [5]. Artificial intelligence refers to the use of computer science programming to imitate human cognitive processes and behavior. This is achieved via the analysis of data and the environment, problem-solving and prediction, as well as learning and self-teaching in order to adapt to various tasks and situations.

LITERATURE SURVEY

1. Bhadra Rrb, Yin yang symbol Pg, Somayajulu Hd, Resort RR, Rattan RR, Resort RR, Riddle RR, Trounce RR, Identification of socially destructive robots in the Form of tweets using learning automaton and ip characteristics. Industrial Electronics on Algorithmic Social Processes, vol. 7, no. 4, pp. 1004-18, May 14, 2020.

Within the following context, we want to examine the interconnectedness of the characteristics and their impact on MSBD. A technique called LA-MSBD has been created by combining a reliable computer program with web address features to teach sentient robots in recognizing socially damaging bots. By integrating probabilistic training with sentiment analysis, we can assess the reliability or trustworthiness of Twitter. The LA-MSBD approach improves accuracy by up to 7% compared to existing algorithms for fraudulent business and virtual Botnet data sources. The Que le technique achieved an accuracy rate of 95.37 percent for MSBD and 91.77 percent for LA.

2. B. Zhang, Officinalis Huang, Y. Xiao, K. Cheng, and X. Zhang. Detecting sociable hackers in Facebook with improved conditioned fcn. IEEE Accessibility, vol. 8, no. 2, 2020, pp. 36664-80.

The next emphasis will be on the additional behaviors and characteristics of socially damaging robots. Extends to more social networking platforms In order to establish a framework for robot detection on social media, it is

necessary to examine platforms such as Facebook and Pinterest, as well as consider the role of computer security and the integration of current systems. In order to improve the overall detection performance of social bots, an advanced conditionally deep convolutional architecture (improved CGAN) was used to expand imbalanced data sets after training classifications. In order to enhance additional circumstances, we will modify the clustering approach. The Polynomial Kernel Densities Peaking Clustering Approach (GKDPCA) aims to minimize information noise and address inequalities across social groups. This measure inhibits the generation of distorted information and minimizes discrepancies within and between the majority class of sociable bots. The updated CGAN outperformed the three most commonly used oversampling algorithms with an F1 score of 97.56 percent. When it comes to creating social robots, efficient oversampling is a crucial factor.

3. Al Pelgrum, R. Sharma, and A. B. S. R. Performing the actions Networking robots and prominent members in online communities are detected using an adjustable shallow Camille system. 2018 Nov;49(11):3947-64.

Computational AI. User-generated content is a popular online community networking (OSN) for news and commentary. However, it is full with fraudulent accounts that disrupt OSNs. Social bots affect Sina Weibo, a popular Chinese OSN. Social bots on Sina Weibo are harder to recognize since they blend in. First, social chatbot traits are hard to extract. Large-scale data collection and classification of user data is tough. Third, typical classification techniques fail to recognize network bots. This study redefines virtual robots in Chinese social media (DABot) using deep learning. Researchers used 30 metadata-based, interaction, material, and choreographic factors to distinguish botnets from humans. This article proposes nine new skills. Additionally, education grows labeled data efficiently. Using a communicate over a network (Rnn), a bi rectified linear unit (BiGRU), and an ann model, RGA is a unique deep learning model for social bot detection. Data show the DABot beats government benchmarks with 0.9887 accuracy.

4. Y. Zhang, J. Li, L. Jiao, and X. Hu. BotFlowMon is a having to learn, content-independent tool for identifying network robot driving patterns. The IEEE Symposium on Telecommunication and Computer Security (CNS) will be held on June 10th, 2019. (pp. 169-177). IEEE.

stream of bots Other data forms, such as sflow, will be added to Mon. More characteristics are being investigated in order to increase the accuracy of detecting virtual bot traffic. flow of bots Numerous new different algorithms are used by Mon devices, including an aggregation technique that extracts money transfer data sources from gross flow documents, an image fusion valsalva maneuver 6 that needs to be extracted from remittance data sets, and a saturation pattern discovery that splits money transfer datasets into different attacks. With 92.33-93.61, it can efficiently categorise information from social bots, chatting bots, amplified bots, post bots, crawlers automation tools, and mix virtual agents.

5. Prunus Shi, Officinalis Zhang, and Yadav Hoo. Using real - time sequences to detect harmful social bots. 2019 Feb 26;7:28855-62 in Open Access.

Bots have had an impact on a variety of social media platforms. Instagram has been hit particularly hard, with bots accounted for a sizable amount of its user base. Those bots were used for nefarious purposes including

distributing fake information about politicians and increasing celebrities' apparent popularity. These bots have the ability to alter the outcomes of standard social media analysis. Hazardous social chatbots are even used to spread misleading info (e.g., fake news), which can have real-world ramifications. As a result, it's critical to identify and remove dangerous virtual bots from online communities. This research presents a unique technique for detecting harmful social bots that includes feature judgement based here on transition process likelihood of web usage sequences as well as moderately clustering. This technique incorporates the temporal characteristic of behaviour as well as the changing and developing of user behaviour touch creeks. In compared to the detection method quantitative analysis of user behaviour, observations from our studies on real shared on social portals show that the classification performance for unique types of malicious social bots by the screening test focusing on conditional probability distribution of user behaviour click vod raises by an overall mean of 12.8 percent.

6. Prof. Thakur. New profile identification of social media. The Conclave on Computing, Telecommunication, and Robotics (ICCCA) was hosted on May 5th, 2017. (pp. 175- 179). IEEE.

Use the most up-to-date income redistribution approaches as well. It has been claimed that efforts were made to affect the popularity of a figure or a commodity in the potential customers. Better effectiveness of false positives and false negatives need a powerful scheduling scheme and knowledge identification approach. There are a variety of approaches for detecting phoney personas and associated online social bots. An examination of social networking websites from a multiagent approach. In the design and testing of profiles, computational approaches were applied. Various strategies are discussed for detecting fraudulent profiles and associated virtual networking bot. Networking sites from a tri standpoint have also been studied. It also goes through the techniques that will be used to create and analyse profiles.

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system. Organized in a way that supports reasoning about the structures and behaviors of the system.

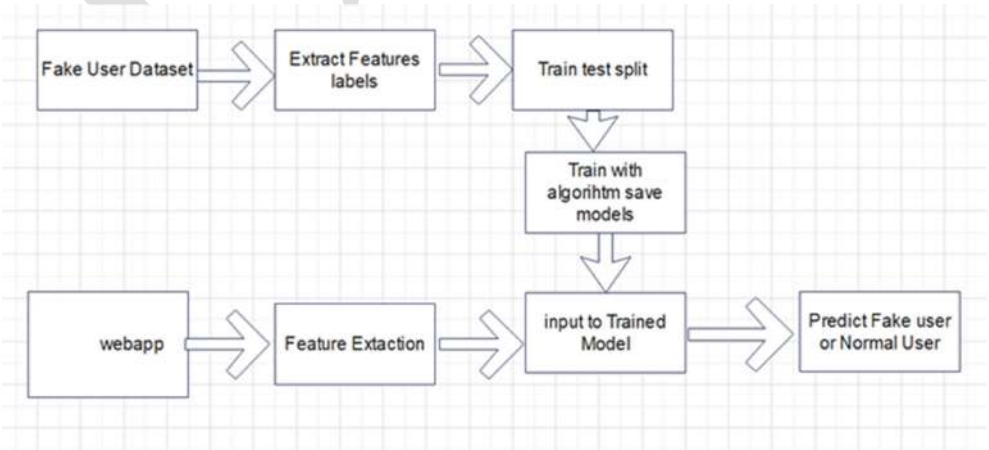


Figure 1 System Architecture

3-Tier Architecture:

The three-tier software architecture (a three-layer architecture) emerged in the 1990s to overcome the limitations of the two-tier architecture. The third tier (middle tier server) is between the user interface (client) and the data management (server) components. This middle tier provides process management where business logic and rules are executed and can accommodate hundreds of users (as compared to only 100 users with the two tier architecture) by providing functions such as queuing, application execution, and database staging.

The three tier architecture is used when an effective distributed client/server design is needed that provides (when compared to the two tier) increased performance, flexibility, maintainability, reusability, and scalability, while hiding the complexity of distributed processing from the user. These characteristics have made three layer architectures a popular choice for Internet applications and net-centric information systems.

CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

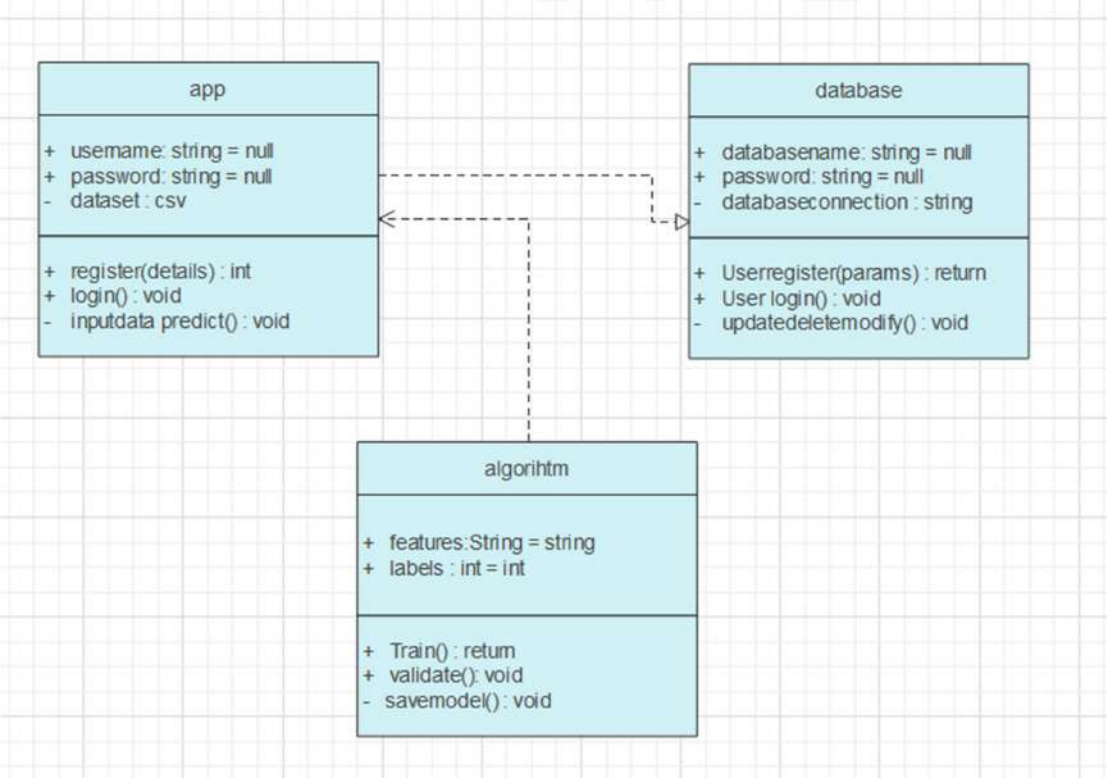


Figure 2 Class Diagram

implementation

To conduct studies and analyses of an operational and technological nature, and To promote the exchange and development of methods and tools for operational analysis as applied to defense problems.

INPUT & OUTPUT REPRESENTATION

Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

Objectives

Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

a. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
b. Select methods for presenting information.
c. Create document, report, or other formats that contain information produced by the system.

TESTING

The main objective of testing is to uncover a host of errors, systematically and with minimum effort and time. Stating formally, we can say, testing is a process of executing a program with intent of finding an error.

1 A successful test is one that uncovers an as yet undiscovered error.
2 A good test case is one that has probability of finding an error, if it exists.
3 The test is inadequate to detect possibly present errors.
4 The software more or less confirms to the quality and reliable standards.

LEVELS OF TESTING

Code testing:

This examines the logic of the program. For example, the logic for updating various sample data and with the sample files and directories were tested and verified.

Specification Testing:

Executing this specification starting what the program should do and how it should performed under various conditions. Test cases for various situation and combination of conditions in all the modules are tested.

Unit testing:

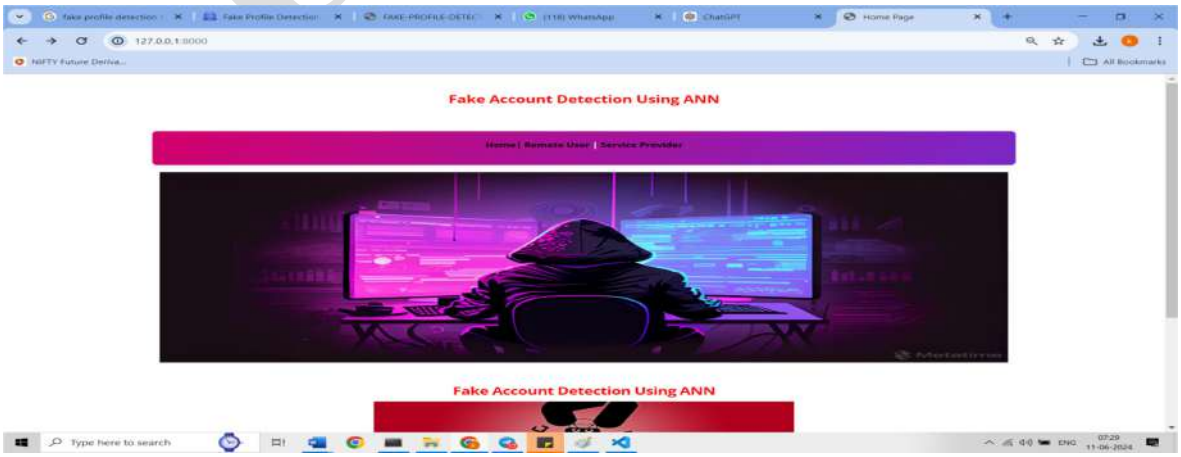
In the unit testing we test each module individually and integrate with the overall system. Unit testing focuses verification efforts on the smallest unit of software design in the module. This is also known as module testing. The module of the system is tested separately. This testing is carried out during programming stage itself. In the testing step each module is found to work satisfactorily as regard to expected output from the module. There are some validation checks for fields also. For example the validation check is done for varying the user input given by the user which validity of the data entered. It is very easy to find error debut the system.

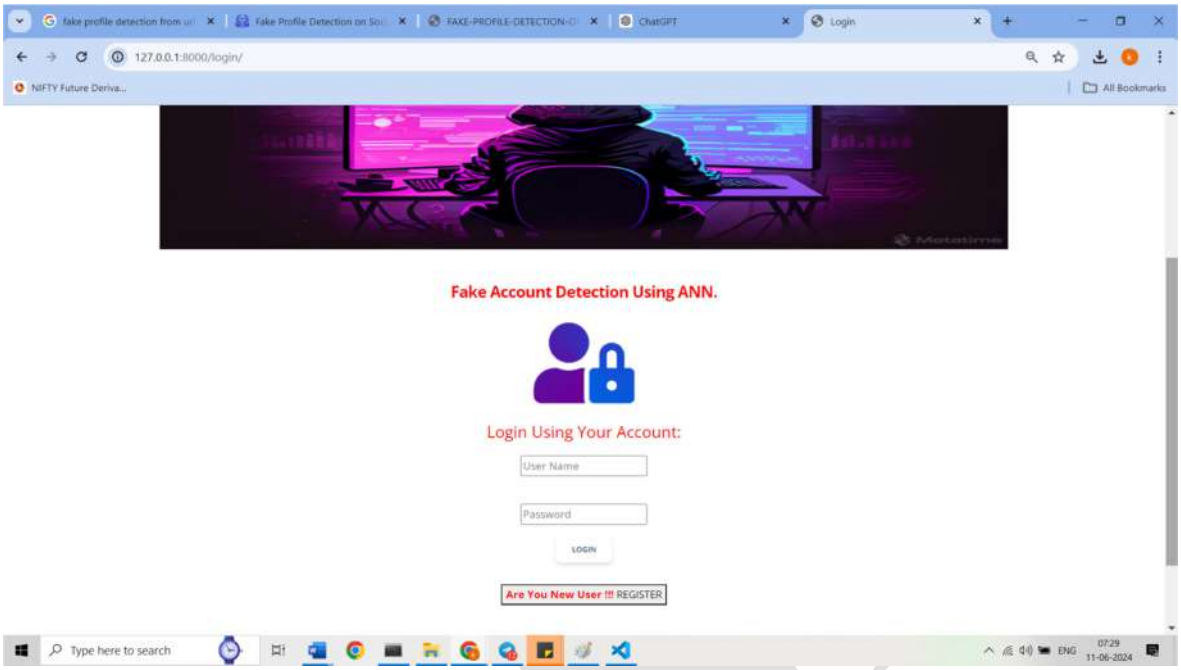
Each Module can be tested using the following two Strategies:

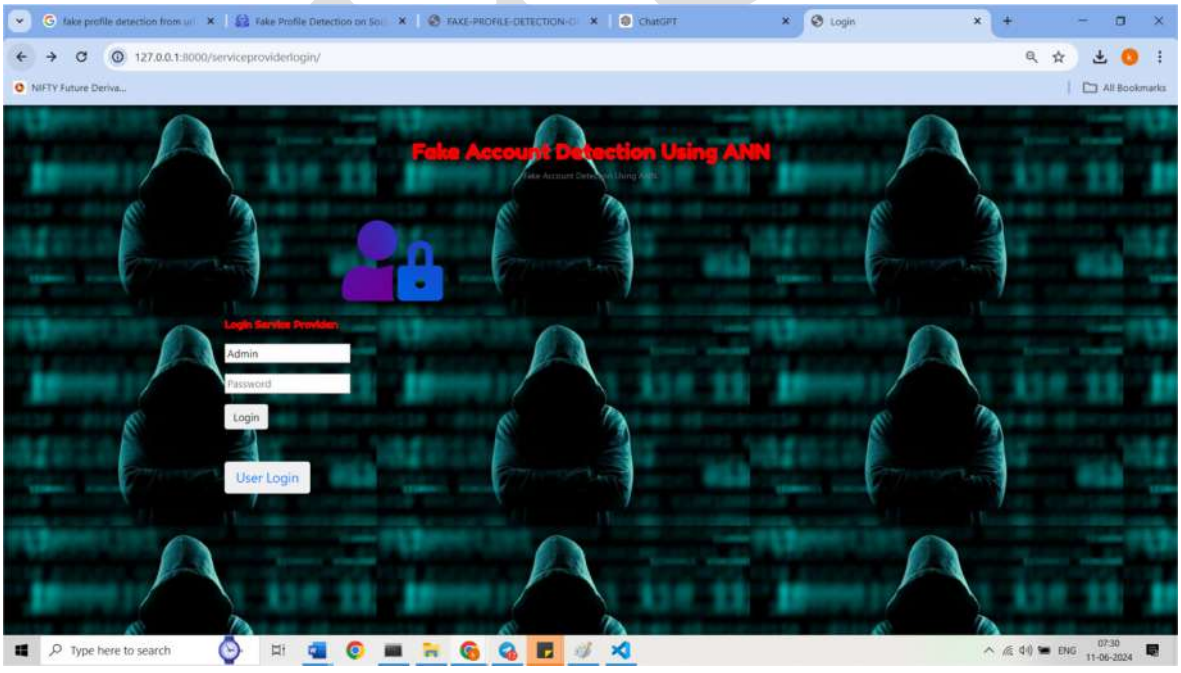
1 Black Box Testing
2 White Box Testing

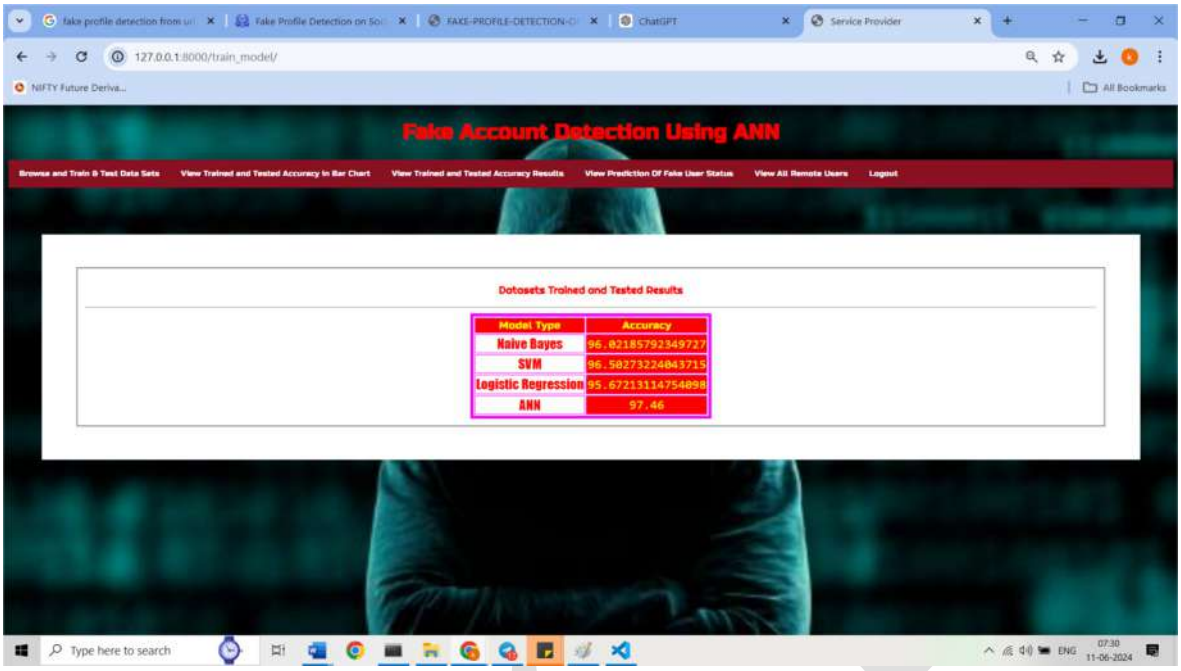
RESULTS

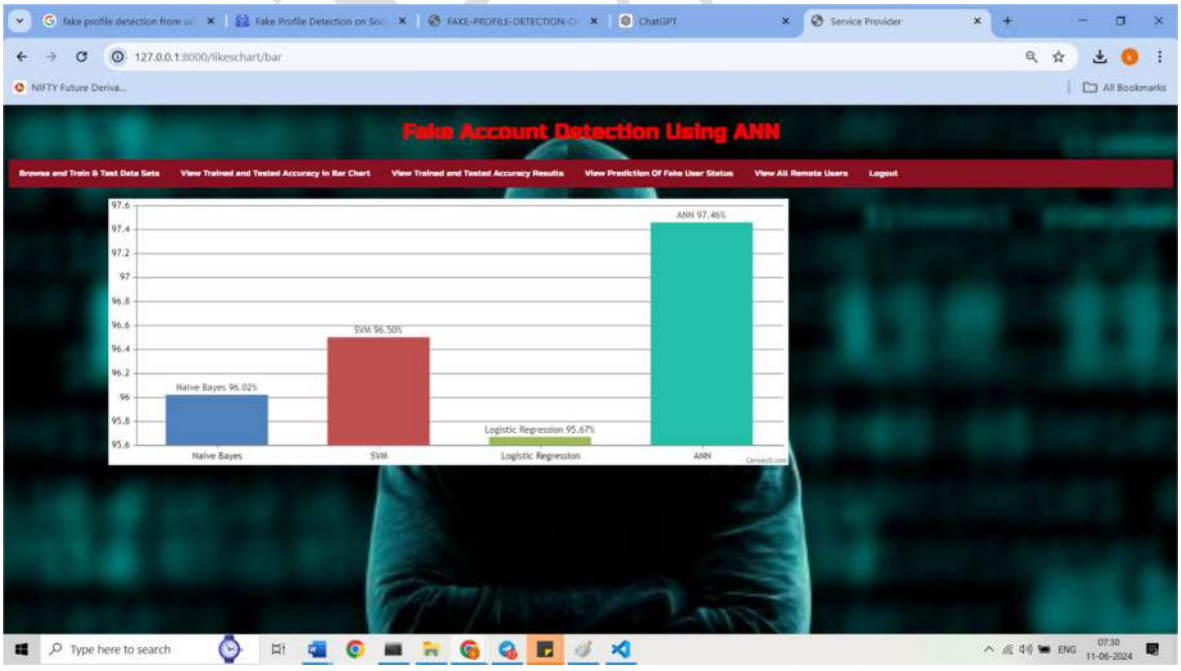
MAIN PAGE

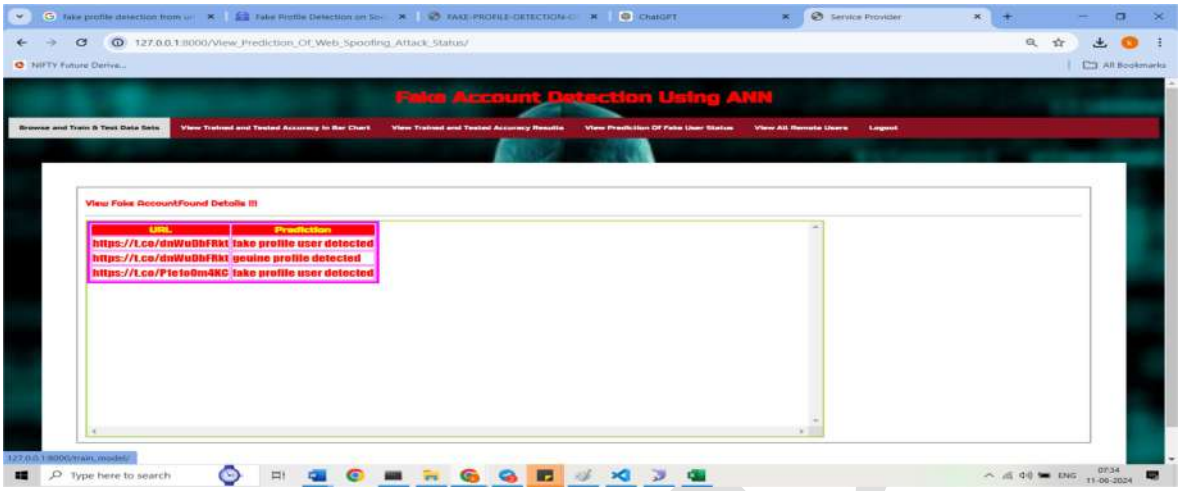



127.0.0.1:8000/login/
Fake Account Detection Using ANN.
Login Using Your Account:
User Name
Password
LOGIN
Are You New User !!! REGISTER
Type here to search


127.0.0.1:8000/serviceproviderlogin/
Fake Account Detection Using ANN
Login Service Provider
Admin
Password
Login
User Login
Type here to search


127.0.0.1:8000/train_model/
Fake Account Detection Using ANN
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fake User Status
View All Remote Users
Logout
Datasets Trained and Tested Results
Model Type
Accuracy
Naive Bayes
96.02185792349727
SVM
96.58273224043715
Logistic Regression
95.67213114754098
ANN
97.46


127.0.0.1:8000/likeschart/bar
Fake Account Detection Using ANN
Browse and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Fake User Status
View All Remote Users
Logout
ANN 97.46%
SVM 96.58%
Naive Bayes 96.02%
Logistic Regression 95.67%
Naive Bayes
SVM
Logistic Regression
ANN



CONCLUSION

In conclusion, the project "Instagram Fake Account Detection using Machine Learning" presents a comprehensive and effective solution for addressing the challenge of differentiating between genuine and fake Instagram accounts. Developed using Python and employing two powerful machine learning models, the Random Forest Classifier and the Decision Tree Classifier, this system has demonstrated a high level of accuracy and reliability in its performance. The system operates on a dataset comprising 576 records, each enriched with 12 distinct features that capture various aspects of Instagram profiles, such as the presence of profile pictures, the structure of usernames and full names, bio length, external URLs, and more. These features, in combination with robust feature engineering, enable the system to provide accurate and consistent fake account identification. Advancements in interpretability, adaptability to emerging threats, content analysis, and privacy considerations further contribute to the system's efficacy and user trust. Algorithm diversity, with the use of multiple classifiers, ensures a more comprehensive evaluation of Instagram profiles. With a 93% test accuracy for the Random Forest Classifier and a 92% test accuracy for the Decision Tree Classifier, the proposed system exhibits a strong ability to generalize and minimize false positives and false negatives. These attributes are essential for maintaining the integrity and security of the Instagram platform. The project, therefore, not only builds upon the strengths of the existing system but also addresses its limitations. It offers a well-rounded solution that aims to enhance.

REFERENCES

1. Bhadra Rrb, Yin yang symbol Pg, Somayajulu Hd, Resort RR, Rattan RR, Resort RR, Riddle RR, Trounce RR, Identification of socially destructive robots in the Form of tweets using learning automaton and ip characteristics. Industrial Electronics on Algorithmic Social Processes, vol. 7, no. 4, pp. 1004-18, May 14, 2020.
2. B. Zhang, Officinalis Huang, Y. Xiao, K. Cheng, and X. Zhang. Detecting sociable hackers in Facebook with improved conditioned fcn. IEEE Accessibility, vol. 8, no. 2, 2020, pp. 36664-80.

3. Al Pelgrum, R. Sharma, and A. B. S. R. Performing the actions Networking robots and prominent members in online communities are detected using an adjustable shallow Camille system. 2018 Nov;49(11):3947-64.

4. 4. Y. Zhang, J. Li, L. Jiao, and X. Hu. BotFlowMon is a having to learn, content-independent tool for identifying network robot driving patterns. The IEEE Symposium on Telecommunication and Computer Security (CNS) will be held on June 10th, 2019. (pp. 169-177). IEEE.
5. Prunus Shi, Officinalis Zhang, and Yadav Hoo. Using real - time sequences to detect harmful social bots. 2019 Feb 26;7:28855-62 in Open Access.
6. 6. Prof. Thakur. New profile identification of social media. The Conclave on Computing, Telecommunication, and Robotics (ICCCA) was hosted on May 5th, 2017. (pp. 175- 179). IEEE.
7. Phanich, M., Pholkul, P., & Phimoltares, S., "Food recommendation system using clustering analysis for diabetic patients," in Proc. of International Conference on Information Science and Applications, pp. 1-8, IEEE, April 2010. Article .
8. Ge, M., Elahi, M., Fernaández-Tobías, I., Ricci, F., & Massimo, D., "Using tags and latent factors in a food recommender system," in Proc. of the 5th International Conference on Digital Health, pp. 105-112, ACM., May 2015.
9. Freyne, J., & Berkovsky, S., "Evaluating recommender systems for supportive technologies," User Modeling and Adaptation for Daily Routines, pp. 195-217, Springer London, 2013.
10. Prof. Prajkta Khaire, Rishikesh Suvarna, Ashraf Chaudhary, "Virtual Dietitian: An Android based Application to Provide Diet", International Research Journal of Engineering and Technology (IRJET),Volume: 07 Issue: 01 | Jan 2020
11. Shivani Singh, Sonal Bait, Jayashree Rathod, Prof. Nileema Pathak," Diabetes Prediction Using Random Forest Classifier And Intelligent Dietician " , International Research Journal of Engineering and Technology (IRJET), Volume: 07 Issue: 01 | Jan 2020
12. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023
13. Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*", Journal of Sensor, Volume2023.
14. Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*", Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).
15. Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*", Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)
16. Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies", Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022
17. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526

18. Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021
19. M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*", in 3rd International Conference ICCIDM, Springer - 978- 981-10-3874-7_3 Dec (2016)
20. Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017
21. Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022
22. Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7
23. Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.
24. Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.
25. Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10
26. Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.
27. Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.
28. Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017
29. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;
30. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
31. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021

32. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
33. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
34. .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011
35. Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253
36. Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)
37. Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)
38. Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486
39. Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016
40. Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)
41. Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)