JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A survey on identifying fake profiles using ANN

Mr. Ch. Vijay Kumar[1], E. Rupa Reddy [2], Nigam Archana [3], S. Ruthik Reddy

Associate Professor[1], Department of Computer Science and Engineering IV B.Tech Students, Department of Computer Science and Engineering [2,3,4] ACE Engineering College, Hyderabad, Telangana, India

ABSTRACT

Fake identities or profiles plays major role in advanced persisted threats, like cyber espinoge, including theft secrets. These are also involved in malicious and dangerous activities. Currently social network plays a major role in order to perform day to day activities by the users. Due to excess use of social media networks different kinds of scammers are attracted to it. These scammers create different fake identities in order to carry out various scams. In this project we are checking what is occurrence that the Facebook details are authentic or not by using Deep Learning-ANN. In order to perform these process we have extracted Facebook dataset from Github.

Different libraries involved in this project. We have also sigmoid function to determine weights. Several parameters of any particular social media site which are very crucial in provided solutions are also consired.

Due to presence of bots and fake profiles there are other dangers to personal data which are used for fraudulent purpose. Bots are type of program which access the data of users without users having information about them, it is also called web scrapping. To gain the access to private information these bots come in form of fake friend request or it can be hidden.

Keywords:

Fake Accounts (profiles) Identification , Artificial Neural Networks of deep learning , SVM and ANN classifications (machine learning) .

INTRODUCTION

Social Media created a revolution in every human being's life. It created its own benchmark. In daily life of a every human being social media plays a crucial role. Social media is a platform where every is connected throughout the world. It connects every one form various sides of the world. We can communicate to every through social media by connecting to internet. Social Media works on internet. It created a scenario like if there is no social media the World stops.

Social Media became apart in many fields internally. Many of the companies promotes their product or business through social media. As many of the things depend on the social media like Facebook, Instagram, WhatsApp, twitter etc., many of the fake profiles are created. As their millions of users of Face book or WhatsApp etc., many of them are fake profiles. This fake profile leads to many security issues. Fake Profiles are created by some one to attract them and cheat them. They steal the personal information by creating fake profiles.

Fake Profiles leads to many worsts situations. Multiple accounts are created with user identities. They affect the victim reputation by spreading fake news. Even they get financial help from victim's friends by sending friends requests. This leads to even suicides of victims. So it is important to identify the fake profiles. By identifying the fake profile we can save the victims.

We have a solution to identify the fake profiles by using artificial neurons technology. It is a algorithm through which we can identify the fake profiles and we are making use of python programming language. This algorithm has potential to identify whether friend request is real or fake. It helps many social media companies to identify the fake profiles and real accounts by training the data set.

LITERATURE SURVEY

In this project, we use artificial neurons networks concept of deep learning to determine wheather that Facebook friend request is authentic or not. In this project, Facebook profile Dataset is taken to identify the fake profiles. Different libraries involved in this project. We have also sigmoid function to determine weights. Several parameters of any particular social media site which are very crucial in provided solutions are also consired.x

S. Dixon [1] Social-media are generally considered to be online platform for younger populations however people of all ages use such platforms for business purpose, politics, socializing and daily communication. In the year of 2021, half of all social media users told they use social media for staying connected with friends and family. In 2021, Facebook was used amongst most of the worldwide marketers with 93% of marketers reporting using Facebook.

Anita Balakrishnan, A. Guttmann [2] From each of its users Facebook makes an average of 6.18$ in Q4, it disclosed "Average Revenue Per User" commonly shortened to ARPU. Facebook makes most of the money by showing users advertisement like sponsored videos from brands or little Ad boxes on the bottom right-hand side of the screen. Other companies pay for that space on Facebook feed, and to filter who sees each Ad based on each viewers interest or likes.

Laura Hautala, Alfred Ng, Richard Nieva [3] According to this article 50 million people on the social media were effected. Facebook has a feature which lets people know how other profiles look and how their profiles look to others. The code related to this feature was exploited by the attackers which helped them to steal access tokens, which can be used to access the control over the other people's account. These tokens are not passwords, this allow people to log in without using it. As per this article 90 million people were logged out of their account by Facebook.

Tiago Pregueiro , Qiang Cao, Xiaowei Yang, Michael Sirivianos [4] At present users are easily believing the information present on the OSN. OSN's suffer from abuse in the form of fake accounts, which is not the account of real human. Online operators currently spend important resources to detect, verify and shut down fake accounts. Due to difficulty in identifying real and fake profiles it is not yet successful. A new tool was introduced in OSN, called sybilRank. This tool is graph based method.

A Mishra, AJ Sarode, [5] According to these authors the approach used to identify fake accounts is OSN. There is a much difference in way the people socialize as their social life has become associated with OSN. So these increased the problems like fake profiles and online impersonation.

Fake profile detection is feasible due to the proposed experimental framework. This is restricted to OSN like Facebook.

Devakunchari Ramalingam, Villiyammai chinnaiah [6] This article gives a detail report on preserving-Privacy fake profile detection.

A set of profiles were given. So, from these set fake accounts will be detected in the LinkedIn dataset. By using the principle component analysis the profiles are processed , features are extracted. Training model is developed by using these features , resilient propagation algorithm is used in SVM and ANN for Classification. To classify the fake accounts to the neural network SVM test data is given.

Sumo3000 in computer security [7] Symantec was able to quantify software code that interferes with computer's normal functions, rank zombie system and observe the number of websites that are phishing sites that are designated to trick computer user into disclosing personal data or banking account information.

Ravneet Kaur, Sarbjeeth Singh [8] For analysis detection abnormal activities. According to this paper, based on various characteristics different types of anomalies and their categorizations are discussed. These anomalies creates various problems, which is to be handled carefully. These gives an idea of number of datamining techniques to detect anomalies. For Eg. Some of the malicious users may use false identities and use them communicate with large number of innocent users.

Mishra and Sarode and [9] The article says to identifies /access different profiles they used a Facebook graph API tool, which is a sequence of steps to detect the fake accounts and extract data**.** The data is converted to structured format which is in JSON format by ML techniques. They also used supervised and unsupervised learning. Supervised learning have higher accuracy.

Year	Technique/Methodology	Pros	Cons
2019	Detection process Using Resilient Back Propagation in neural networks and SVMs	90% of the 200k accounts designated by SybilRank is likely to be fake.	There are some limitations that should be be addressed and to worked.
2019	Detection process Using Back Propagation, minimizing costs.	It considers social media parameters and determines Result.	No. of Limitations (very less Accuracy)
2019	Detection process Using deep learning (RNN and VAE models)	It supports for both text and user profile.	No additional tasks which are used for cyberbullying
2020	Detection process Using Generative Adversarial Network.	It easily determines fake or real.	unprecedented levels of accuracy and fidelity

2020	Detection process Using Navi bayes and KNN, random forest, Bagging Classifier.	Mails are verified based on content and verified domain names.	As this has a class-conditional independence. It make the machine misclassify some of the tuples.
2020	Detection process Using Reinforcement, SVM, Ada boost.	Both supervised and unsupervised are used.	Accuracy differs for different parameters.
2021	Detection process Using neural network SVM.	Its works effectively for small data, noise free data.	Not Suitable for large data, data has more noise.
2022	Detection process using AI synthesized faces.	Helps in easy Integration	Vulnerable Detection, privacy issues.

CONCLUSION

The reason for the study is to build up an Artificial Neural Network by persistently acquiring article from newspaper, when we open or login to social media we get many friend requests. Requests may be Real or Fake. This paper explains in detail how to identify the fake accounts or fake profiles using Artificial Neural Network.

ACKNOWLEDGEMENT

We would like to thank our guide Mr. Ch. Vijay Kumar and Mrs. Soppari Kavitha for dedicating their valuable time and guidance. Also, we are extremely grateful to Dr. M. V. VIJAYA SARADHI, Head of Computer Science and Engineering Department for his invaluable time, support, Ace Engineering College.

REFERENCES

[1] **S. Dixon**, Social Media – Statistics and Facts, Jun 21, 2022.

[2] **Anita Balakrishnan, A. Guttmann**, Political Advertising Spending On Facebook between 2014 and 2018 by sponsor category, Sep 18, 2018. Facebook made an average of $6.8 off each user in Q4, Jan 31, 2018

[3] **Richard Nieva, Laura Hautala** Facebook breach put data of 50 million users at risk, Sept 28, 2018

[4] **Tiago Pregueiro, Qiango Cao, Xiaowei Yang, Michal Sirivianos,** Aiding the detection of fake Accounts in large scale social online services, Conference: Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (NSDI'12), April 2012.

[5]**A Mishra, Akshay J. Sarode**, Audit and Analysis of Impostors : "An experimental approach to detect fake profile in online social network", Proceedings of 6th International Conference on Computer and Communication Technology 2015(ICCCT'15), PP. 1-8, 2015.

[6] **D Ramalingam, V Chinnaiah** – Fake profile detection techniques in large-scale online social network : A Comprehensive review, Computers & Electrical Engineering, Vol. 65, PP.177, 2018.

[7] **Sumo 3000** in Computer Security, list of top Countries found to have the most Cybercrime, Enigmasoftware.com

[8] **R Kaur, S Singh** , " A survey of data mining and social network analysis based anomaly detection techniques", Egyptian informatics journal, Vol. 17, no. 2, PP. 199-216, December 2015.

[9] **Arun Mishra and Akshay J. Sarode**. Using Facebook graph API Tool, IRE Journals, 2015