IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101267

Eliminating Creation of Fake Profile in Social Networks by using National Identification Number

Prof. Himanshu Taiwade[1], Aman Yerwarkar[2], Gaurav Sewatkar[3], Mayur Mandape[4], Milind Patle[5], Sagar Koli[6]

Assistant Professor, Department of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur, India[1]

Student, Department of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur, India[2,3,4,5,6]

Abstract: People use Online Social Networks to build social connections with others who are having similar personal interests or come from the same backgrounds and professions. These social platforms make people's lives better while generating lots of problems for society. Malicious individuals use social media to clone profiles by obtaining sensitive and crucial information from a target person. These attacks damage the reputation of legitimate users. Detecting these identical fraudulent accounts has thus become a critical aspect of modern social media. Many researchers have attempted to address the issue of detecting fake profiles in online social networks. More solid solutions, on the other hand, must be pursued. In this paper, we report on the investigation of a possible approach to eliminating fake profile creation.

Keywords: Online Social Networks, National Identification Number, National ID, Fake Profile, Profile Cloning.

I. INTRODUCTION

The use of social media sites such as Facebook, Instagram, and Twitter is growing every day. Individuals and organizations use social networks to express their views, advertise their products, and express their careers at their companies and organizations. Users tend to reveal a large amount of personal information to the public because of the socializing nature of online social networks, and this sensitive data may be utilized by exploitative users to create fraudulent profiles for various objectives. In most social platforms, user identification is mainly based on limited displayed user details and this makes the user authentication feeble since it is possible to have more than one account with an equivalent name and lots of other similar details. Because of this ability, identity cloning attacks are one of the most serious security threats on social media. When a fraudster creates a profile that appears identical to an existing one and posts obscene content while impersonating someone else in order to get personal information and destroy the victim's reputation. Encountering or recognizing fake profiles on social media nowadays is very difficult. To solve this problem the proposed approach in this project. To eliminate fake profiling there should be a system that allows a user to make only one account. This can be implemented in social networks by allowing users to authenticate with a national ID. This will also eliminate fake user information sharing about their Profiles.

II. REVIEW OF LITERATURE

Studies show that various fake profiles recognition approaches, according to studies, are based on the examination of individual interpersonal organizational profiles with the goal of identifying the traits or a combination of attributes that aid in the detection of authentic and false records. In[5] the author uses some approaches, Following the extraction of numerous information from profiles and posts, classification methods such as Support Vector Machine(SVM), Naive Bayes, and Decision trees are utilized to build a classifier capable of identifying bogus records. Hence, as a result, clone profile identification has become a hot topic in computer science research throughout the world, with 75 percent of available methods discovered after 2010[1].

Research [6] suggests that phantom profiles in online social gaming can be detected and characterized. This article analyzes phantom Facebook accounts created to achieve higher privileges (e.g., higher rank, higher rewards, points) by inviting phantom profile players to a legitimate player's friend list. This leads to an increase in Phantom Profile accounts. The author identifies 13 attributes for each user of the game and performs a classification algorithm. However, the article concludes that this method does not have perfect accuracy in finding users as real or fake. The study [7] shows that not only do humans build fake accounts these days; machine learning techniques are also employed to launch false accounts. These algorithms are known as Social Bots. The author described a technique for detecting social media bots as thousands

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101267

of characteristics extracted from public data with accompanying meta-data are used in this context. The Twitter bots dataset was used to test the classification method. 9% to 15% of Twitter accounts are bots, according to the algorithm.

National Identification Number-based registration, which enables the registration of users who belong to that information. Then users will get an OTP on their registered mobile number which is linked to their Aadhaar id. The data which is related to that Aadhaar id will get fetched automatically. This system will protect against fake profile cloning.

III. RESEARCH METHOD

The proposed module is used to eliminate fake profiling here how it works. When a user visits 1st time then it has to register on our system by providing a National Identification Number. After giving National Identification Number as input, our system will check that is it in a National Database by API (Application Programming Interface) request if that id does not exist in the National ID database then the system will give an error that please enter valid National id else if national id exists in National ID Database, then OTP (One Time Password) will send on the registered phone number with that ID which will be valid only for 1 minute. When the user completes the OTP authentication step, after that the details associated with National ID will get fetched and the user not able to change the name this feature helps people discover user account by user's name then the user will proceed for the next and final step where user have to set username and password after that user can register itself. So, when users visit a second time, they just need to log in. This will eliminate fake profiling as every person has a single National ID.

Advantages:

1) It will eliminate fake profile making.
2) It will assure us that we are sharing our information with a genuine person.

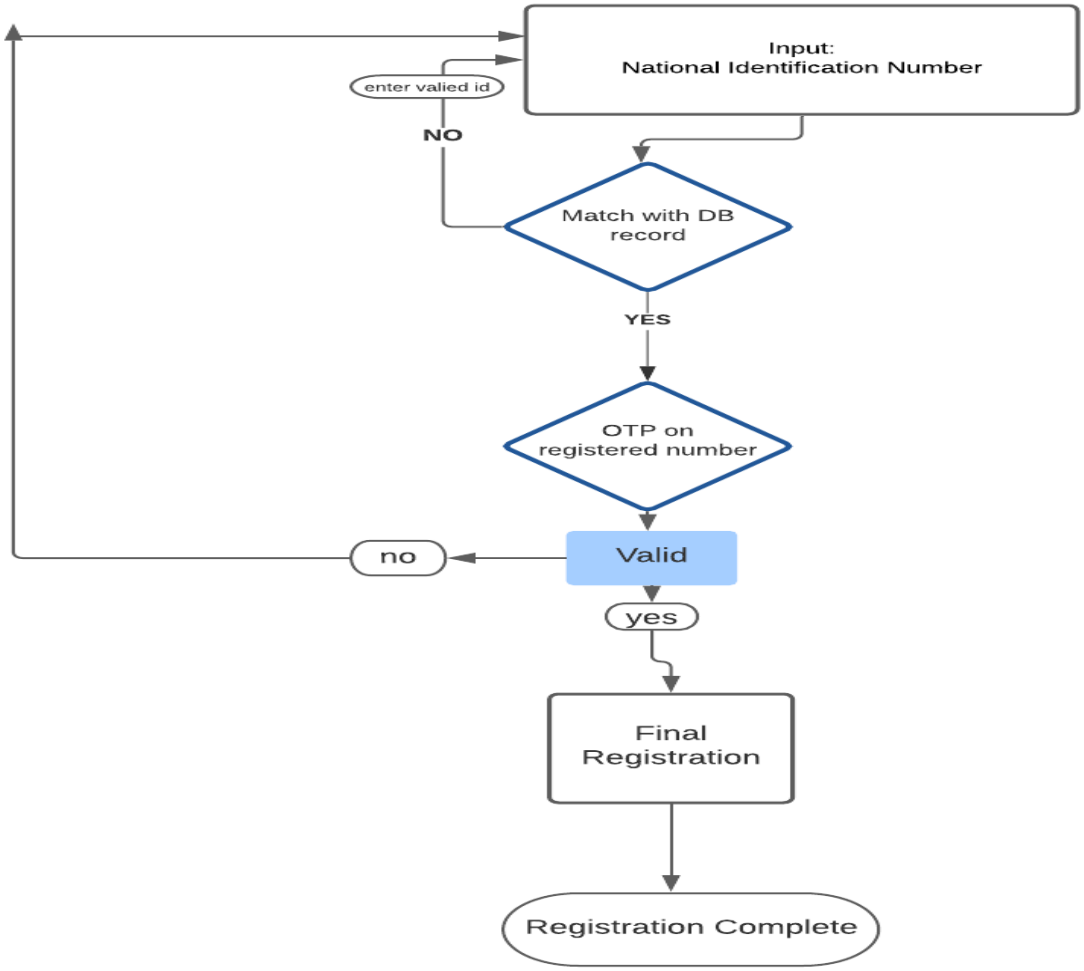

Fig.3.1: Data Flow Diagram

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101267

IV. FINDING AND ANALYSIS

People use various social media apps for entertainment, and there are various malicious users who clone the profiles and details creating fake profiles of the users and creating problems with privacy of the users. With the help of Aadhaar authentication we can eliminate the threat of the creation of users from fake profile cloning. (Twitter, Facebook).
As a result of the study [8], we find that, recently, Facebook published its latest Community Standards Enforcement Report based on Q3 of the year 2021. This includes all entities that they took action on, it contains accounts created with malicious intent to violate the company's policies, personal profiles created to represent business and organization, and most of the accounts used in spam campaigns. Social bot accounts created by machine learning algorithms were also reported by Facebook. Similar work was done in the study [7] showing contributions using user metadata.

Presumptive analysis of fake accounts and profiles created for malicious activity, spam, and more. represents approximately 5% of global monthly active users based on Facebook analytics in Q3 2021. Recent year's analysis graph is shown in fig 4.1.
In fact, despite all efforts to detect fake accounts on Facebook, there are still many fake accounts. As mentioned, the relative number of fake accounts will never change as tools evolve, so there will always be millions of fake Facebook profiles at any given time. Something seems to work, but it doesn't. That's why the National Identification number-based authentication leads to eliminating the fake profile creation at the root level.

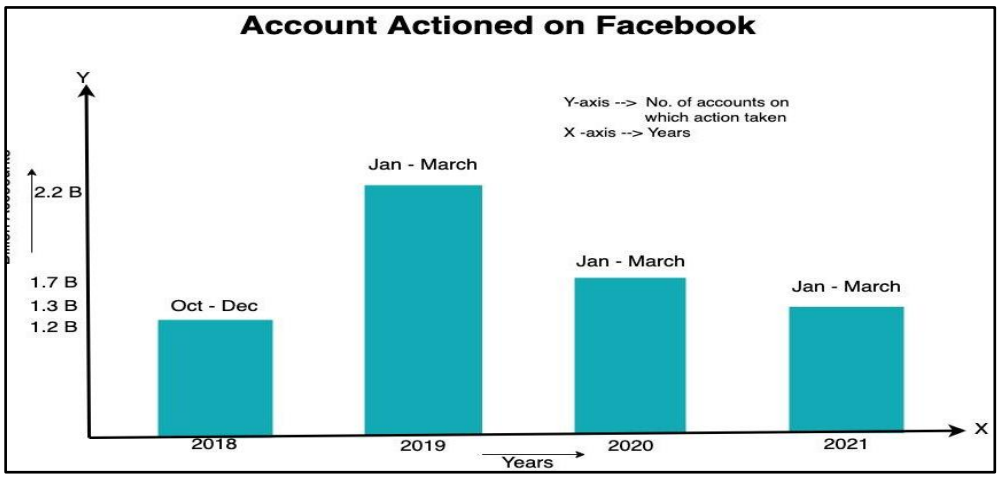

Fig.4.1: No. of Accounts actioned by Facebook during years 2018, 2019, 2020, 2021

V. RESULTS

By implementing this module in Online Social Networks we can easily eliminate fake profile attacks.

VI. DISCUSSION

BY CONSIDERING ALL THE ASPECTS OF ONLINE SOCIAL NETWORKS WE HAVE PROPOSED A MODEL THROUGH WHICH WE CAN ELIMINATE FAKE PROFILING.

VII. LIMITATIONS

1. The Proposed Module cannot be implemented in the region/country which doesn't have National Identification policies for residents.

VIII. CONCLUSION

Creating profile cloning is a serious problem that has developed throughout online social networks in recent years, causing harm to genuine members in the network by exploiting personal information. Several researchers have attempted to address this issue by recognizing clone profiles across various social media networks. However, due to the difficulty in finding real datasets for research and the higher diversity of profiles in these networks, fully compatible solutions are still to be taken. This approach enables us to eliminate fake profiles threats using National Identification Number. For false profile detection, an overview of strategies employed by various researchers is offered. Sincere efforts have been made to collect in one place everything about malicious objects that exist in social networks on the Internet. To some extent, several studies have attempted to alleviate the detrimental impacts of fake profiles, but more specific efforts are required… Also, a brief outlining of the pros and cons of several existing cyber laws to curb online fake profiles has been

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 12, December 2021
DOI: 10.17148/IJARCCE.2021.101267

highlighted. It may be inferred that the demand for more advanced approaches for safe social networks remains unmet. To build automated techniques to identify suspicious users, the right procedures must be taken at the right time.

IX. FUTURE SCOPE

Some proposed techniques have been found after investigating current approaches. The study has suggested a biometric authentication method to use user fingerprints, voice and signatures to verify the identity of a user in a social network platform. This may result more accurate solutions since biometric characters are unique to each person. Some have proposed a user relationship prediction model to forecast future clone profiles. This will be more useful since prevention of attack is better than detection after the attack.

REFERENCES

1) Liyanage C.R, Premarathne S.C "A Walkthrough on Clone Profile Resolution in Social Networks".
2) Katharina Krombholz, Dieter Merkl, Edgar Weippl "Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model."
3) Bharti, Mr. Rajesh Yadav "Survey Paper on Automatic Detection of Fake A Profiles Over Social Networks."
4) A. Gupta and R. Kaushal, "Towards Detecting Fake User Accounts in Face- book," ISEA Asia Conf. 2017, ISEASP 2017, vol. 1, pp. 1–6, 2017.
5) N. Kumar and R. N. Reddy, "Automatic Detection of Fake Profiles in Online Social Networks," National Institute of Technology Rourkela Rourkela-769 008, Orissa, India, 2012.
6) Atif Nazir, Saqib Raza, Chen-Nee Chuah, Burkhard Schipper, "Ghostbusting Facebook: Detecting and Characterizing Phantom Profiles in Online Social Gaming Applications".
7) Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, Alessandro Flammini "Online Human-Bot Interactions: Detection, Estimation, and Characterization".
8) Facebook Community Standards Enforcement Report Available:[online]"https://transparency.fb.com/data/community-standards-enforcement/fake-accounts/facebook/#content-actioned"