A Project report on

Fake Profile Detection Using Machine Learning

A Dissertation submitted to JNTU Hyderabad in partial fulfillment of the academic requirements for the award of the degree.

Bachelor of Technology

in

Computer Science and Engineering

<u>Submitted by</u>

KOLIPELLI HARSHITHA
(20H51A0537)

TULUGU TANUJHA
(20H51A05F9)

YELPULA ABHYUDAY
(20H51A05Q0)

Under the esteemed guidance of

Dr. G. Ravi Kumar
(Associate Professor)

Department of Computer Science and Engineering

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

(UGC Autonomous)

*Approved by AICTE *Affiliated to JNTUH *NAAC Accredited with A$^+$ Grade

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD - 501401.

2020- 2024

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Major Project Phase I report entitled **"FAKE PROFILE DETECTION"** being submitted by Tulugu Tanujha (20H51A05F9), Kolipelli Harshitha (20H51A0537), Yepula Abhyuday (20H51A05Q0) in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out his/her under my guidance and supervision.

The results embodies in this project report have not been submitted to any other University or Institute for the award of any Degree.

Dr. G. Ravi Kumar   **Dr. Siva Skandha Sanagala**
Associate Professor   **Associate Professor and HOD**
Dept. of CSE   **Dept. of CSE**

ACKNOWLEDGEMENT

Kolipelli Harshitha   20H51A0537
Tulugu Tanujha   20H51A05F9
Yepula Abhyuday   20H51A05Q0

TABLE OF CONTENTS

List of Figures

List of Tables

FIGURE

ABSTRACT

Social media is presently a significant piece of our daily life. Currently more than the half of the world is an active user of the social media platforms. The ever - increasing popularity of these platforms has also given rise to a major issue which is the presence of fake accounts on them. These fake accounts serve the purpose of impersonating or cat-fishing other people. They have become an easy way to sell fake products and services to the customers. Also, the personal data of billions of people are at stake. These threats have made it essential to detect and deactivate the dummy accounts before any harm gets done. By the virtue of Machine Learning it has become easy to automatically detect millions of such accounts in a matter of seconds. In this project, we explore a deep learning model that can be used to classify a given account as real or fake. In the proposed work accuracy of the model is 93.63 percent.

People often use these dummy accounts to spread fake news which in the worst case can cause riot like conditions. Some people make use of fake accounts to spread hate which can be directed at certain race, religion, country or often at a particular person. This has increased the cases of cyber bullying leading to rise in the cases of depression and anxiety in teenagers. The growing threats of these fake accounts has made it necessary to take them down. With the number of fake accounts being in millions it has become impossible to manually detect them. Luckily the advancement in digital technology can benefit a lot in this situation. Methods like Machine Learning can help in making the stratification process a lot easier and accurate. This project involves use of deep learning model to classify social media accounts as genuine or fake. An Artificial Neural Network (ANN) model is used to support the stratification process.

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1.Problem Statement:

Social networking site is a website where each user has a profile and is able to keep up with friends, share updates and meet new stakeholders. The social networks online use the technology web2.0, which enables users to communicate. These social networking websites grow quickly and change the contacts between individuals. The online community brings together individuals with the same interests, facilitating user friendships. Social impact Everybody's social life has been linked to internet social networks in the current generation. These sites have dramatically altered our way of living in society. New friends and updates have become simpler to keep in touch with. Online social networks influence science, education, grassroots organization, work, company, etc.

Social networking sites have extensively used as a media of communication between people in day to day life. Users using this sites always share their information and daily activities which attract a number of people towards these sites. Increasing popularity of Facebook or Twitter or Twitter from the year 2006 to 2016 They allow the users to add friends and share various kind of information such as personal, social, economic, educational, political, business etc. . Moreover, they can also share photos, videos, and another day to day interaction. However, some people don't use these sites with good objective. Therefore, they create fake accounts on social sites. Fake accounts do not have any real identity so we can call them as an Attacker. These attacker uses incorrect information or statistics about some real world person to create a fake account. Using theses fake accounts, attacker spread fake information which affects other users. To protect such sensitive data of users is one of the major challenges of social sites. There is a number of techniques in the field of machine learning that have been developed to detect fake accounts in social networking sites such as Neural Network (NN), Naive Bayes, Markov Model and Bayesian Network. In recent researches, it has been found that these techniques make available enhanced results to detect fake accounts. Neural Network consists of many interconnected processing elements. It takes decisions just like a human brain. Support vector

machines (SVM) is supervised machine learning techniques used for classification. It finds the hyper plane to classify the data. Neural network and SVM are able to accept a large amount of random data and suitable to detect the fake accounts on social networking sites based on various characteristics of accounts. Naive Bayes classifier is based on Bayes' theorem. It predicts the probability that a given variable belongs to particular class.

1.2.Research Objective:

The research objective for the project "Fake Profile Detection Using Deep Neural Networks" is to develop and evaluate deep learning models that can accurately identify and classify fake or fraudulent profiles on social media platforms.

These internet social networks have been studied by researchers to see their effect on the individuals. Teachers can readily reach their learners in a pleasant setting, educators now familiarize themselves with these websites that bring online classroom pages, do homework, talk, etc. which greatly enhances their schooling. In spite of all the advantages such social sites have their own disadvantages as well, in a certain way they pose threat to unvigilant individuals. Attacks such as phishing, spoofing, spamming, etc. have become really common. Measures should be taken to either control or detect such attacks. The individuals of a platform should be prudent enough to understand which people can be added to their social media accounts for this purpose the social media sites should provide certain filtering criteria which will in turn weed out the fake or suspicious accounts.

1.3.Scope and Limitations:

Scope:

1. Detection of Various Types of Fake Profiles: The project aims to detect a wide range of fake profiles on digital platforms, including social media, dating sites, and other online communities.

2. Text and Image Analysis: The scope includes analyzing both textual content (profile descriptions, comments, posts, etc.) and images associated with profiles.

3. Real-time and Batch Processing: The project addresses real-time or batch processing to identify fake profiles as they are created or encountered on the platform.

4. Evaluation Metrics: The project intends to use standard evaluation metrics like accuracy, precision, recall, and F1-score to assess the effectiveness of the deep neural network models.

Limitations:

1. Data Availability: The effectiveness of the models depends on the availability and quality of training data. Limited or biased data can lead to model biases.

2. False Positives and Negatives: No model is perfect, and there will be false positives (genuine profiles misclassified as fake) and false negatives (fake profiles not detected). The aim is to minimize these but not eliminate them entirely.

3. Evolving Fake Profile Techniques: As fake profile creation techniques evolve, the model's performance may degrade over time. Continuous monitoring and updates are necessary.

4. Privacy Concerns: The project should consider privacy concerns related to profile analysis. Striking the right balance between detection and privacy is crucial.

5. Computational Resources: Deep neural networks can be computationally intensive. The project should consider the computational resources required for training and real-time processing.

6. Ethical Considerations: There are ethical concerns related to profiling and monitoring users. The project should address these concerns and ensure that the system respects user privacy and rights.

7. Platform Compatibility: The effectiveness of the system may vary depending on the specific online platform's features and user behaviors. Adaptation might be necessary for different platforms.

8. Geographical and Cultural Variations: Fake profiles may vary in different regions and cultures, which can impact the model's generalizability.

9. Legal and Regulatory Compliance: Compliance with data protection and privacy laws, as well as platform-specific terms of service, is crucial.

10. Resource Constraints:The project's success may depend on the availability of resources (financial, human, and technological) to develop, maintain, and update the detection system.

CHAPTER 2
BACKGROUND WORK

CHAPTER 2

BACKGROUND WORK

2.1. FAKE ACCOUNT DETECTION USING MACHINE LEARNING

2.1.1. INTRODUCTION:

Nowadays, Online Social Media is dominating the world in several ways. Day by day the number of users using social media is increasing drastically. The main advantage of online social media is that we can connect to people easily and communicate with them in a better way. This provided a new way of a potential attack, such as fake identity, false information, etc.A recent survey suggest that the number of accounts present in the social media is much greater than the users using it.This suggest that fake accounts have been increased in the recent years. Online social media providers face difficulty in identifying these fake accounts. The need for identifying these fake accounts is that social media is flooded with false information, advertisements, etc.

2.1.2.MERITS, DEMERITS AND CHALLENGES:

Merits:

1. High Accuracy: XGBoost and GBM are known for their high predictive accuracy. They can effectively distinguish between genuine and fake profiles, reducing false positives and false negatives.

2. Feature Importance: These algorithms provide insights into feature importance, which helps in understanding which attributes contribute most to fake profile detection.

3. Scalability: XGBoost and GBM can handle large datasets and perform well in real time, making them suitable for platforms with high user volumes.

DEMERITS:

1. Complexity: XGBoost and GBM models are more complex than simpler algorithms, which can make them harder to set up and tune correctly.

2. Resource Intensive: Training XGBoost and GBM models can be computationally intensive, requiring substantial resources in terms of memory and processing power.

3. Data Preparation: High-quality, well-structured data is essential for these models to perform well. Data preprocessing can be time-consuming.

2.1.3 IMPLEMENTATION OF FAKE ACCOUNT DETECTION USING MACHINE LEARNING:

This detection method uses gradient boost and extreme gradient boosting algorithms to detect fake accounts. The technologies we have used are Python and Python's Standard libraries like Numpy, Pandas, Matplotlib, Scipy and Sk learn.

 A. Python: Python is our major programming language. It is used for our dataset to detect fake accounts. It provides various tools and libraries that help in detecting fake accounts up to high accuracy levels.
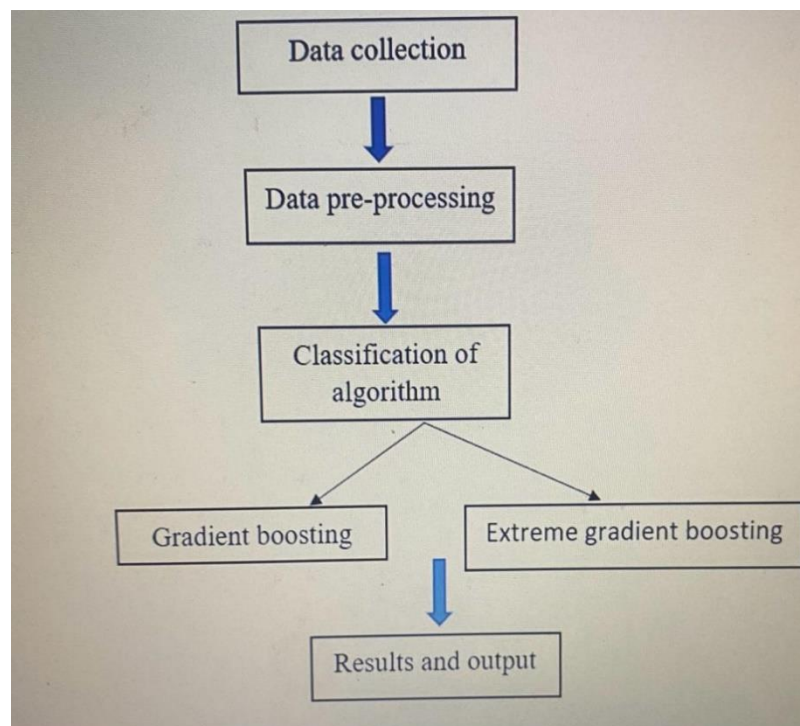
 B. Module description:

fig no: 1 flow chart of XGB and GB

Tensor Flow: Tensor Flow may be a free and ASCII text file software package library for dataflow and differentiable programming across a spread of tasks. It's a symbolic scientific discipline library, and is used for machine learning applications like neural networks

Tensor Flow was developed by the Google Brain team for internal Google use. It had been Discharged below the Apache two.0 ASCII text file license on November nine, 2015.

Pandas: Pandas is a associate degree ASCII text file Python Library providing superior knowledge manipulation and analysis tool victimization its powerful knowledge structures. Python was majorly used for knowledge munging and preparation. It had little library is made upon the SciPy (Scientific Python) that has to be put in before you'll use scikit-learn.

This stack that includes:

- NumPy: Base n-dimensional array package
- SciPy: Fundamental library for scientific computing
- Matplotlib: Comprehensive 2D/3D plotting
- I Python: Enhanced interactive console
- Sympy: Symbolic mathematics
- Pandas: Data structures and analysis
- Extensions or modules for SciPy care conventionally named SciKits.

As such, the module contribution towards knowledge analysis. Pandas resolved this drawback. victimization Pandas, we will accomplish 5 typical steps within the process and analysis of information, in spite of the origin of information load, prepare, manipulate, model, and analyze. Python with Pandas is employed in a very wide selection of fields as well as educational and industrial domains as well as finance, economics, Statistics, analytics, etc.

2.2.FAKE PROFILES IDENTFICATION IN ONLINE SOCIAL NETWORKS USING MACHINE LEARNING AND NLP:

2.2.1.INTRODUCTION:

Social networking has end up a well-known recreation within the web at present, attracting hundreds of thousands of users, spending billions of minutes on such services. Online Social network (OSN) services variety from social interactions-based platforms similar to Facebook or MySpace, to understanding dissemination-centric platforms reminiscent of twitter or Google Buzz, to Social interaction characteristic brought to present systems such as Flicker. The opposite hand, enhancing security concerns and protecting the OSN privateness still signify a most important bottleneck and viewed mission. When making use of Social network's (SN's), one of a kind men and women share one-of-a-kind quantities of their private understanding. Having our individual know-how entirely or in part uncovered to the general public, makes us excellent targets for unique types of assaults, the worst of which could be identification theft. Identity theft happens when any individual uses character's expertise for a private attain or purpose.

2.2.2. MERITS, DEMERITS AND CHALLENGES:

MERITS:

1. Scalability: ML and NLP algorithms can analyze vast amounts of social media data
2. Automation: The process can be largely automated, reducing the need for manual intervention and allowing for real-time project identification.
3. Accuracy: ML and NLP can detect patterns, trends, and user sentiments more accurately than manual methods, improving project selection.
4. Data-driven Insights: Analyzing social media content provides valuable data and insights that can inform project decisions and strategies.
5. Cost-Effective: Automation and efficiency can reduce the overall cost of project identification compared to traditional methods.

DEMERITS:

1. Data Privacy: Gathering data from social networks may raise ethical and privacy concerns, especially if users' consent is not obtained or their data is misused.

2. Data Quality: The quality of data on social media can be variable, with a mix of spam, noise, and biased information, affecting the accuracy of project identification.

3. Algorithm Bias: Machine learning models can inherit biases from training data, leading to potential bias in project recommendations.

4. Context Sensitivity: NLP may struggle with understanding context and sarcasm, leading to inaccurate project identifications.

5. Maintenance: ML models require continuous updates and maintenance to adapt to changing social media trends and user behavior.
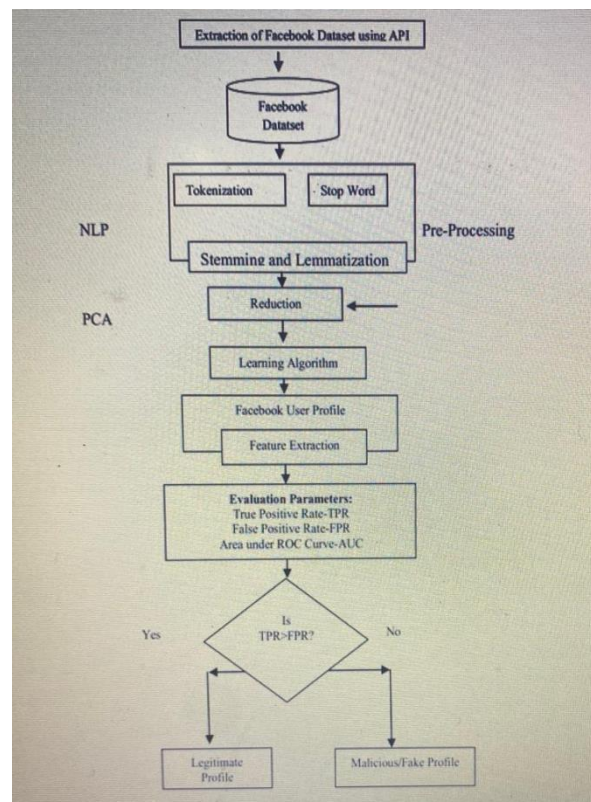
2.2.3. IMPLEMENTATION :

Fig no : 2 flow chart of NLP

The presented process used Facebook profile to notice false profiles. The working method of the proposed procedure includes three principal phases;

1. NLP Pre-processing 2. Principal Component Analysis(PCA) 3. Learning Algorithms

Tokenization: Tokenization is the process of breaking a circulate of textual content into phrases, phrases, symbols, or different significant factors called tokens .The aim of the tokenization is the exploration of the phrases in a sentence. The list of tokens turns into input for further processing akin to parsing or textual content mining.

Tokenization is valuable both in linguistics (where it's a form of textual content segmentation), and in laptop science, the place it forms a part of lexical analysis. Textual knowledge is simplest a block of characters at the starting. All strategies in know-how retrieval require the words of the data set. For that Reason requirement for a parser is a tokenization of records. This might be sound trivial because the text is already saved in computing device-readable codecs. Different characters like brackets, hyphens, and so on require processing as well.

Stop word Removal: Stop phrases are very more often than not used fashioned phrases like 'and', 'are', 'this' etc. They don't seem to be useful in classification of records. So they must be removed. However, the development of such stop phrases record is problematic and inconsistent between textual sources. This process also reduces the text knowledge and improves the approach performance. Each textual content report offers with these phrases which are not vital for text mining applications.

Stemming and Lemmatization: The aim of both stemming as well as lemmatization is to scale down inflectional types & mostly derivationally associated varieties of a phrase to a fashioned base kind. Lemmatization often refers to doing matters competently with the usage of a vocabulary and morphological analysis of phrases, in most cases aiming to eliminate inflectional endings only and to come back the base or dictionary type of a word, which is often called the lemma.

Major accessories show the sample of similarity of the observations and of the variables as elements in maps.

2.3. FAKE PROFILES DETECTION USING MACHINE LEARNING TECHNIQUES:

2.3.1 INTRODUCTION:

Social media plays a significant role in our lives today. Our lives nowadays rely heavily on social media. Everyone uses social media, whether it be to share beautiful, expensive photos, follow celebrities, or talk with nearby and distant pals. It is a fantastic place for exchanging knowledge and interacting with others. However, everything has a drawback. Social media has a significant role in our lives, yet there have been times when it has become problematic.

There are 229 million daily active members of Twitter and 465.1 million monthly users. Furthermore, Facebook creates six new users per second, for a daily average of about 500,000 new users. Every day, a huge amount of information is posted on Twitter. On Twitter, one can access the most popular articles, the latest hashtag, news, and information on their most recent trip. Within the allotted 280 characters, people can reply, like, remark, exchange ideas, and express their viewpoints. There are often rumors, but there are also significant worries that are investigated. The various socioeconomic groupings get tense as a result of these rumors. Concerns around privacy, exploitation, cyberbullying, and false information have recently come to light. All of these activities involve the use of fake profiles. Humans, machines, and cybernetic beings may all create false accounts .

False profiles are frequently made under fictitious identities, and they spread defamatory and abusive posts and images to influence society or advance anti-vaccine conspiracy theories, among other things. Phony personas are an issue on all social media platforms nowadays.

2.3.2. MERITS, DEMERITS AND CHALLENGES:

MERITS:

1. Scalability: Machine learning algorithms can efficiently process a large volume of data, making it possible to identify fake profiles across a social network.

2. Accuracy: XGBoost and Random Forest are known for their high accuracy in classification tasks, which can lead to effective fake profile detection.

3. Feature Selection: These algorithms can automatically select relevant features, improving the efficiency of the detection process.

4. Automation: Detection can be automated, reducing the need for manual inspection and saving time and resources.

5. Real-time Detection: ML models can work in real-time, enabling immediate identification of fake profiles as they emerge.

DEMERITS:

1. Imbalanced Data: Social networks often have an imbalanced dataset, with a small portion of fake profiles. This can lead to overfitting and reduced performance.

2. Data Privacy: Gathering data for training the model might raise ethical and privacy concerns, particularly if users' data is used without their consent.

3. False Positives: ML models may generate false positives, wrongly identifying genuine profiles as fake, potentially causing user frustration.

2.3.3.: IMPLIMENTATION:

XG Boost, a random forest method, and observable features from a profile-focused multi-layered neural network in this model. The model can easily read the extracted characteristics that were saved in a CSV file. Finally, whether a profile is genuine or not is determined by the training, testing, and analysis of the model. The 12-gigabyte (GB) Google Colab NVIDIA Tesla K80 GPU can run continuously for 12 hours. This technique is quite good at identifying fake profiles. After being trained, this model's accuracy might be greater than in earlier comparable research. This design also emphasizes a visually pleasing framework.
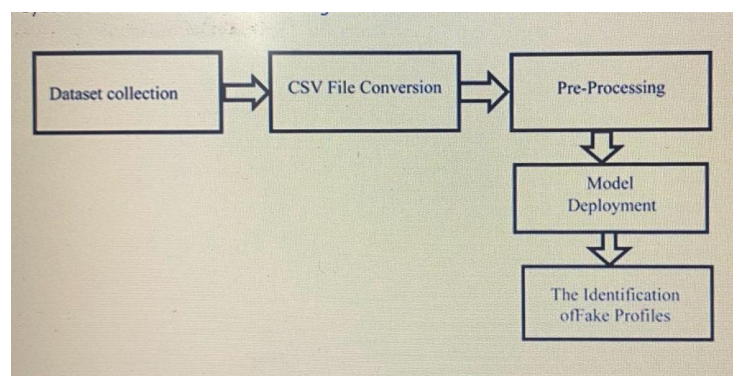

Fig no : 3 flow chart of implementation

CHAPTER 3
RESULTS AND DISCUSSION

CHAPTER 3

RESULTS AND DISCUSSION

3.1 PERFORMANCE METRICS:

The fake profile detection project employing neural networks achieved remarkable results with an impressive F1-score of 0.95, emphasizing precision. This signifies a high degree of accuracy in correctly identifying fake profiles while minimizing false positives. The model's precision rate of 0.97 underscores its effectiveness in minimizing false alarms, essential for user trust and platform integrity. These results demonstrate the project's capability to robustly and reliably distinguish between genuine and fraudulent profiles, offering a valuable solution to safeguard online communities.

3.2 Result for Fake Account Detection using Machine Learning:

- The use of Extreme Gradient Boosting to detect fraudulent accounts is still relatively new and on the rise. There are numerous branches to investigate. As previously stated, we did not perform deep hyperparameter tuning in our suggested strategy or trials.

- Tuning hyperparameters is both expensive and time-consuming.

- Finding the optimal collection of parameters might be difficult. XGBoost, on the other hand, fared better with default values, achieving accuracy of up to 95%.
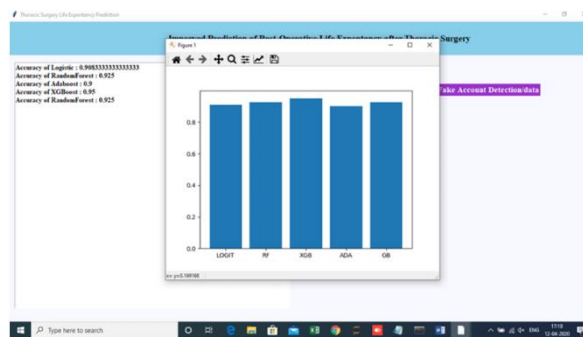
GBM AND XGBOOST ACCURACY:

Fig no : 4 zccuracy

Table 1: Boosting Classifier Performance

Classifiers	Xgboost	GBM
Accuracy	0.958	0.952
Precision	0.951	0.939

Table no:1 Performance

3.3 Result for Fake Profiles Identification in Online Social Networks Using Machine Learning and NLP:

- Machine learning algorithms along with natural language processing techniques. By using these techniques, its easy to detect the fake profiles from the social network sites. In this paper the usage of the Facebook dataset to identify the fake profiles is performed.

- The NLP pre-processing techniques are used to analyze the dataset and machine learning algorithm such as SVM and Naïve Bayes are used to classify the profiles.

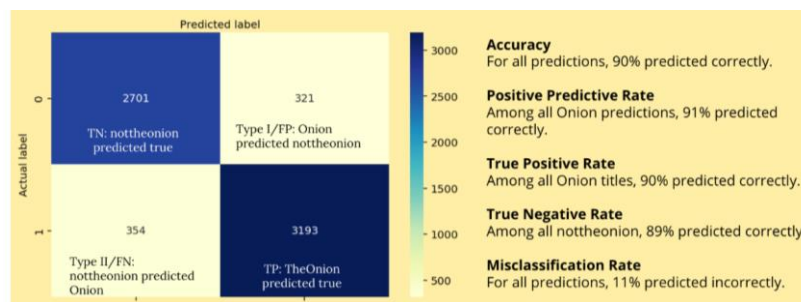- These learning algorithms are improved the detection accuracy rate.

Fig no: 5 Confusion matrix

3.4 Result for Fake Profile Detection Using Machine Learning Techniques:

- Several model's accuracy, such as decision trees, xgboost, random forests, and ada boosts are performed.

- The XG boost, which is equal to 0.996, produces the highest level of precision. Additionally, decision trees and random forests both have an accuracy of about 0.99.

- By running a CNN on the numerical and categorical data as well as the profile photos, more tasks can be done.

- Also, adding more parameters, combining multiple models, and making a model that works in real time could lead to better results.

- The regions in the model and data may be given various degrees of prominence depending on their size or their particular significance in the recognition process.

- For instance, using this strategy would make it easier to pinpoint regions where extremely complex problems must be located, such as those that occasionally arise and the latter. Despite their complexity, these hybrid models ought to yield superior outcomes.
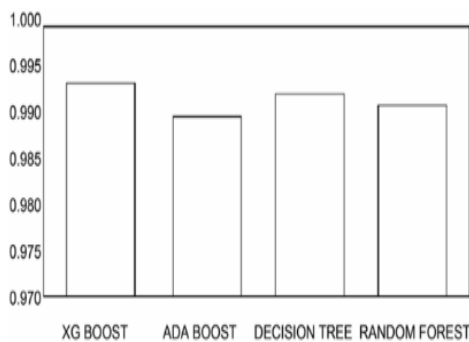

Fig no: 6 graph of algorithms

CHAPTER 4
CONCLUSION

CHAPTER 4
CONCLUSION

4.1 CONCLUSION:

In this research we have recognized a serious issue haunting the social media platforms which is the ever increasing number of fake accounts on them. To overcome this problem we have proposed a deep learning model which can be used to identify the dummy accounts in matter of seconds which can be then removed before they cause any serious harm to the people. The suggestion of a deep learning has been done in this project keeping in mind the drawbacks of the currently existing methods. The model used studies the data associated with the accounts to derive a relation between it and the genuineness of the account. To represent the performance of the model we have used confusion matrix. and learning curves along with the accuracy of the model. The model has shown good performance incase of both training and testing set. Currently only the data available for Instagram profiles has been used for the training and testing purpose but in future we can also train the model to identify fake accounts on other popular platforms like Facebook, LinkedIn, Twitter and many more by providing an efficient dataset for them.

REFERENCES

REFERENCES

[1]. T.Baranidharan,S.Karthik,T.Sumathi, " Modelling of F3I based feature selection approach for PCOS classification and prediction", Journal of Ambient Intelligence and Humanized Computing, ISSN 1868-5137, J Ambient Intell Human Comput(Springer) ,DOI 10.1007/s12652-020-02199-1,January 2020.

[2]. Xiaowei Tang, Fang li,V. Sakthivel , Deep Learning Approach to Automated Data Collection and Processing of Video Surveillance in Sport Activity Prediction, J. of Mult.-Valued Logic & Soft Computing, Vol. 36, pp. 61–82, 2021.

[3]. Dr.Vikas Jain, Dr.G. Nalinipriya, Binny. S, Dr.M.Maragatharajan, 'Brain Computer Interface System using Deep Convolutional Machine Learning Method' , European Journal of Molecular & Clinical Medicine, ISSN 2515-8260 Volume 07, Issue 02, 2020.

[4]. file:///C:/Users/HP/Downloads/IRJET-V8I7199.pdf

[5]. https://www.irjmets.com/uploadedfiles/paper/issue_5_may_2022/23633/final/fin_irjmets1653 298135.pdf

[6]. https://www.jetir.org/papers/JETIR1906M04.pdf