Detection of Fake Social Media Profiles Using Machine Learning Techniques

Dr. Nitalaksheswara Rao K[1], Dr. Uma Devi D[2],Dr. Sreekanth P[3], Dr. Soujanya D[4]

[1,3,4]Assistant Professor Department of Computer science and Engineering GST, GITAM University Visakhapatnam Andhra Pradesh , India.

[2]Associate Professor, Department of computer science and Engineering, Gayatri Vidya Parishad College of Engineering (Autonomous), Visakhapatnam, Andhra Pradesh, India

Mail- kolukulanitla@gmail.com[1],umadevi@gvpce.ac.in[2]srikanthpuli66@gmail.com[3]sduvvi3@gitam.edu[4]

Corresponding Author- Dr. Nitalaksheswara Rao K, kolukulanitla@gmail.com

ABSTRACT

Social media' sex plosive growth and the vast amounts of user-provided personal information have drawn attackers who steal data, spread fake news, and engage in other criminal activity. Some harmful accounts are employed to advance agendas and spread false information. An important step is the detection of malicious profiles. The system consists of a binary classifier which takes profile information as input and outputs whether the profile is genuine or fake. It uses the classification algorithms like SVM-NN, Light GBM and compares them to the existing system algorithms to give a final model with better results.

Keywords: *Social media, Fake profiles, Machine learning, Light GBM, SVM-NN*

1. INTRODUCTION

Over the past few years, online social networks (OSNs) including Facebook, Twitter, LinkedIn, and Google have grown in popularity. People use OSNs to interact with one other, share knowledge, organise events, and even run their own online companies. OSNs are vulnerable to Sybil attacks due to their open architecture and the vast amount of subscriber-provided personal information. In addition to publishing false news, hate speech, sensational, and polarising content, Facebook detected abusein 2012. Online social networks (OSNs)have drawn interest from researchers for other reasons as well, including data mining and analysis, user behavior analysis, and finding unusual behavior .

Approximately 14 million of Facebook's monthly active users, according to a 2015 estimate, are truly unwanted, reflecting malicious false identities that were made in violation of the website's terms of service. The report, which was initially made public in the first quarter of 2018, describes Facebook's internal rules for upholding community standards from October 2017 to March 2018. It displays the quantity of problematic information that was removed and covers six categories: graphic violence, adult crudeness and sexual activity, terrorist propaganda, hate speech, spam, and fraudulent accounts. Facebook has removed almost 81 million pieces of offensive content that breach other guidelines in addition to eliminating 837 million spam postings and 583 million fraudulent accounts. Despite efforts to prohibit millions of them from being established, it was estimated that 88 million Facebook profiles are still fraudulent.

Attackers use images and accounts that are either fabricated or illegally constructed in order to spread false information and obtain personal data about victims. They act in this manner because they think that OSN user accounts are "keys to walled gardens," which they may use to impersonate other people. These fictitious accounts are known as imposters. Because theyroutinelyinundatepeoplewithspamorstealtheirpersonalinformation,thesephoneyaccounts frequently harm users and neither time are they acting with good motives. They areready to seduce specific trusting customers into phoney ties that lead to sex frauds, human trafficking, and even political as troturfing .

Adrian Chen, a reporter for the New Yorker, noticed in December 2015 that many of the Russian accounts he was monitoring had switched to pro-Trump campaigns, but many of those accounts were more accurately described as troll accounts, which were operated by real people with the intention of imitating American social media users. Similar facts were claimed in Italy's online blogs and media in the months leading up to the general elections in February 2013 regarding a supposedly high number of phoney supporters of the major candidates. It has become crucial to identify those risky accounts in OSNs in order to stop various illegal actions, ensure account security for users ,and protect personal data.

In order to identify fake accounts, researchers analyse user level activity by extracting data from recent users, suchas the number of posts, followers, and profiles. They differentiate between real and fake accounts using trained machine learning techniques. A different approach models the OSN as a graph, which is really just a collection of nodes and edges. Every edge represents a relationship, and every node represents an entity (such an account) (e.g.friendship).OSN semploya range of mitigation strategies and detectional go rithms to address the rising problem of malicious accounts.

2. LITERATURESURVEY

To identify the false profiles on social media, numerous articles used various techniques, tools, and machine learning algorithms. The major goal of the below mentioned publications is to accurately and reliably identify malicious profiles. Therefore, in order to achieve better results, the most suitable tactics must be employed.

A.T.K abakus and R. Kara,“ A survey of spam detection methods on twitter”, International Journal of Advanced Computer Science and Applications, vol. 8, no. 3, pp.29–38,2017. in this paper authors clearly explains about various methods to detect spam messages on twitter social media platform and explains how these effect the local environment.

A.-Z. Ala’M, H. Faris et al., “Spam profile detection in social networks based on public features”, in Information and Communication Systems (ICICS),20178th International Conference on.IEEE,2017,pp.130–135. In this paper authors detailed describes and explains by using public features how the spam profiles are detected in social networks like twitter, Facebook etc.

R. Kaur and S. Singh, “A survey of data mining and social network analysis based a nomaly detection techniques,” Egyptian informatics journal, vol. 17, no. 2, pp. 199–216,2016. In this paper authors describes about various anomaly detection techniques in social network analysis using data mining

A.K.Ameen and B.Kaya,“ Detecting spammers in twitter network,” International Journal of Applied Mathematics,ElectronicsandComputers,vol.5,no.4,pp.71–75,2017. in this paper authors explained and experimented about spammers detection in twitter network by using different methods and techniques.

S. D. Jadhav and H. Channe, “Comparative study of K- NN, naive bayes and decision tree classification techniques,”International Journal of Science and Research,vol.5,no.1,2016. In this paper authors explained and described about various machine learning classification techniques to assess the performance of the algorithms.

3.SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing system follows the very popular traditional classification algorithms, namely Random Forest (RF), Support Vector Machine (SVM), Neural Networks(NN) etc., to identify the fake and genuine accounts on social media. Based on various evaluation indicators , the performance of these classifier sisassessed and compared.

3.2PROPOSED SYSTEM

The proposed system consists of a binary classifier (machine learning model) which takes profile information as input and outputs whether the profile is genuine or fake. This system uses classification algorithms like SVM-NN, Light GBM (Boosting method) and compares them to the existing system algorithms to give a final model with better results.

3.3 IMPLEMENTATION PLATFORM

• Processor	:IntelI5orAbove
• RAM	: 8GB(Min)
• Hard Disk	:128GB(Min)
• Input Devices	:Keyboard, Mouse
• Monitor	:Any

• Operating System	:Windows10orAbove
• Server-side Script	:HTML,CSS&JS
• IDE	: PyCharm
• Programming Language	:Python3.6orAbove
• Libraries	**:**Pandas,Numpy, Sklearn,etc.,

3.4 TECHNOLOGIESUSED:

NumPy:

A library for the Python programming language called Numpy adds support for big, multidimensional arrays and matrices as well asatonneo fhigh-level mathematical operations that can be performed on the searrays.Jim Holguin and a number of other programmers collaborated to produce Numeric, the predecessor of Numpy. Travis Oliphant developed Numpy in 2005 by heavily modifying Numeric to incorporate capabilities of the rival Numarray. Numerous people have contributed to NumPy, which his open-source software.

Pandas:

Panda is a data analysis and manipulation software package created in the Python programming language. It contains data structures and procedures specifically for working with time series and numerical tables. The three-clause BSD licence was used to release the free software. The name is derived from the econometrics phrase"panel data," which refers to data sets with both time-series and cross-sectional data.

Scikit-Learn:

David Cournapeau's Google Summer of Code projects cikits Learn served as the prototype for Scikit-learn. Its name refers to a separately created and widely distributed SciPy modification known as a "Scikit" (SciPy Toolkit). In November 2012, scikit-learn and scikit-image were among the scikits that were referred to as"well-maintained and popular."

OS:

The operating system can be interacted with using the python OS module's functions. The standard utility modules for Python in clude OS. Operating system-dependent functionality can be used portable thanks to the module. Numerous functions for interacting with the file system are included in the“os” and“os.path”modules.

Seaborn:

Python's Seaborn package allows for the graphical representation of statistical plotting.To make the production of various statistical charts in Python more visually appealing, Seaborn offers a variety of colour palettes and elegant default styles.

Matplotlib:

By employing Python scripts, 2 D graphs and plots can be produced using the Mat plotlib module. By offering features to adjust line styles, font attributes, formatting axes,etc.,its py plot module makes things simple for plotting. Histograms, bar charts, power spectra, error charts, etc. are just a few of the many graphs and plots it

4.SYSTEMDESIGN

4.1 UMLDIAGRAMS:

Unified Modeling Language is known as UML. Ageneral-purpose modelling language with standards, UML is used in the field of object-oriented software engineering. The Object Management Group oversees and developed the standard. The objective is for UML to establish it self as a standard language for modeling object-oriented computer programmes. UML now consists of a meta-model and a notation as its two main parts. In the future, UML might also be coupled with or added to in the form of a method or process. Unified Modeling Language is a standard language used for business modeling , non-software systems, and specifying, visualising, building, and documenting the arte facts of a software system. The UML is a collection of best engineering principles that have been successful in simulating big, complicated systems. UML is a crucial component of the software development process and the creation of objects-oriented software. The UML primarily employs graphical notations to explain the design of software projects.

GOALS:

The primary goals in the design of the UML areas follows:

1. Provide users with an expressive visual modeling language that is ready to use so they can create and trade meaningful models.
2. Provide mechanisms for specialization and extensibility to expand the fun damental ideas.
3. Beunreliant on specific development methodologies and programming languages.

4. Establish a formal framework for comprehending the modeling language.
5. Encourage the growth of the tools market.
6. Encourage the use of higher-level development concepts like components, frameworks, patterns, and collaborations.
7. Integrate best practices.

4.2 BLOCKDIAGRAM:

A block diagram illustrates how data is handled by a system in terms of inputs and outputs. Its concentration, as its name suggests, is on information flow, specifically where data comes from, where it flows, and how it is kept. The data flow diagram mostly used modeling. It's used to represent the system's many components. These components include the system's operation, the data it utilizes, an external entity that interacts with it, and the information that flows inside it. Block diagram may be applied to any level of abstraction to depict a system. Block diagram can be divided into levels, each of which reflects an in crease in information flow.

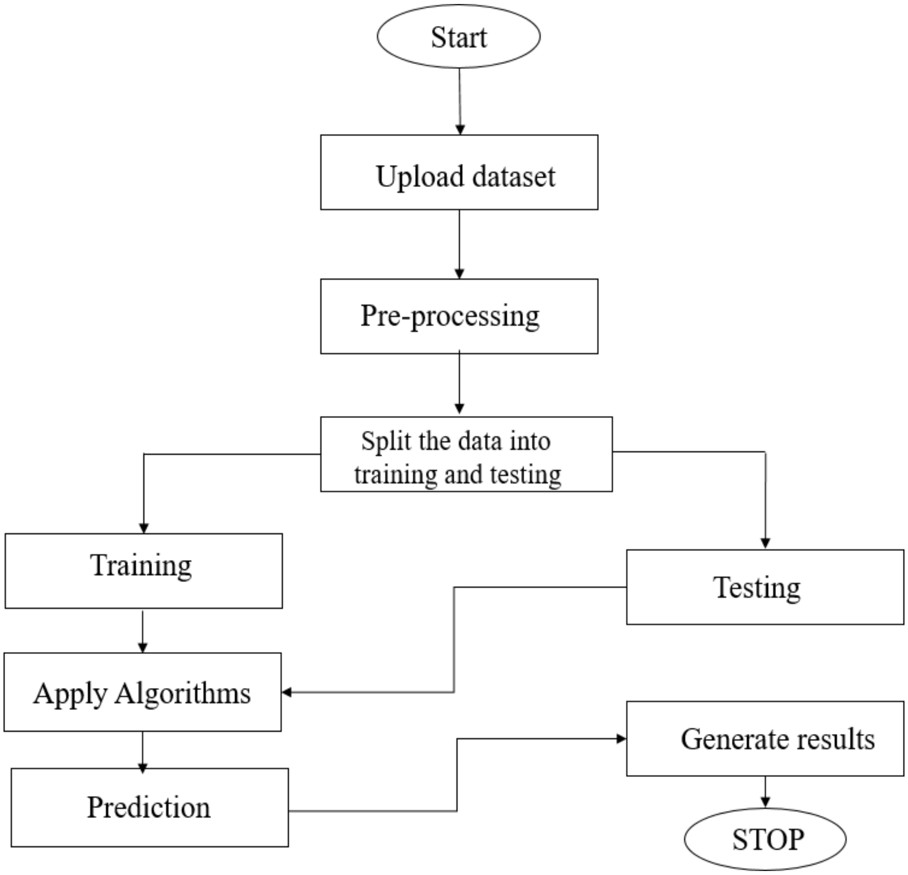


Fig.4.1 Data handled by the system

4.3 SVM-NN Algorithm:

In order to potentially increase classification accuracy, a novel methodology known as SVM-NN (Hybrid model) has been developed. This methodology employs SVM-trained model decision values to train a NN model and SVM-testing decision values to test the NN model. SVM-NN is a supervised and hybrid machine learning algorithm.

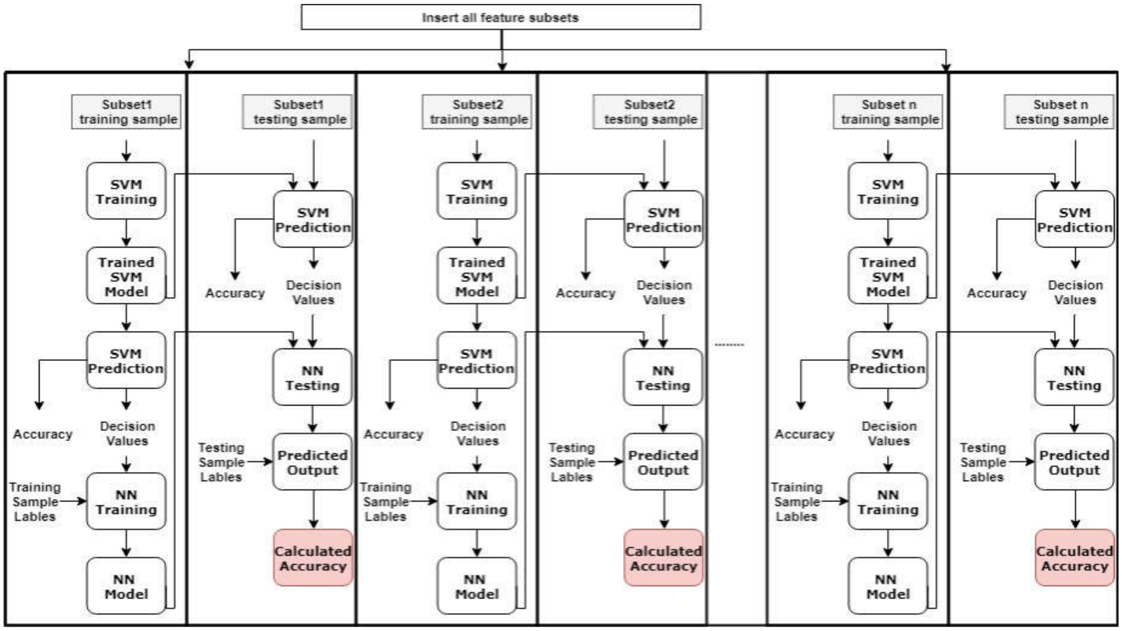


Fig. 4.2 SVM-NN Algorithm working model

SVM-NN Working Structure:

Steps involved in SVM-NN algorithm:

Step1: Using feature reduction techniques, identify the list of reduced features.

Step2: Arrange those best attributes in the data set.

Step3: Subsets of the S that include potential values for the best attribute should be created.

Step3: Split your data in to testing and training.

Step4: Set the training and testing identifying labels.

Step 5: SVM decision values were used to train a NN model, and SVM decision values were used to test the NN model. The hybrid classification algorithm will be implemented by applying the Neural Network classification algorithm to the decision values obtained from the SVM classification method.

4.4 Light GBM Algorithm:

Light GBM, or Light Gradient Boosting Machine, is a distributed gradient boosting system for machine learning that was first created by Microsoft. Light GBM is a gradient boosting framework based on decision trees that enhances model performance while consuming less memory..

In order to address the constraints of the histogram-based approach, which is largely employed in all GBDT (Gradient Boosting Decision Tree) frameworks, it employs two innovative techniques: gradient-based one side sampling and exclusive feature bundling (EFB). Together, they enable the model to function effectively and provide it an advantage over competing GBDT frameworks. Light GBM's "Light" name refers to its ability to perform calculations quickly. Also it takes less memory to run and is able to deal with large amounts of data.

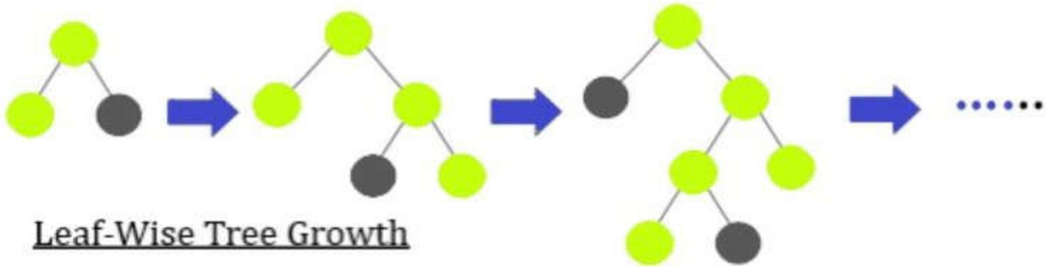


Fig. 4.3 Leaf- wise tree growth

Light GBM Working Structure:

Step1: Import all the relevant libraries.

Step2: Load the Data set for the training and testing purposes.

Step3: Separate the data in to independent and dependent variables.

Step4: Use python Sklearn functions to separate data in to training and testing data.

Step5: Prepare the data for Light GBM model.

Step6: Specify the required parameters and train the Light GBM model.

Step7: Then find predictions for test data which will stored in the target column

5. Outcome Analysis

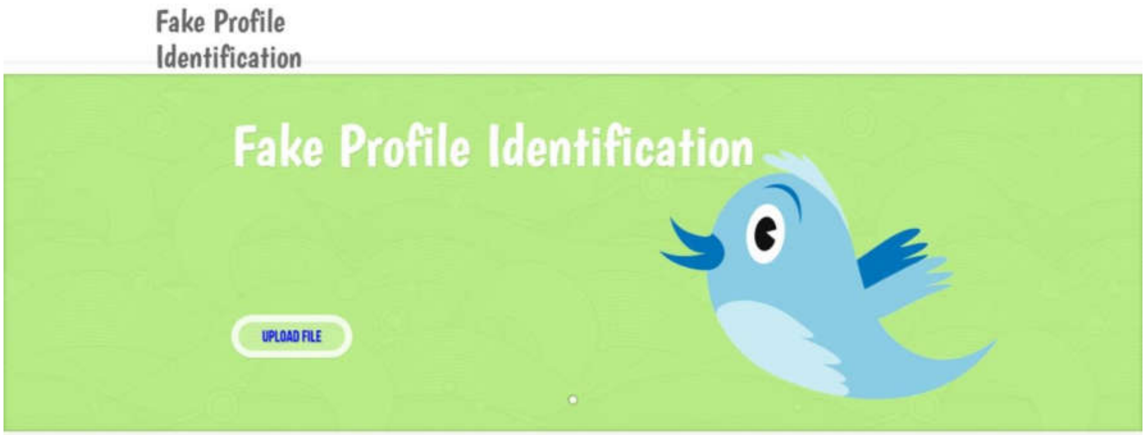


Fig5.1:It is the home page for the fake profile identification.

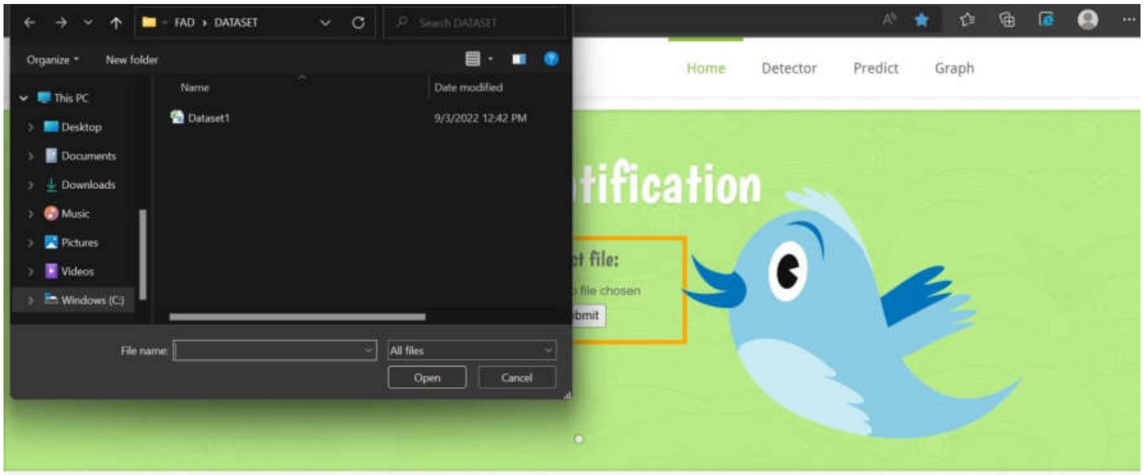
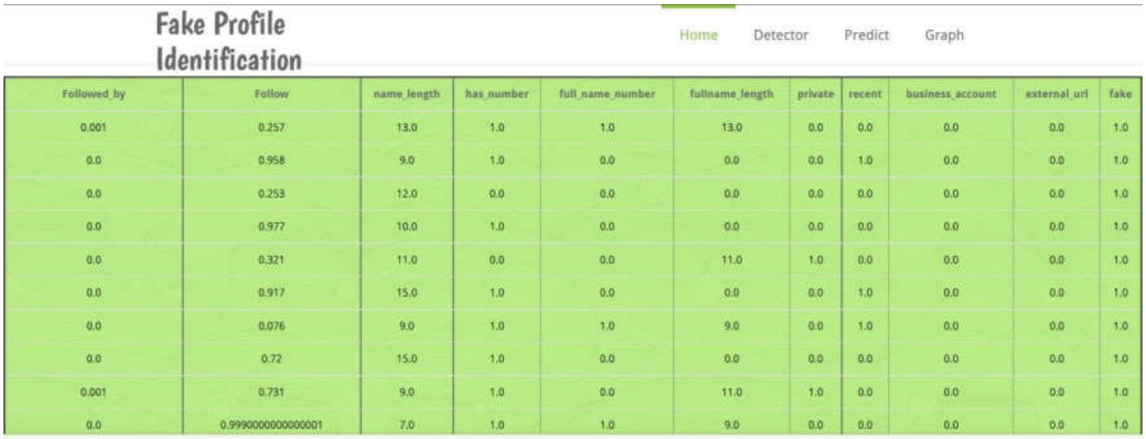


Fig5.2: Uploading of data set using upload button.



Followed_by	Follow	name_length	has_number	full_name_number	fullname_length	private	recent	business_account	external_url	fake
0.001	0.257	13.0	1.0	1.0	13.0	0.0	0.0	0.0	0.0	1.0
0.0	0.958	9.0	1.0	0.0	0.0	0.0	1.0	0.0	0.0	1.0
0.0	0.253	12.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
0.0	0.977	10.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
0.0	0.321	11.0	0.0	0.0	11.0	1.0	0.0	0.0	0.0	1.0
0.0	0.917	15.0	1.0	0.0	0.0	0.0	1.0	0.0	0.0	1.0
0.0	0.076	9.0	1.0	1.0	9.0	0.0	1.0	0.0	0.0	1.0
0.0	0.72	15.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0
0.001	0.731	9.0	1.0	0.0	11.0	1.0	0.0	0.0	0.0	1.0
0.0	0.9990000000000001	7.0	1.0	1.0	9.0	0.0	0.0	0.0	0.0	1.0

Fig5.3: View data after uploading the dataset.

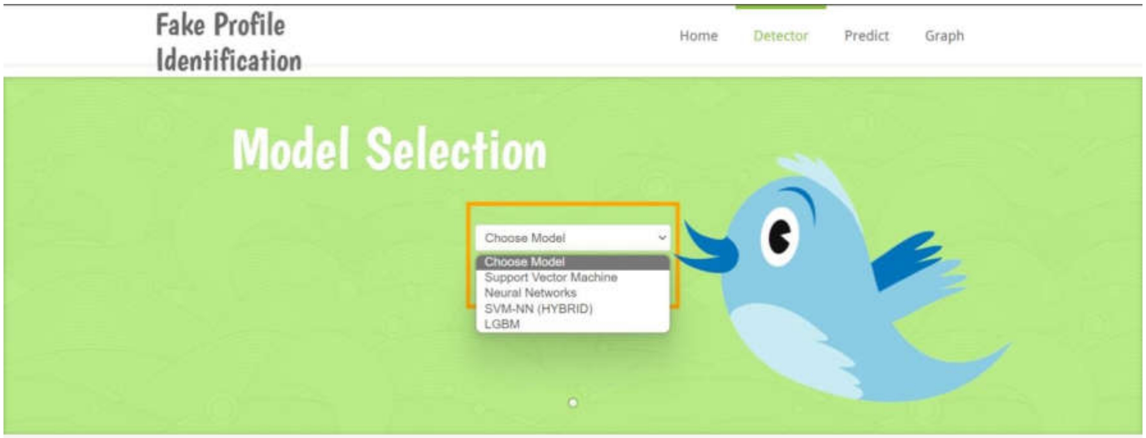
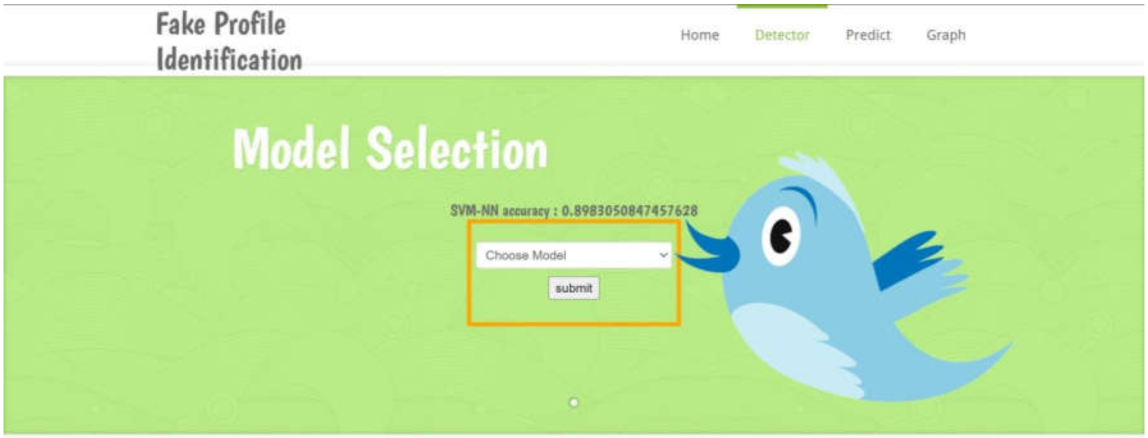
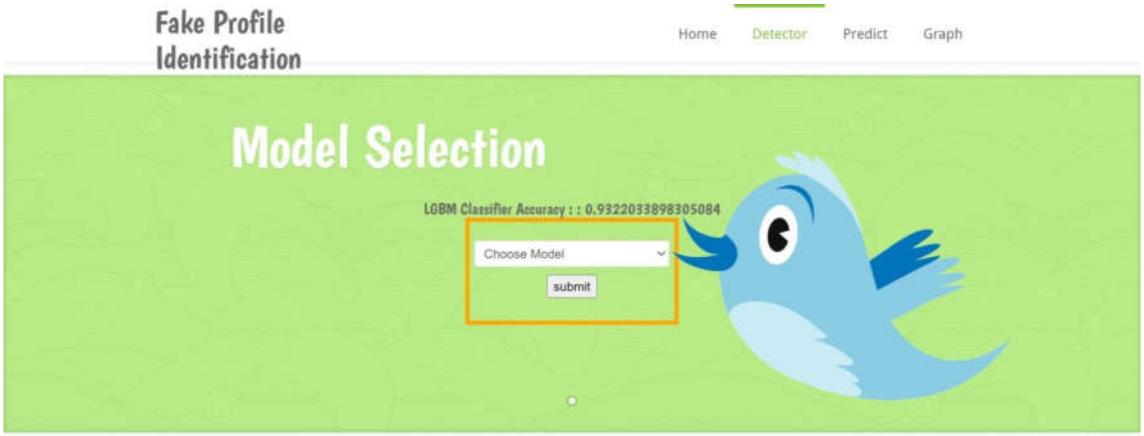


Fig5.4: Selection of the required machine learning model.



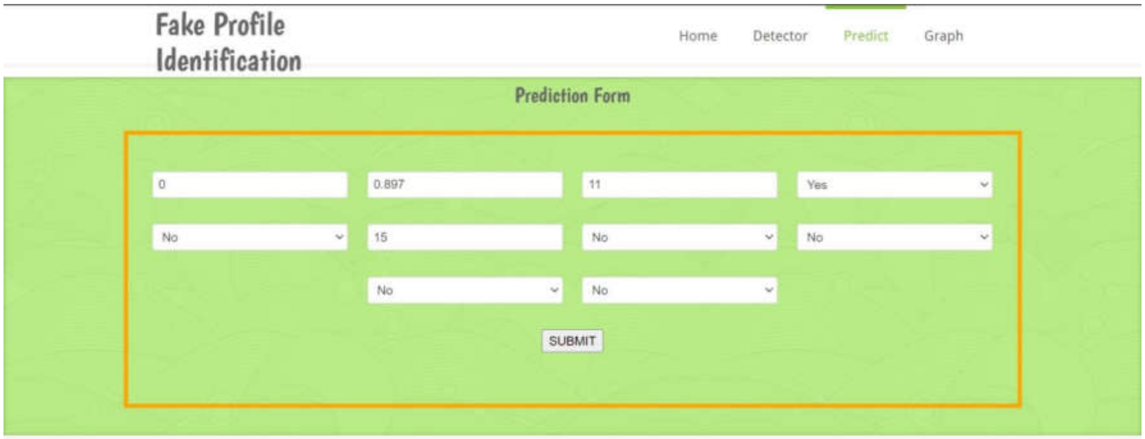
SVM-NN accuracy : 0.8983050847457628

Fig5.5: View the SVM-NN accuracy by selecting the SVM-NN model.



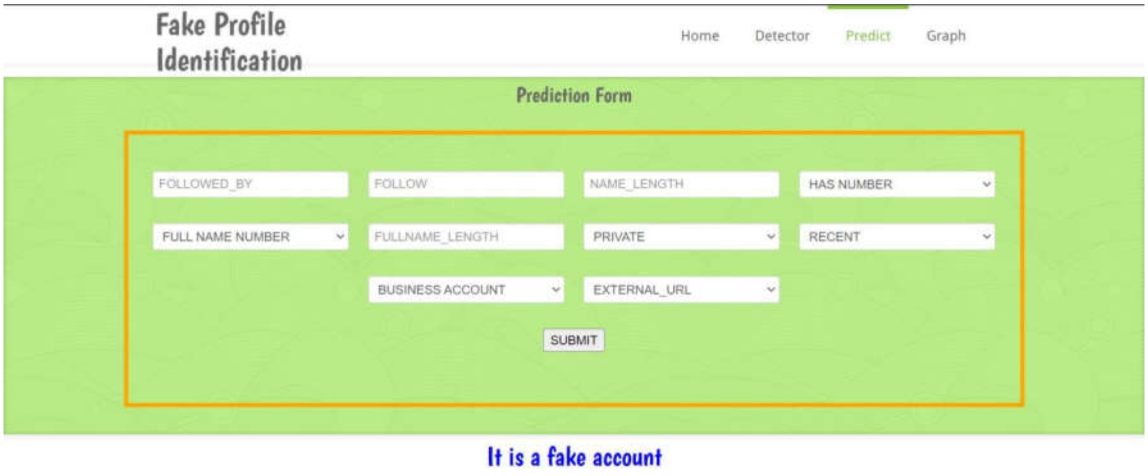
LGBM Classifier Accuracy : : 0.9322033898305084

Fig5.6: View the Light GBM accuracy by selecting the Light GBM model.



0	0.897	11	Yes
No	15	No	No
	No	No	

Fig5.7: Enter the user profile details for prediction.



Fake Profile Identification

Home Detector Predict Graph

Prediction Form

FOLLOWED_BY FOLLOW NAME_LENGTH HAS NUMBER

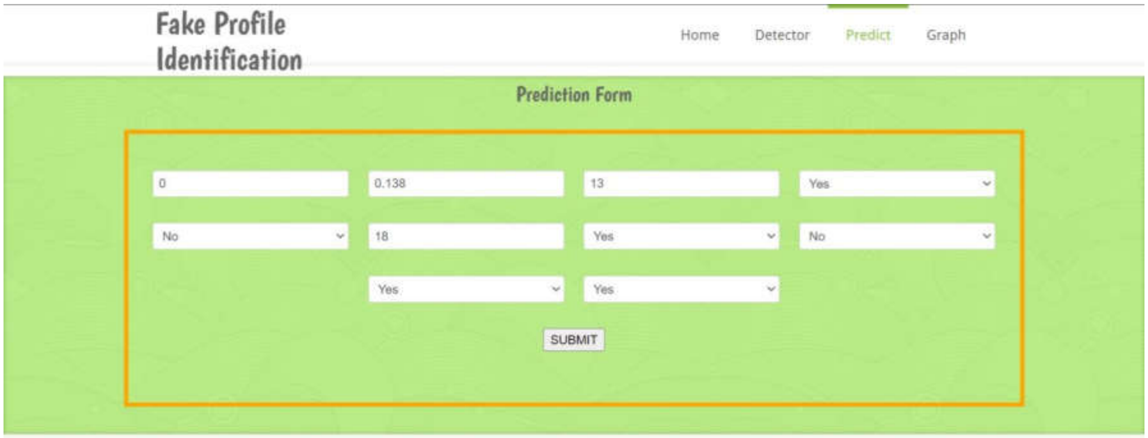
FULL NAME NUMBER FULLNAME_LENGTH PRIVATE RECENT

BUSINESS ACCOUNT EXTERNAL_URL

SUBMIT

It is a fake account

Fig5.8:This shows the sample output prediction of 7.7.



Fake Profile Identification

Home Detector Predict Graph

Prediction Form

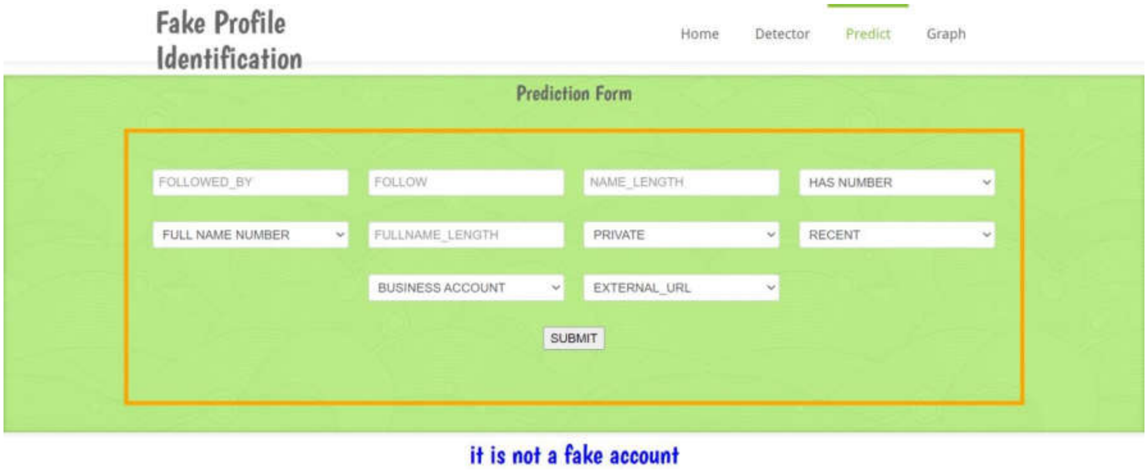
0 0.138 13 Yes

No 18 Yes No

Yes Yes

SUBMIT

Fig5.9: Enter the user profile details for prediction.



it is not a fake account

Fig5..10: This shows the sample output prediction of 7.9.

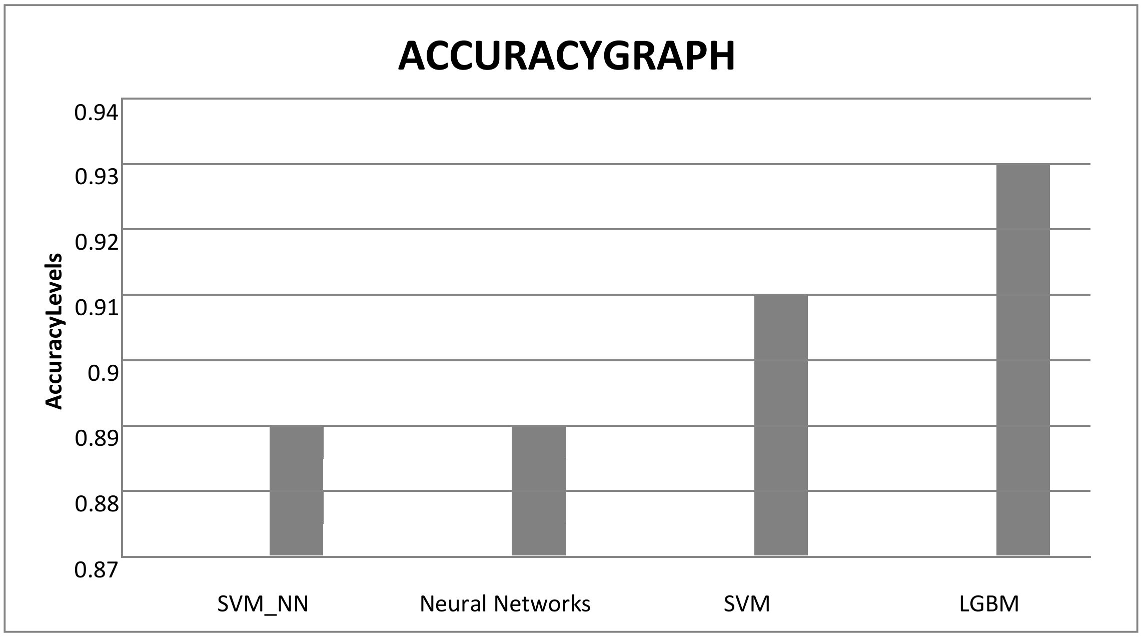


Fig5.11: Comparing the accuracies for the differential gorithms.

6. CONCLUSION

Identification of fake profiles on social media works well on the proposed system. After the proper analysis and comparison, it was found that LGBM i.e., Light Gradient Boosting Machine Learning algorithm gives the better results when compared with the other classifiers. The accuracy score for Light GBM model is 93.2%. Through the performance comparison analysis, we showed that our proposed solution is feasible and is capable to give better results than other existing systems. In the future, it may be possible to alter the dataset size and work on enhancing the machine learning algorithms to produce a more potent model that can swiftly categorise all varieties of phoney profiles from various social networks.

References:

(1) A.T.Kabakus and R.Kara,"A survey of spam detection methods on twitter", International Journal Of Advanced Computer Science And Applications, vol. 8, no. 3, pp.29–38,2017.

(2) A.-Z. Ala'M, H. Faris et al., "Spam profile detection in social networks based on public features", in Information and Communication Systems (ICICS), 20178th International Conference on.IEEE,2017,pp.130–135.

(3) R. Kaur and S. Singh, "A survey of data mining and social network analysis based a nomaly detection techniques," Egyptian informatics journal, vol. 17, no. 2, pp. 199–216,2016.

(4) A.K.Ameen and B.Kaya,"Detecting spammers in twitter network," International Journal of Applied Mathematics, Electronics and Computers,vol.5,no.4,pp.71–75,2017.

(5) S. D. Jadhav and H. Channe, "Comparative study of K- NN, naive bayes and decision tree classification techniques," International Journal of Science and Research,vol.5,no.